



UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Enhanced Two-Phase Contention Window MAC Protocol for Wireless Sensor Networks Applications

Luís Miguel Moreira Borges

Tese para obtenção do Grau de Doutor em
Engenharia Electrotécnica e de Computadores
(3º ciclo de estudos)

Orientador: Prof. Doutor Fernando José da Silva Velez
Co-orientador: Prof. Doutor António Sérgio Portela Lebres

Covilhã, Outubro de 2012

To my beloved Family and Elisabete Martins

Acknowledgements

Above all, I owe my deepest gratitude to my supervisor Professor Fernando J. Velez and my co-supervisor Professor António Sérgio Lebres. Without their friendship, continuous optimism concerning the work, corrections improvements, ideas and constructive discussions this would hardly have been completed. I also want to thank them for encouraging me to pursue this PhD as well as for helping me on changing my view over research work. I am deeply grateful to Professor Rodolfo Oliveira from the Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, that revealed to be essential in the conception of the formulations for the proposed collision probability models. I want to express my gratitude to Professor Pedro Sebastião from ISCTE-IUL, for helping me in the comprehension and interpretation of several aspects of the Data Link Layer. I am also grateful to Thomas Watteyne that helped me a lot in the revision of the journal papers, as well as for helping me with the LaTeX editor. My gratitude also goes to Instituto de Telecomunicações (IT) and UBI, for the outstanding logistics provided that made this thesis possible. In particular, I would like to thank to Dr^a. Sara Correia. I want to express my deepest gratitude to Andreia Rente and Norberto Barroca for being good friends, for the important collaboration in this PhD and helping me in the development and testing of different solutions for the WSN projects in which I participated, giving me the possibility of developing interdisciplinary research work. To all my colleagues from the WE-MOVE@IT group, Orlando Cabral, João M. Ferro, João Oliveira, Daniel Robalo and Rui Paulo for their support, sharing of ideas and good companion environment. To all the remaining colleagues from the WE-MOVE@IT group goes my special thanks. Also a special thanks to the colleagues from the Computational Fluid Dynamics (CFD) group from UBI for their fellowship. A special thanks is owed to a group of friends from “Pingulim’s House” in Covilhã: Elisabete Martins, José Oliveira, César Marques, Hélder Henriques, Hélder Duarte, Joana Malheiro, Michal Karlicki and Katarzyna Sobieszek. This work was supported by the PhD FCT grant SFRH/BD/38356/2007 and IT grant PEst-OE/EEI/LA0008/2011. I also acknowledge several projects where I was involved in: COST IC1004, COST 2100, MobileMAN, OPPORTUNISTIC-CR, PROENERGY-WSN, Smart-Clothing, and INSYSM . I want to express my gratitude to Mr. Rui Barata, for his help and time spent in the fabrication of several PCB boards. I would also like to thank to J. Heidemann and W. Ye, who helped me in the interpretation of the SCP-MAC protocol, and to Prof. Anna Guerman, who helped on bringing to light the combinatory solution from the model. We would like to thank to Bernhard Firner for giving permission to use the following material in Figure 7.3 from Chapter 7. Finally, I am very grateful to my beloved Elisabete Martins, for all the support given and patience throughout this years, since I initiated my PhD work. I also owe my deepest gratitude to Elisabete Martins for all the help in the edition in LaTeX and for the suggestions and advices. A special gratitude to my parents: Rui Borges Pereira and Maria Emilia Pereira, my brother Valter Borges, closest family and friends, for their love, encouragement and unconditional support, always present, during all my live. My apologies to all for the moments of less presence and for understanding the reason, during the periods of more involvement in this work.

Abstract

Nowadays, the user of Wireless Sensor Networks (WSNs) is becoming more and more demanding in terms of choice and diversity of applications. As a consequence, as the diversity of applications continues to grow there is a need to identify and classify the set of detailed characterization parameters that facilitates to sketch up a taxonomy for WSN applications. The proposed taxonomy identifies the services offered by each application makes a tool available to better understand the services and requirements of each application, along with a holistic overview of the WSN proposed application taxonomy. The research also involved the actual development of WSN applications within different research projects, namely in the fields of healthcare (Smart Clothing), civil engineering structure monitoring (INSYSM) and precision agriculture.

Different medium access control mechanisms employ different collision avoidance schemes to cope with packet collision and retransmission, trading-off complexity, energy inefficiency and control of packet overhead. In particular, this PhD thesis addresses the study the packet collision probability for a MAC protocol that employs a collision avoidance mechanism with two contention window and consequent proposal of a model for the collision probability. Simulation results validate the model for saturated traffic. For unsaturated traffic and with a small number of nodes, the accuracy of the model is limited by numerical rounding. It is shown that, by using our analytical model, we have been able to obtain performance metrics such as network throughput and average service time for the successful transmissions.

In addition, the Enhanced Reliability Decision Algorithm in the physical layer has been proposed. The frame capture effect (FC) feature has been implemented in the IEEE 802.15.4 compliant physical layer of the MiXiM framework. The proposed decision algorithm utilizes the Signal to Noise-plus-Interference ratio (SNIR) and the size of the packet to guarantee the delivery with certain reliability to the MAC layer, of a packet received at the PHY layer. A gain of more than 10 % has been achieved in the delivery ratio. Promising results have also been obtained for the SCP-MAC protocol with the FC effect enabled, for different values of reliability.

As one of the main contributions of this thesis, an innovative efficient multi-channel MAC protocol, based on SCP-MAC, was proposed, the so-called Multi-Channel Scheduled Channel Polling (MC-SCP-MAC) protocol. The influential range concept, denial channel list (which considers the degradation metric of each slot channel), extra resolution phase algorithm and frame capture effect have been explored to achieve the maximum performance in terms of delivery ratio and energy consumption. It has been shown MC-SCP-MAC outperforms SCP-MAC and MC-LMAC in denser scenarios, with improved throughput fairness. Considering the influential range concept reduces the redundancy level in the network facilitating to reduce the energy consumption whilst decreasing the latency.

The conclusions from this research reveal the importance of an appropriate design for the MAC protocol for the desired WSN application. Depending on the objective or mission of the WSN application, different protocols are required. Therefore, the overall performance of a WSN application certainly depends on the appropriate development and application of the appropriate communication protocols (e.g., MAC, network layer).

Keywords

Wireless Sensor Networks, WSN applications taxonomy, MAC protocols, collision avoidance mechanism, frame capture effect, multi-channel, enhanced two-phase contention window

Resumo

Hoje em dia, os utilizadores de Redes de Sensores sem Fios (RSSFs) estão-se a tornar cada vez mais exigentes em termos de escolha e diversidade de aplicações. Assim, é fundamental identificar e classificar o conjunto de parâmetros de caracterização que possibilitam elaborar uma taxonomia para as aplicações em RSSFs. Esta taxonomia identifica os serviços oferecidos por cada aplicação e preenche o vazio existente na literatura das RSSFs, através da descrição da classificação e dos parâmetros de caracterização (critérios), possibilitando uma melhor compreensão dos serviços e dos requisitos de cada aplicação, em conjunto com uma visão geral holística da taxonomia proposta para as aplicações. A investigação também envolveu o desenvolvimento real de aplicações em RSSFs no contexto de diferentes projectos.

Mecanismos de controlo de acesso ao meio (MAC) distintos aplicam esquemas diferentes de prevenção de colisões para lidar com as colisões e as retransmissões, um equilíbrio entre a complexidade, eficiência energética e controlo de *overhead* de pacotes. Em particular, investiga-se a probabilidade de colisão de pacotes para um protocolo MAC que considera um mecanismo de prevenção de colisões com duas janelas de contenção, e a respectiva proposta dum modelo para a probabilidade de colisão. Embora as simulações validem os resultados para tráfego saturado, para tráfego não saturado e um número reduzido de nós, a precisão do modelo é limitada pelos arredondamentos numéricos. Mostra-se que, aplicando o nosso modelo analítico, conseguem-se obter métricas de desempenho, como o débito binário e o tempo médio de serviço.

Adicionalmente, propôs-se um algoritmo de decisão baseada em fiabilidade na camada física, de acordo com a norma IEEE 802.15.4, o efeito de captura de tramas (FC), no MiXiM. O algoritmo de decisão proposto considera a relação sinal-ruído-mais-interferência (SNIR) e o tamanho dos pacotes de forma a garantir a entrega de pacotes da camada física à camada MAC, com uma certa fiabilidade. Foi obtido um ganho superior a 10 % na entrega de pacotes com sucesso. Obtiveram-se resultados promissores para o protocolo *Scheduled Channel Polling* (SCP-MAC) em função da fiabilidade, considerando a habilitação do efeito de captura de tramas.

Uma das principais contribuições desta tese é a proposta de um protocolo MAC eficiente e inovador, baseado no SCP, o protocolo multi-canal de acesso calendarizado regular (MC-SCP-MAC). Exploraram-se os conceitos de área de influência, lista de negação de canais, fase de resolução extra e efeito de captura de tramas, de forma a maximizar a de entrega de pacotes e consumo de energia. Demonstra-se que o MC-SCP-MAC supera o SCP-MAC e o MC-LMAC em cenários com elevada densidade de nós, com uma *fairness* melhorada para o débito binário. A aplicação do conceito de área de influência no MC-SCP-MAC, origina uma redução do nível de redundância na rede, com a consequente redução do consumo de energia e do atraso extremo-a-extremo.

As conclusões extraídas desta investigação demonstram a importância dum dimensionamento adequado dos protocolos MAC para a aplicação de RSSFs pretendida. Dependendo do objectivo ou missão da aplicação, será necessário utilizar protocolos diferentes. Portanto, o desempenho global duma aplicação em RSSFs depende certamente do desenvolvimento e aplicação dos protocolos de comunicação apropriados (por exemplo, MAC e de nível de rede).

Palavras-chave

Redes de Sensores sem Fios, taxonomia de aplicações em RSSFs, protocolos MAC, mecanismo de prevenção de colisões, efeito de captura de tramas, multi-canal, protocolo MAC melhorado com janelas de contenção com duas fases

Contents

1	Motivation and Framework	1
1.1	Introduction	1
1.2	Motivation and approach	2
1.3	Main Objectives	5
1.4	Contributions	6
1.5	Structure of the Thesis	7
2	Taxonomies for the Characterization and Classification of WSNs Services and Applications	11
2.1	State-of-the-Art and Motivation	11
2.2	WSN Services and Applications	13
2.2.1	WSN services	13
2.2.2	WSN applications	13
2.3	Taxonomy for the Characterization Parameters	14
2.3.1	Service Parameters	15
2.3.2	Traffic Parameters	16
2.3.3	Communication Parameters	18
2.3.4	Service Components and Data Acquisition/Dissemination	21
2.3.5	Network Parameters	21
2.3.6	Node Parameters	23
2.3.7	Operation Environments	28
2.4	Range of Variation for the Characterization Parameters	31
2.4.1	Holistic Overview of the WSN Applications Taxonomy	32
2.4.2	New WSN Applications Categories	36
2.4.3	Example for the WSN Applications Taxonomy	42
2.5	WSN Applications Roadmap and Trends	49
2.6	Summary and Conclusions	53
3	WSN Real World Applications and Scenarios	55
3.1	Smart Clothing for Foetal Movement Monitoring Application	55
3.1.1	Challenges	55
3.1.2	Experimental Apparatus	57
3.1.3	Experimental Results and Conclusions	62
3.1.4	Summary and Conclusions	67
3.2	Concrete Structural Integrity - INSYSM Project	68
3.2.1	Introduction	68
3.2.2	Motivation and Objectives	68
3.2.3	SHT15 Humidity and Temperature Sensor	69
3.2.4	SHT21S Humidity and Temperature Sensor	70
3.2.5	Joint Verification of Shielded SHT15 and SHT21S Sensors	72
3.2.6	Results and Discussions	75
3.2.7	Joint Verification of Shielded SHT15 and SHT21S Sensors	78
3.2.8	Limitations and Challenges	80
3.2.9	Summary and Conclusions	81

3.3	Precision Agriculture - InterNodal Network Project	81
3.3.1	Introduction	81
3.3.2	Sensor Nodes	82
3.3.3	Master Node	84
3.3.4	Setting an Automatic Configuration of InterNodal Network	84
3.3.5	Practical Results	86
3.3.6	Summary and Conclusions	88
3.4	Final Remarks	88
4	Medium Access Control and Physical Layers in WSNs	89
4.1	Protocol Stack for WSNs	89
4.2	Other Protocol Stacks for WSNs	92
4.3	Evolution of the IEEE 802 Standards	95
4.4	IEEE 802.15.4 and ZigBee	96
4.5	IEEE 802.15.4 Physical Layer	98
4.5.1	IEEE 802.15.4 Device Types	99
4.5.2	IEEE 802.15.4 Device Roles	99
4.5.3	IEEE 802.15.4 Network Topologies	100
4.5.4	IEEE 802.15.4 PHY Specifications	101
4.5.5	IEEE 802.15.4 PHY Packet Structure	102
4.6	IEEE 802.15.4 MAC Layer	103
4.6.1	IEEE 802.15.4 Beacon-Enabled - Star topology	103
4.6.2	IEEE 802.15.4 Non-Beacon-Enabled - Star topology	104
4.6.3	IEEE 802.15.4 Non-Beacon-Enabled - Peer-to-peer topology	105
4.6.4	SuperFrame Structure	105
4.6.5	IEEE 802.15.4 MAC frames	108
4.7	Taxonomy for Medium Access Control	110
4.7.1	Survey on Unscheduled MAC protocols	117
4.7.2	Survey on Scheduled MAC protocols	118
4.7.3	Survey on Hybrid MAC protocols	119
4.7.4	Survey on QoS MAC protocols	121
4.7.5	Survey on Cross-Layer MAC protocols	122
4.7.6	Survey on Multiple based MAC protocols	123
4.8	Classification of MAC Protocols Characteristics	123
4.9	Summary and Conclusions	127
5	Scheduled Channel Polling MAC protocol	129
5.1	Context and Motivation	129
5.2	Two-Phase Scheduled Channel Polling mechanism	131
5.3	Synchronization Phase	132
5.4	State Transition Diagram for SCP	134
5.5	Implementation of the SCP Simulation Framework	138
5.5.1	SCP Simulator Parameters and General Definitions	138
5.5.2	SCP Simulator Layer Modes	139
5.6	Summary and Conclusions	141

6	SCP Performance Evaluation	143
6.1	Single-hop Performance results	143
6.1.1	Power Consumption without Piggyback and periodic traffic	145
6.1.2	Power Consumption with Piggyback and periodic traffic	146
6.1.3	Throughput Performance with heavy traffic load	147
6.2	Multi-hop Energy Efficiency - Linear Chain Scenario	149
6.3	Lifetime Analysis with piggyback (periodic traffic)	151
6.4	Performance Analysis of a Two-Phase Contention Scheme for Scheduled Channel Polling	158
6.4.1	Motivation for Using Two Contention Windows	158
6.4.2	Overview for the Saturated Regime	159
6.4.3	Overview for the Unsaturated Regime	159
6.4.4	Stochastic Collision Probability Model for the Saturated Regime	160
6.4.5	Stochastic Collision Probability Model for the Unsaturated Regime	166
6.4.6	Simulation Scenario	170
6.4.7	χ^2 Test in the unsaturated traffic regime	171
6.4.8	Discussion of the Results	173
6.5	Service Time and Throughput Theoretical Model for a Two- Phase Contention Window Mechanism	177
6.5.1	Stochastic Service Time and Throughput Model for the Saturated Regime	177
6.5.2	Simulation and Analytical Results Comparison	179
6.5.3	Summary and Conclusions	180
6.6	Simulation of SCP in the Context of IEEE 802.15.4	181
6.6.1	IEEE 802.15.4 Compliant	181
6.6.2	Comparison between IEEE 802.15.4 Compliant and IEEE 802.15.4 Absence	182
6.6.3	Summary and Conclusions	187
6.7	Final Remarks	188
7	Frame Capture Effect and Reliability Based Decider	189
7.1	Definition of Frame Capture	189
7.1.1	Related Work	190
7.1.2	Main Causes	191
7.1.3	Work Principles for the Frame Capture	191
7.2	Frame Capture Scenarios	192
7.3	Potential Impact on the Performance of MAC Protocols	199
7.4	Implementation of the Frame Capture Effect	200
7.4.1	Frame Capture Effect in Simulators	200
7.4.2	Physical Layer and Decision on Airframes	201
7.4.3	IEEE 802.15.4 BER Calculation	207
7.5	Reliability Concept and Decision Thresholds in FC	209
7.5.1	Enhanced Reliability Decision Algorithm in the Decider	212
7.5.2	Justification for the Frame Capture Decision Thresholds	217
7.6	Performance Evaluation	217
7.6.1	Simulation Scenario	218
7.6.2	Performance Metrics	219
7.7	Results	219
7.7.1	Previous Decider implementation	220

7.7.2	Enhanced <i>Decider</i> with Frame Capture	223
7.7.3	SCP-MAC Throughput and Delivery Ratio with Frame Capture	229
7.8	Summary and Conclusions	230
8	Multi-Channel-Scheduled Channel Polling Protocol	233
8.1	Motivation	233
8.2	Main States of the MC-SCP Protocol	234
8.2.1	Startup State	234
8.2.2	Synchronization State	235
8.2.3	Slot Channel Choice State	238
8.2.4	Discovery-Addition State	242
8.2.5	Medium Access State and Algorithm	243
8.3	Fundamentals of the Protocol	245
8.3.1	Enhanced-Two Phase Contention Window Mechanism	246
8.3.2	Packet Structure	248
8.3.3	Influential Range Concept	251
8.3.4	Denial Channel List	252
8.3.5	Frame Capture	254
8.3.6	Node Topology and Envisaged Real-World Scenarios	255
8.3.7	Extra Resolution Phase Decision Algorithm	256
8.4	State Transition Diagram and Description	257
8.5	Discussion of the Simulation Results for the MC-SCP-MAC Protocol	266
8.5.1	Collision Probabilities	266
8.5.2	Energy Efficiency per Delivered Packet	268
8.5.3	Collision Probability Performance	269
8.5.4	Energy Efficiency with Multiple Slot Channels and Contention Window Sizes	271
8.5.5	IR Concept and Energy Performance Evaluation	273
8.5.6	Impact of Traffic Periodic and Exponential Patterns in the Overall Performance	277
8.5.7	Impact of the Density of Nodes	285
8.5.8	Performance Analysis in the Cluster Topology	291
8.5.9	Performance Analysis in a Linear Chain Topology	298
8.5.10	Fairness Index Evaluation for the Throughput	303
8.6	Enhancements to be implemented in MC-SCP-MAC	305
8.7	Summary and Conclusions	306
9	Conclusions and Suggestions for Further Research	311
9.1	Conclusions	311
9.2	Suggestions for Future Research	320
A	Choice of the Simulator: Simulators Classification	323
A.1	Introduction	323
A.2	Objectives	323
A.3	Simulation Tools	323
A.3.1	Introduction to Simulation Tools	323
A.3.2	Comparing Simulation Tools	323
A.4	Conclusions	329

B	WSN Applications Tables for Characterization and Classification Taxonomies	331
B.1	Applications areas-description for Category 1 and 2 WSNs	331
B.2	Tables for WSN applications taxonomy	341
C	Smart-Clothing Description - Other applied solutions	357
D	Description of the INSYSM Project	359
D.1	Negative Temperature Thermistor Specification and Results	360
D.2	SHT21S - Humidity and Temperature Sensor characteristics	361
D.3	eZ430-RF2500 kit	362
D.3.1	SHT21S eZ430-RF2500 Acquisition System	363
E	Modelling Radio Frequency Propagation in MiXiM Framework	365
E.1	Mixed Simulator (MiXiM)	365
E.2	Environmental Models	365
E.3	Propagation Models	366
E.3.1	Friis Free Space Path Loss Model	367
E.3.2	Log-distance Path Loss Model	368
E.3.3	Log-normal Shadowing Path Loss Model	368
E.3.4	IEEE 802.15.4 Path Loss Models	369
E.3.5	IEEE 802.15.6 (draft) Path Loss model (WBAN)	372
F	IEEE 802.15.4 PHY Layer	375
F.1	IEEE 802.15.4 Country Regulations	375
F.2	IEEE 802.15.4 Frequency Bands	375
F.3	IEEE 802.15.4 Data Rates	376
F.4	IEEE 802.15.4 Network Topologies	377
F.4.1	IEEE 802.15.4 Star topology	377
F.4.2	IEEE 802.15.4 Peer-to-peer topology	377
F.4.3	IEEE 802.15.4 Cluster Tree Topology	378
F.5	IEEE 802.15.4 PHY Specifications	378
F.5.1	Receiver Energy Detection	378
F.5.2	Link Quality Indication (LQI)	379
F.5.3	Carrier Sense (CS)	379
F.5.4	Clear Channel Assessment (CCA)	379
F.5.5	Channel Selection	380
F.6	IEEE 802.15.4 PHY Packet Structure	380
G	IEEE 802.15.4 Standard MAC Layer	383
G.1	SuperFrame Structure	383
G.1.1	Timing Parameters	383
G.1.2	InterFrame Spacing	383
G.2	IEEE 802.15.4 MAC Frames	383
G.2.1	Beacon Frames	384
G.2.2	Data Frames	386
G.2.3	Acknowledgement Frames	386
G.2.4	MAC Command Frames	386
G.2.5	Slotted and Unslotted CSMA-CA Algorithm Phases	387

G.3	MAC Protocols Taxonomy	389
G.3.1	Unscheduled MAC protocols	389
G.3.2	Scheduled MAC protocols	391
G.3.3	Hybrid MAC protocols	395
G.3.4	QoS MAC protocols	397
G.3.5	Multiple based MAC protocols	398
G.4	Comparison of the WSN MAC Protocols	398
H	Birthday Paradox Problem	411
H.1	Birthday Paradox	411
H.1.1	Birthday Paradox Problem Solution	411
H.2	Birthday Paradox applied to packet collision analysis in WSN	412
I	Computation of the CW1 and CW2 Collision Probabilities	419
J	Extra Results for the MC-SCP-MAC Protocol	421
J.1	Extra Results of the Collision probabilities of MC-SCP-MAC	421
J.2	Extra Results for the Energy Performance from the IR Concept	422
J.3	Extra Results of the Impact of Traffic Patterns in the Overall Performance	423
J.4	Extra Results of the Impact of Traffic Patterns in Higher Density Deployments . .	424
J.5	Extra Results of the MC-SCP Performance Analysis in the Cluster Topology	425
J.6	Extra Results of the Impact of Density in the MC-SCP-MAC Protocol	427
	References	433

List of Figures

Figure 2.1	Application interface with the protocol stack in the: a) absence or b) presence of a general service interface.	14
Figure 2.2	Definition of the service classes within communication parameters. . . .	19
Figure 2.3	Basic service components.	21
Figure 2.4	Main types of sinks with single-hop communication.	28
Figure 2.5	Multi-hop network.	29
Figure 2.6	Deployment scenarios with multiple sources and/or multiple sinks. . . .	29
Figure 2.7	Deployment scenario with the presence of a mobile sink.	30
Figure 2.8	Event mobility in wireless sensor and actuator networks.	31
Figure 2.9	WSN applications roadmap and future trends.	49
Figure 3.1	Hierarchical network considering the WBAN and other communication networks.	56
Figure 3.2	Smart-Clothing main healthcare scenario.	57
Figure 3.3	Flex sensor belt.	58
Figure 3.4	Flex sensor belt acquisition system diagram.	58
Figure 3.5	Theoretical and calibration curves for the Flex sensor.	59
Figure 3.6	Algorithm diagram for the flex sensor acquisition system.	60
Figure 3.7	Block Diagram for the acquisition system.	61
Figure 3.8	Patient monitoring and IEEE 802.15.4 wireless networking.	61
Figure 3.9	Piezoelectric sensor MLT1010 (ADI Instruments).	62
Figure 3.10	Foetal movement curves (upper=belt, lower=mother): (a) detected by mother and belt, (b) detected by belt only, and (c) detected only by the mother.	62
Figure 3.11	Main window for Flex Sensor View application.	63
Figure 3.12	Real-time view chart plot for the Flex Sensor.	63
Figure 3.13	Results when patient stands up at time $t = 190$ s.	64
Figure 3.14	Results from Flex sensor 1 when patient is sited.	64
Figure 3.15	Results from Flex sensor 2 (Patient sited).	65
Figure 3.16	Results when patient is sited.	65
Figure 3.17	Diagram for the circuit to acquire the signals from the sensor.	66
Figure 3.18	Field tests for foetal movements' detection.	66
Figure 3.19	Test results for foetal movements' detection.	67
Figure 3.20	Schematic representation of temperature and humidity sensor inside a concrete cube (10 cm length size).	69
Figure 3.21	Preparation and placement of the temperature and humidity sensors inside a mortar cube (for its protection).	70
Figure 3.22	SHT21S acquisition system for the standalone version.	71
Figure 3.23	SHT21S wireless acquisition system.	72
Figure 3.24	Filter cap protection for the SHT15 and SHT21S sensors.	72
Figure 3.25	Mounting schematics for the filter cap protection for the SHT15 and SHT21S sensors.	73

Figure 3.26	Humidity and temperature results obtained using the SHT15 and SHT21S sensors for a controlled humidity of 75 %.	73
Figure 3.27	Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which silica gel particles are replaced by ice cubes.	74
Figure 3.28	Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which the desiccator is filled with water.	74
Figure 3.29	Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which the water is replaced by silica gel particles.	75
Figure 3.30	Sensor probe temperature versus measured temperature inside the fridge chamber by using an SHT15 temperature sensor.	76
Figure 3.31	Setup to measure temperature and humidity using an SHT15 sensor inside a mortar cube for sensor protection.	76
Figure 3.32	Preparations to measure early age concrete temperature and humidity using a SHT21S sensor inside a mortar cube.	77
Figure 3.33	Results for the humidity and temperature for the SHT21S sensor obtained in a cube placed in outdoor environmental conditions during summer.	77
Figure 3.34	Software program for the acquisition of the SHT21S eZ430-RF2500 sensor data.	78
Figure 3.35	Humidity and temperature results obtained using the SHT15 and SHT21S sensors during 5 days.	79
Figure 3.36	Preparations to measure early age concrete temperature and humidity using the SHT15 and SHT21S sensors inside a mortar shell.	79
Figure 3.37	Humidity and temperature results obtained using the SHT15 and SHT21S inside a mortar shell for 100 hours.	80
Figure 3.38	DAPR node.	83
Figure 3.39	Circuit Diagram of DAPR node.	83
Figure 3.40	Master node connection to PC.	84
Figure 3.41	Multi-hop data packet.	86
Figure 3.42	Plan of InterNodal network layout.	86
Figure 3.43	InterNodal network deployment.	87
Figure 4.1	Comparison between the WSN OSI, OSI and WLAN computer models.	90
Figure 4.2	Proposed WSN protocol stack.	92
Figure 4.3	Sensor network data-centric stack models (SensorNet example).	93
Figure 4.4	Functionality blocks over a WSN stack model.	94
Figure 4.5	Layered model.	94
Figure 4.6	Wireless standards.	95
Figure 4.7	Short-range wireless networking classes.	96
Figure 4.8	Power consumption in IEEE 802 based networks.	96
Figure 4.9	ZigBee® functional layer architecture and protocol stack.	97
Figure 4.10	Network Protocol based on IEEE 802.15.4 and not conform to the ZigBee Standard.	98
Figure 4.11	Channelization at the 868/915 MHz and 2.4 GHz bands.	99
Figure 4.12	Device roles in the IEEE 802.15.4.	100
Figure 4.13	IEEE 802.15.4 star topology.	100
Figure 4.14	IEEE 802.15.4 peer-to-peer topology.	101
Figure 4.15	IEEE 802.15.4 cluster tree topology.	101

Figure 4.16	PPDU format.	102
Figure 4.17	IEEE 802.15.4 operational modes.	104
Figure 4.18	Star network data transfer from network device in a beacon-enabled network.	104
Figure 4.19	Star network data transfer from a PAN coordinator in a beacon-enabled network.	105
Figure 4.20	Star network data transfer from a network device in a non-beacon-network.	105
Figure 4.21	Star network data transfer from a PAN coordinator in a non-beacon-enabled network.	106
Figure 4.22	Superframe structure with GTS.	106
Figure 4.23	The incoming and outgoing Superframes temporal evolution.	107
Figure 4.24	General MAC frame format and details of the frame control field.	108
Figure 4.25	Slotted and unslotted CSMA-CA mechanism for MAC Layer.	109
Figure 4.26	Taxonomy for WSN MAC protocols.	112
Figure 4.27	Taxonomy for the Unscheduled MAC protocols and different sub-categories.	113
Figure 4.28	Taxonomy for the Scheduled MAC protocols and different sub-categories.	114
Figure 4.29	Taxonomy for the Hybrid MAC protocols and different sub-categories.	114
Figure 4.30	Taxonomy for the QoS MAC protocols and different sub-categories.	115
Figure 4.31	Taxonomy for the Cross-layer MAC protocol for different sub-categories.	116
Figure 4.32	MAC protocols distribution among different categories.	117
Figure 4.33	BMAC packet exchange.	118
Figure 4.34	S-MAC frame format.	118
Figure 4.35	Preamble sampling mechanism.	119
Figure 4.36	IEEE 802.15.4 beacon-enabled superframe structure.	120
Figure 4.37	SCP-MAC two-phase contention window mechanism.	120
Figure 4.38	Transmission mechanism for collision avoidance of MERLIN.	122
Figure 5.1	SCP time frame period structure.	131
Figure 5.2	Wake-up tone duration as a function of the CW_1 chosen slot.	131
Figure 5.3	SCP Synchronization phase.	133
Figure 5.4	SCP State Transition Diagram.	137
Figure 5.5	Node's deployment example.	138
Figure 5.6	OMNeT++ SCP protocol stack and the different layers from a sensor node.	138
Figure 5.7	Simple linear chain wireless sensor network.	141
Figure 6.1	Comparison between the lower/upper bound and the simulation results for the power consumption per node set of SCP simulations with no piggybacking.	146
Figure 6.2	Comparison between the lower/upper bound and the simulation results for the power consumption per node set of SCP simulations with piggybacking.	147
Figure 6.3	SCP-MAC throughput performance considering high traffic load for different contention windows sizes configurations and number of transmitting nodes.	148
Figure 6.4	Mean energy consumption per node for multi-hop experiments with different contention windows sizes configurations (20 data packets over 9 hops), $k \in \{1, 2\}$	152

Figure 6.5	Expected lifetime with piggyback (higher bound), while considering $CW_1^{max}=8$ and $CW_2^{max}=16$ for different inter arrival periods, with $n_{peuk}=1.2$	155
Figure 6.6	Expected lifetime with piggyback (higher bound), while considering $CW_1^{max}=8$ and $CW_2^{max}=16$ for different inter arrival periods, with $n_{peuk}=1.4$	155
Figure 6.7	Battery voltage discharge, while considering $CW_1^{max}=8$ and $CW_2^{max}=16$ for different inter arrival periods, with $n_{peuk}=1.2$ and $n=211$	156
Figure 6.8	Battery voltage discharge, while considering $CW_1^{max}=8$ and $CW_2^{max}=16$ for different inter arrival periods, with $n_{peuk}=1.2$ and $n=91$	157
Figure 6.9	Battery voltage discharge, while considering $CW_1^{max}=CW_2^{max}=208$ for different inter arrival periods, with $n_{peuk}=1.2$ and $n=211$	157
Figure 6.10	Battery voltage discharge, while considering $CW_1^{max}=CW_2^{max}=208$ for different inter arrival periods, with $n_{peuk}=1.2$ and $n=91$	158
Figure 6.11	CW_1 collision probability as a function of n	161
Figure 6.12	Expected number of nodes that successfully pass from CW_1 to CW_2	162
Figure 6.13	CW_2 collision probability under saturated regime considering a individual slot state analysis, $k \in \{1, 2\}$	164
Figure 6.14	CW_2 collision probability considering saturated regime using a combinatorics approach, $k \in \{1, 2\}$	165
Figure 6.15	Uniform distribution example of nodes over the intervals.	166
Figure 6.16	Probability of a node to choose one of the G possible intervals as a function of θ and n , for $T_{tR}=50$ s.	167
Figure 6.17	Expected number of nodes to choose one of the G possible intervals as a function of θ and n , for $T_{tR}=50$ s.	168
Figure 6.18	CW_1 collision probability for the saturated (black solid and dash-dot lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n , for $\theta=0.1$	169
Figure 6.19	Expected number of successful nodes from CW_1 to CW_2 for the saturated (black solid and dash-dot lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n , for $\theta=0.1$	170
Figure 6.20	CW_2 collision probability for the saturated (black lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n for $\theta=0.1$, $k \in \{1, 2\}$	171
Figure 6.21	Homogeneous uniform WSN deployment simulation.	171
Figure 6.22	Simulation and analytical results for the $E[S], \hat{E}[S]$ in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max}=8$	174
Figure 6.23	Simulation and analytical results for the $E[S], \hat{E}[S]$ in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max}=16$	174
Figure 6.24	Simulation and analytical results for the CW_1 collision probability in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max}=8$	175
Figure 6.25	Simulation and analytical results for the CW_1 collision probability for $CW_1^{max}=16$ in unsaturated (solid line) and saturated (dashed line) regimes.	176
Figure 6.26	Simulation and analytical results for the CW_2 collision probability for $CW_k^{max}=8, k \in \{1, 2\}$ in unsaturated (solid line) and saturated (dashed line) regimes.	176

Figure 6.27	Simulation and analytical results for the CW_2 collision probability for $CW_k^{max} = 16, k \in \{1, 2\}$ in unsaturated (solid line) and saturated (dashed line) regimes.	177
Figure 6.28	Simulation and analytical results for the service time for $CW_k^{max} = \{4; 8; 16\}$, $k \in \{1, 2\}$ in the saturated regime.	179
Figure 6.29	Simulation and analytical results for the throughput for $CW_k^{max} = \{4; 8; 16\}$, $k \in \{1, 2\}$ in the saturated regime.	180
Figure 6.30	Lower/upper bound and simulation results with no piggyback for the power consumption per node of CC1100, CC2420 and AT86RF231.	183
Figure 6.31	Lower/upper bound and simulation results with piggyback for the power consumption per node of CC1100, CC2420 and AT86RF231.	183
Figure 6.32	SCP throughput in function of the number of transmitting nodes and maximum contention windows sizes, $k \in \{1, 2\}$	185
Figure 6.33	Average energy consumption in function of the inter-arrival time and different contention windows sizes for the multi-hop experiments, $k \in \{1, 2\}$	186
Figure 6.34	Mean packet latency over 9 hops in function of number of hops, for $CW_1^{max} = CW_2^{max} = 16$, while enabling/disabling ACK packets feature.	186
Figure 6.35	DPSR in function of the simulator run over 9 hops, for $CW_1^{max} = CW_2^{max} = 16$, while enabling/disabling the ACK feature.	187
Figure 7.1	Signal strength and reception for two signals transmitted simultaneously (adapted from [FXHZ10]).	193
Figure 7.2	Frame capture sections with one interfering frame (interference regions 1-5 are defined by the overlapping between the two frames).	195
Figure 7.3	The packet reception rates for (a) packets in collision regions 1-3, and (b) packets in collision regions 4-5 (b). The error bars define the estimated 95 % confidence intervals. (extracted from [FXHZ10])	196
Figure 7.4	Frame capture scenarios with more than one interfering frame for five different overlapping regions.	198
Figure 7.5	Interference region that may happen when times of arrival are not induced.	199
Figure 7.6	MiXiM physical layer diagram (extracted from [WSKW09], Figure 2).	201
Figure 7.7	<i>AirFrames</i> on the shared channel (adapted from [WSKW09]).	202
Figure 7.8	MiXiM physical layer TX flow diagram (adapted from [WSKW09]).	204
Figure 7.9	Flow diagram for the MiXiM reception layer. The colours from the blocks show the functionality called at each phase.	206
Figure 7.10	BER results for IEEE Std 802.15.4.	208
Figure 7.11	Results for PER for the IEEE Std 802.15.4 link layer and packets with 64 and 336 bits.	208
Figure 7.12	SNIR Mapping procedure in the IEEE 802.15.4 physical layer of MiXiM.	208
Figure 7.13	Minimum number of trials, k^* , needed to ensure that the packet reaches the receiver with a probability $\delta \in \{0.9; 0.99\}$, as a function of the BER for different packet lengths.	214
Figure 7.14	Reliability decision algorithm implemented in the MiXiM <i>Decider</i>	214
Figure 7.15	Upgraded MiXiM <i>Decider</i> - Modifications performed to enable Frame capture.	216
Figure 7.16	Example of a deployment scenario (the red circle is the sink node while the remaining ones are sources.	218

Figure 7.17	SNIR histogram distribution for the MiXiM <i>Decider</i> default implementation under Collision Scenario 1. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.	220
Figure 7.18	Normalized SNIR histogram distribution for the MiXiM <i>Decider</i> default implementation under Collision Scenario 2. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.	221
Figure 7.19	Normalized SNIR histogram distribution for the MiXiM <i>Decider</i> default implementation under Collision Scenario 3. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.	221
Figure 7.20	Normalized SNIR histogram distribution for the MiXiM <i>Decider</i> default implementation under Collision Scenario 4. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.	222
Figure 7.21	Normalized SNIR histogram distribution for the MiXiM <i>Decider</i> default implementation under Collision Scenario 5. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.	222
Figure 7.22	PSR versus SNIR distribution for all Collision Scenarios (1 to 5) of MiXiM <i>Decider</i> current implementation.	223
Figure 7.23	BER versus SNIR distribution for all the collision scenarios (1 to 5) in the MiXiM <i>Decider</i> default implementation.	223
Figure 7.24	Probability of success versus the number of, N , interfering nodes for different collision scenarios, with the reliability decision algorithm ($\delta_1 = 0.9$), considering the FC effect enabled and disabled.	224
Figure 7.25	Mean absolute error for all collision scenarios in the case the FC effect is enabled or disabled, ($\delta_1 = 0.9$).	225
Figure 7.26	Probability of success as a function of the number of interfering nodes, N , for the Collision Scenario 3, with the FC effect enabled and disabled, with $\delta_1 = 0.9$ and $\delta_2 = 0.99$	226
Figure 7.27	Variation of the mean absolute error with N for the Collision Scenario 3, with the FC enabled and disabled ($\delta_1 = 0.9$ and $\delta_2 = 0.99$).	226
Figure 7.28	Histogram with total, successful and discarded packets for the Collision Scenarios 1 or 4, with the FC enabled and disabled, with $\delta_1 = 0.9$	227
Figure 7.29	Histogram with total, successful and discarded packets for the Collision Scenario 3, with the FC effect enabled and disabled, with $\delta_1 = 0.9$	228
Figure 7.30	Histogram with total, successful and discarded packets for the Collision Scenarios 2 or 5, with the FC enabled and disabled, with $\delta_1 = 0.9$	228
Figure 7.31	Throughput of SCP-MAC protocol in the case of FC enabled and disabled with $\delta_1 = 0.9$ and $\delta_2 = 0.99$	229
Figure 7.32	Delivery ratio for the SCP-MAC protocol with the FC effect enabled and disabled, with $\delta_1 = 0.9$ and $\delta_2 = 0.99$	230
Figure 8.1	General FSM of MC-SCP.	234
Figure 8.2	One way message dissemination.	237

Figure 8.3	LCG cyclic behaviour.	240
Figure 8.4	Probability of nodes choosing the same slot channel when $N_{ch}=15$	241
Figure 8.5	Probability of nodes choosing the same slot channel when $N_{ch}=15$ for the cases of neighbouring IDs of the nodes are sequential or random.	241
Figure 8.6	Frame structure for the MC-SCP-MAC protocol.	244
Figure 8.7	SCP two-phase contention window mechanism: a) Sensor node has neither data to send nor to receive; b) Sensor node is ready to receive data; c) Sensor node has data to be sent.	246
Figure 8.8	Wake-up tone duration as a function of the CW_1 chosen slot.	247
Figure 8.9	Structure for the data packet in the MC-SCP-MAC protocol.	249
Figure 8.10	Structure for the SYNC packet.	249
Figure 8.11	Packet structure for the wake-up tone in the MC-SCP-MAC protocol.	250
Figure 8.12	Beacon packet structure for the MC-SCP-MAC protocol.	250
Figure 8.13	Structure for the MC-ACK and MC-NACK packets.	250
Figure 8.14	Influential range.	252
Figure 8.15	Considered topology: full tree topology scenario.	255
Figure 8.16	Considered single- and multi-hop scenarios.	256
Figure 8.17	Chain scenario (multi-hop).	256
Figure 8.18	Detailed finite state machine for the MC-SCP-MAC protocol.	259
Figure 8.19	Comparison of the CW_1 collision probability between the MC-SCP-MAC and SCP-MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max}=8$	266
Figure 8.20	Comparison of $E[S]$, $\hat{E}[S]$ between the MC-SCP-MAC and SCP-MAC protocols in the saturated (*) and unsaturated (**) regimes, for $CW_1^{max}=8$	267
Figure 8.21	Comparison of the CW_2 collision probability between the MC-SCP-MAC and SCP-MAC protocols in the saturated (*) and unsaturated (**) regimes, for $CW_1^{max}=8$	267
Figure 8.22	Comparison of the energy consumption per packet successfully delivered between MC-SCP-MAC and SCP-MAC protocols for the CC2420 and AT86RF231 transceivers.	268
Figure 8.23	Comparison of the dependence of the CW_1 collision probability with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max}=8$	269
Figure 8.24	Comparison of the dependence of the $E[S]$, $\hat{E}[S]$ with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max}=8$	270
Figure 8.25	Comparison of the dependence of the CW_2 collision probability with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_k^{max}=8$, $k \in \{1, 2\}$	270
Figure 8.26	Energy consumption per delivered packet with variable number of slot channels and contention window sizes between MC-SCP-MAC and MC-L-MAC, $k \in \{1, 2\}$	271
Figure 8.27	Comparison of the delivery ratio for different transmitter powers, for the MC-SCP-MAC and MC-LMAC protocols, $k \in \{1, 2\}$	272
Figure 8.28	Comparison of the energy consumption per delivered packet for different transmitter powers, for the MC-SCP-MAC and MC-LMAC protocols, $k \in \{1, 2\}$	273

Figure 8.29	Average energy consumption per node when IR is enabled (∇) and disabled (*) for different sizes of the network (50 packets are transmitted from each node to the PAN).	274
Figure 8.30	Average energy consumption per node when IR is enabled (∇) and disabled (*), for different sizes of the network (600 packets).	274
Figure 8.31	Energy consumption savings per node with IR enabled, for different sizes of the network when each node generates either 50 packets (*) and 600 packets (∇).	275
Figure 8.32	Average energy consumption per node when IR is enabled for different sizes of the network and number of data slot channels, i.e., $N_{ch} \in \{8, 15\}$ (600 packets).	276
Figure 8.33	Energy consumption savings per node with IR enabled for different sizes of network and $N_{ch} \in \{8, 15\}$ (600 packets).	276
Figure 8.34	1, 2 and 3-hidden terminal scenarios.	277
Figure 8.35	Aggregate throughput as a function of the number of sources for MC-SCP-MAC, MC-LMAC, CSMA and MMSN, with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.	278
Figure 8.36	Delivery rate of MC-SCP-MAC as a function of the number of source nodes with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.	279
Figure 8.37	Energy consumption per node of MC-SCP-MAC as a function of the number of sources with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.	280
Figure 8.38	Energy consumption per packet successfully delivered of MC-SCP-MAC as a function of the number of nodes with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.	281
Figure 8.39	Latency of MC-SCP-MAC as a function of the number of sources with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.	281
Figure 8.40	Aggregate throughput for the MC-SCP-MAC, MC-LMAC, CSMA and MMSN protocols with periodic (*) and exponential (∇) traffic patterns for different number of sources in the $50 \times 50 \text{ m}^2$ deployment scenario.	282
Figure 8.41	Delivery rate for the MC-SCP-MAC protocol with periodic (*) and exponential (∇) traffic patterns for different number of sources in the $50 \times 50 \text{ m}^2$ deployment scenario.	283
Figure 8.42	Energy consumption per node of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$	284
Figure 8.43	Energy consumption per packet successfully delivered of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$	284
Figure 8.44	Latency of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$	285
Figure 8.45	Aggregate throughput of MC-SCP-MAC, MC-LMAC and CSMA protocols with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) for different deployment scenario side lengths when IR enabled or disabled.	286

Figure 8.46	Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	287
Figure 8.47	Delivery ratio of MC-SCP-MAC, MC-LMAC and CSMA as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	287
Figure 8.48	Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	288
Figure 8.49	Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	288
Figure 8.50	Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	289
Figure 8.51	Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	290
Figure 8.52	Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.	291
Figure 8.53	Saving gain percentage per node of MC-SCP-MAC as a function of the deployment scenarios side lengths when IR is enabled with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).	291
Figure 8.54	Network deployment in the cluster topology.	292
Figure 8.55	Aggregate throughput as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR enabled (*) or disabled (∇) while varying the number of slot channels, for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).	293
Figure 8.56	Aggregate throughput as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR enabled (*) or disabled (∇) while varying the number of slot channels, for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).	294
Figure 8.57	Delivery ratio as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).	294
Figure 8.58	Delivery ratio as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).	295
Figure 8.59	Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).	296
Figure 8.60	Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).	296
Figure 8.61	Latency for MC-SCP-MAC as a function of Π_{irmax} when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).	297

Figure 8.62	Latency for MC-SCP-MAC as a function of Π_{irmax} when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).	298
Figure 8.63	Latency as a function of the number of hops for the MC-SCP-MAC and SCP-MAC protocols, with ACK enabled (∇) or disabled ($\nabla\nabla$) with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in the linear chain topology, for the MC-SCP-MAC and with T_{poll} as a parameter for the SCP-MAC with the number of slot channels as a parameter.	299
Figure 8.64	Latency of MC-SCP-MAC with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in linear chain topology for different number of slot channels.	300
Figure 8.65	Latency as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.	300
Figure 8.66	Latency as a function of the number of hops for MC-SCP-MAC protocol with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.	301
Figure 8.67	Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.	301
Figure 8.68	Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.	302
Figure 8.69	Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.	302
Figure 8.70	Throughput fairness index of MC-SCP-MAC for $n=10$	304
Figure 8.71	Throughput fairness index of MC-SCP-MAC for $n=30$	304
Figure 8.72	Throughput fairness index of MC-SCP-MAC for $n=99$	305
Figure A.1	Simple and compound modules in OMNeT++.	325
Figure A.2	A 3D visualization model	327
Figure A.3	NetTopo simulator components.	327
Figure A.4	NetTopo graphical user interface.	328
Figure C.1	Smart-Clothing On-Off belt with fabric pressure sensor.	357
Figure C.2	System diagram for the Conductive Fabrics based belt.	358
Figure D.1	On-going measurement of temperature with wireless sensors inside a concrete cube.	360
Figure D.2	Verification of the sensor probe and measured temperatures inside the concrete cube by using an NTC temperature sensor.	361
Figure D.3	Schematic principle of SDM signal. X represents either RH or T at different levels of sensor output.	362
Figure D.4	Frame sent by the ED.	363
Figure D.5	Frame sent by the AP.	363
Figure D.6	SHT21S eZ430-RF2500 version acquisition system.	363
Figure E.1	Linear interpolation for the standard deviation as function of distance.	370

Figure E.2	Comparison of the IEEE 802.15.4 path Loss models as function of distance.	371
Figure E.3	Normalized data packet success rate as function of distance.	372
Figure G.1	The IFS in (a) Acknowledged transmission and (b) unacknowledged transmission.	384
Figure G.2	MAC beacon frame structure and the PHY frame structure.	385
Figure G.3	Detailed description for the beacon frame fields.	385
Figure G.4	The MAC data frame structure and the PHY frame structure.	386
Figure G.5	The MAC acknowledgement frame structure and the PHY frame structure.	387
Figure G.6	IEEE 802.15.4 MAC command frame [GCB03, Far08].	387
Figure G.7	T-MAC data transferring mechanism.	392
Figure G.8	Time division structure of NAMA protocol.	394
Figure G.9	Data packet transfer in WiseMAC protocol.	395
Figure G.10	Comparison of the timelines between LPL's and X-MAC's approaches. . .	397
Figure H.1	Probability that two people do not have the same birthday in a group of n people.	412
Figure H.2	Probability that at least two people have the same birthday in a group of n people.	413
Figure H.3	Pascal's Triangle.	415
Figure H.4	Probability that at least two nodes choose the lowest order slot with $CW^{max} = 365$	417
Figure I.1	Flowchart for the algorithm to analyze the CW_1 and CW_2 collision probabilities.	420
Figure J.1	MC-SCP-MAC simulation results for the CW_1 collision probability as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$. . .	421
Figure J.2	MC-SCP-MAC simulation results for the $E[S], \hat{E}[S]$ as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$	422
Figure J.3	MC-SCP-MAC simulation results for the CW_2 collision probability as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_k^{max} = 8$, $k \in \{1, 2\}$	422
Figure J.4	Average energy consumption per node as a function of Π_{irmax} , when IR is enabled for different sizes of network (50 packets) and number of data slot channels, i.e., $N_{ch} \in \{8, 15\}$	423
Figure J.5	Aggregate throughput as a function of the number of sources for MC-SCP-MAC, MC-LMAC, CSMA and MMSN with periodic traffic generation.	423
Figure J.6	Aggregate throughput as a function of the number of sources for MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation.	424
Figure J.7	Aggregate throughput as a function of the number of sources for the MC-SCP-MAC, MC-LMAC, CSMA and MMSN protocols with periodic traffic generation in the 50×50 m ² deployment scenario.	424
Figure J.8	Aggregate throughput as a function of the number of sources for MC-SCP-MAC protocol with periodic (*) and exponential (∇) in the 50×50 m ² deployment scenario.	425

Figure J.9	Aggregate throughput as a function of Π_{irmax} for MC-SCP-MAC when IR is disabled with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} s^{-1}$).	425
Figure J.10	Delivery ratio as a function of Π_{irmax} for MC-SCP-MAC when IR is disabled with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} s^{-1}$).	426
Figure J.11	Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC when IR is enabled (*) and disabled (∇) with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} s^{-1}$). . .	426
Figure J.12	Latency as a function of Π_{irmax} for MC-SCP-MAC when IR is enabled (*) and disabled (∇) with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} s^{-1}$).	427
Figure J.13	Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with periodic traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	427
Figure J.14	Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with exponential traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	428
Figure J.15	Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	428
Figure J.16	Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	429
Figure J.17	Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	429
Figure J.18	Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	430
Figure J.19	Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	430
Figure J.20	Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 s^{-1}$) when IR enabled or disabled.	431
Figure J.21	Saving gain percentage per node of MC-SCP-MAC as a function of the deployment scenarios side lengths when IR is enabled with periodic traffic generation ($\lambda = 1/10 s^{-1}$).	431

List of Tables

Table 2.1	Characterization parameters for WSN applications.	15
Table 2.2	Application requirements in a WSN network with QoS support [CV04]. . .	17
Table 2.3	Definition of the acronyms for the traffic classes.	19
Table 2.4	Service components versus type of information.	21
Table 2.5	System on a chip characteristics of microcontrollers.	26
Table 2.6	System on a chip characteristics of microcontrollers (cont.).	27
Table 2.7	Typical values for the average velocity from WSN entities.	31
Table 2.8	Comparison of the C1WSNs and C2WSNs characteristics.	32
Table 2.9	Comparison of the ED and PE classes.	33
Table 2.10	Characterization of Category C1WSNs applications. †- PE; ⊕- PE&ED; ‡- ED	33
Table 2.11	Characterization of Category C2WSNs applications. †- PE; ⊕- PE&ED; ‡- ED	34
Table 2.12	Categories for time related applications.	36
Table 2.13	Aggregation of WSN applications for time related categories.	37
Table 2.14	Categories for data stream related applications.	38
Table 2.15	Aggregation of WSN applications for data stream related categories. . . .	39
Table 2.16	Categories for delivery and delay sensitivity related applications.	40
Table 2.17	Aggregation of WSN applications for delivery and delay sensitivity related categories.	41
Table 2.18	Service characterization parameters of WSN applications (I).	42
Table 2.19	Service characterization parameters of WSN applications (I) (cont.). . . .	43
Table 2.20	Service characterization parameters of WSN applications (II).	43
Table 2.21	Service characterization parameters of WSN applications (II) (cont.). . . .	43
Table 2.22	Traffic, Communications, service components, network and node parameters for WSN applications (I).	46
Table 2.23	Traffic, Communications, service components, network and node parameters for WSN applications (II).	47
Table 3.1	DAPR node consumptions.	84
Table 3.2	Table with configuration times computations.	86
Table 3.3	Data from InterNodal network indoor.	87
Table 3.4	Data from InterNodal network outdoor.	87
Table 5.1	SCP-MAC events and actions.	135
Table 5.2	SCP-MAC events and actions (cont.).	136
Table 5.3	Parameters defined in the configuration file for the different sensor node layers.	139
Table 5.4	Symbols used in radio analysis, and typical values for CC1100 radio working at 868 MHz and at full data rate.	140
Table 6.1	Parameters for a monitoring application that uses Mica2 motes.	153
Table 6.2	Simulation parameters.	172
Table 6.3	Monte Carlo simulation results for different seeds, $n = 10$	173
Table 6.4	Typical values for CC1100, CC2420 and AT86RF231 radios ($P_{tx}=1$ mW). . .	182

Table 7.1	Collision ratio in each collision region (example for the CC1100 transceiver, extracted from [FXHZ10]), with $\delta_{preamble}=32$ bits, $\delta_{sync}=32$ bits, $\delta_{data}=16$ bits, and $\delta=80$ bits.	193
Table 7.2	Frame Capture regions (data rate of 6 Mbps) [LKL ⁺ 07].	195
Table 7.3	Time of arrival (ToA) and time of ending (ToE) of the interfering signals.	198
Table 7.4	RSSI, Noise and SNIR mappings in dBm.	209
Table 7.5	SNIR distribution for the MiXiM <i>Decider</i> default implementation for the different collision scenarios.	220
Table 7.6	Values of the SNIR for a non-null PSR under different collision scenarios.	222
Table 7.7	Comparison of the average gains (%) between the cases of frame capture feature enabled and disabled.	225
Table 8.1	Duration of CS, sensitivity channel switch time for CC2420 and AT86RF231 radio transceivers.	246
Table 8.2	Reward and punishments for the degradation level metric from the denial channel list policies in MC-SCP-MAC.	253
Table 8.3	MC-SCP events and actions.	260
Table 8.4	Correspondence between N_{ch} and Δt_{SC} for the throughput fairness index for the MC-SCP-MAC protocol.	303
Table B.1	WSN applications areas description for Category 1 WSNs.	331
Table B.2	WSN applications areas description for Category 1 WSNs (cont.).	332
Table B.3	WSN applications areas description for Category 1 WSNs (cont.).	333
Table B.4	WSN applications areas description for Category 1 WSNs (cont.).	334
Table B.5	WSN applications areas description for Category 1 WSNs (cont.).	335
Table B.6	WSN applications areas description for Category 1 WSNs (cont.).	336
Table B.7	WSN applications areas description for Category 2 WSNs.	337
Table B.8	WSN applications areas description for Category 2 WSNs (cont.).	338
Table B.9	WSN applications areas description for Category 2 WSNs (cont.).	339
Table B.10	WSN applications areas description for Category 2 WSNs (cont.).	340
Table B.11	Service, traffic, communication, service components, network and node characteristics of metropolitan operation applications.	342
Table B.12	Service, traffic, communication, service components, network and node characteristics of military applications.	343
Table B.13	Service, traffic, communication, service components, network and node characteristics of civil engineering applications.	344
Table B.14	Service, traffic, communication, service components of environmental monitoring applications.	345
Table B.15	Network and node characteristics of environmental monitoring applications	346
Table B.16	Service, traffic, communication, service components, network and node characteristics of logistics applications.	347
Table B.17	Service, traffic, communication, service components, network and node characteristics of position & animals tracking applications.	348
Table B.18	Service, traffic, communication, service components, network and node characteristics of transportation applications.	349

Table B.19	Service, traffic, communication, service components, network and node characteristics of automobile, sensor & robots, reconfigurable WSN applications.	350
Table B.20	Service, traffic, communication, service components, network and node characteristics of industrial automation applications.	351
Table B.21	Service, traffic, communication, service components of health and mood-based services applications.	352
Table B.22	Network and node characteristics of health and mood-based services applications.	353
Table B.23	Service, traffic, communication, service components, network and node characteristics of entertainment applications.	354
Table B.24	Service, traffic, communication, service components of Smart office applications.	355
Table B.25	Network and node characteristics of Smart office applications	356
Table D.1	SHT21S pin assignment.	361
Table E.1	Path loss exponents and standard deviations measurements for different propagation environments and frequencies (adapted from [Rap01]). . . .	369
Table E.2	Path loss coefficients and standard deviations for different propagation environments ([MGAL04]).	373
Table F.1	IEEE 802.15.4 data rates and frequencies of operation.	377
Table F.2	Channel assignments.	380
Table F.3	Preamble field lengths and durations.	381
Table F.4	SFD field lengths.	381
Table G.1	Timing parameters in beacon enabled operating mode.	383
Table G.2	MAC commands frame types.	387
Table G.3	Unscheduled MAC protocols comparison.	399
Table G.4	Unscheduled MAC protocols comparison (cont.).	400
Table G.5	Unscheduled MAC protocols comparison (cont.).	401
Table G.6	Scheduled MAC protocols comparison.	402
Table G.7	Scheduled MAC protocols comparison (cont.).	403
Table G.8	Scheduled MAC protocols comparison (cont.).	404
Table G.9	Hybrid MAC protocols comparison.	405
Table G.10	Hybrid MAC protocols comparison (cont.).	406
Table G.11	Hybrid MAC protocols comparison (cont.).	407
Table G.12	QoS MAC protocols comparison.	408
Table G.13	Cross-Layer MAC protocols comparison.	409
Table G.14	Cross-Layer MAC protocols comparison (cont.).	410
Table H.1	Possible number of combinations for different number of nodes in the slot.	415

List of Acronyms

ABR	Available Bit Rate
ACK	Acknowledgement
Act	Active Period
ADC	Analog-to-Digital Converter
Adapt	Adaptive
AES	Advanced Encryption Standard
AMB	Sound Ambient Traffic
AP	Access Point
APL	Application
App	Application Demand
APS	Application Sub Layer
ASK	Amplitude-Shift Keying
AtAG	Abstract Task Graph
AWGN	Additive white Gaussian noise
BAN	Body Area Networks
BE	Backoff Exponent
Be	Beacon mode
BER	Bit Error Rate
BI	Beacon Interval
BLE	Battery Life Extension
BMAC	Berkeley MAC
BO	Beacon Order
BPSK	Binary Phase-Shift-Keying
BSC	Binary Symmetric Channel
BSN	Beacon Sequence Number
Busy	Busy Tone
BWSN	Building Wireless Sensor Network
C1WSNs	Category 1 WSNs
C2WSNs	Category 2 WSNs
CAP	Contention Access Period
CA-MAC	Channel Access MAC
CBR	Constant Bit Rate
CCA	Clear Channel Assessment
CCC	Common Control Channel
CD	Channel Detection
CDMA	Code Division Multiple Access
Cent	Centralized Scheduling
CFCP	Conditional Frame Capture Probability
CFP	Contention-Free Period
ChAP	Channel Assignment Packet
CID	Cluster Identifier
CLH	Cluster Head
CL	Cross-Layer
CMR	Centralised Management of Resources
Co	Reducing collisions

Conv	Converge cast
CR	Cognitive Radio
CRC	Cyclic Redundancy Check
CS	Carrier Sense
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CSS	Chirp Spread Spectrum
CW	Contention Window
C-MAC	Classifier MAC
DaP	Data Prediction
DAPR	Data Acquisition Processor Radio
Db & Fi	Double CW & Fixed size
Db & Var	Double CW & Variable size
DFS	Depth First Search
Dis	Dynamic size
Dist	Distributed Scheduling
DLL	Data Link Layer
DpR	Data frame preamble
DPSR	Data Packet Success Rate
DSCR	Dual-Stage Contention Resolution
DSSS	Direct-Sequence Spread Spectrum
DSSS-O-QPSK	Direct Sequence Spread Spectrum- Offset-Quadrature Phase-Shift Keying
DSMAC	Dynamic MAC
DT	Delay Tolerant
DtS	Data Packet Sampling
Dual	Dual-Channel
E2RMAC	Energy-Efficient Reliable MAC
EDe	Event Detection
ED	End Device
ECG	Electrocardiogram
EEG	Electroencephalogram
EnD	Energy Detection
ETSI	European Telecommunications Standards Institute
FC	Frame Capture
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDX	Full Duplex
FFD	Full- Function Device
FFT	Fast Fourier Transform
FHR	Foetal Heart Rate
Fi	Fixed
FlexiMAC	Flexible MAC
FN	Forwarder Node
FPA	Fast Path Algorithm
FPS	Flexible Power Scheduling
FrD	Framelets Division
FrH	Frequency hopping
FRTS	Future Request To Send

FSK	Frequency-Shift Keying
FSM	Finite State Diagram
FTS	Fault Tolerant Slot
GFSK	Gaussian Frequency-Shift Keying
Glob	Global Schedule
GSM	Global System for Mobile Communications
GTIM	Gateway Traffic Indication Information
GTSs	Guaranteed Time Slots
GTNetS	Georgia Tech Network Simulator
GUI	Graphical User Interface
G-MAC	Gateway MAC
HDS	High Data Stream Applications
HDX	Half Duplex
Hi	High Traffic
HID	High-Rate Data
HR	High-Rate
IEEE	Institute of Electrical and Electronic Engineers
IC	Integrated Circuit
IL	Reducing Idle Listening
ICT	Information and Communication Technology
IFS	Interframe Spacing
ISO	Isochronous Traffic
IP	Internet Protocol
IPTV	Internet Protocol Television
IR	Influential Range
ISM	Industrial, Scientific and Medical
ITU-R	International Telecommunications Union
LAMA	Link Activation Multiple Access
LDS	Low Data Stream Applications
LEACH	Low Energy Adaptive Clustering Hierarchy
LI	Loss Intolerant
LiB	Link Activation based
LIFS	Long IFS
LLC	Logical Link Control
LMAC	Lightweight MAC
LPL	Low Power Listening
Lo	Low traffic
Local	Localized Collision free based
LOD	Low-Rate Data
LoS	Line-of-Sight
LPRA	Loosely Prioritized Random Access
LQI	Link Quality Indication
LR	Low-Rate
LS	Least Square
LSB	Least Significant Bit
LT	Loss Tolerant
LTA	Long-Term Applications
LTE	Long-Term Evolution

M2M	Machine-to-Machine
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
MBAN	Medical Body Area Network
MC-SCP-MAC	Multi Channel Scheduled Channel Polling MAC
McMAC	Multi Channel MAC
MCU	MicroController Unit
MDP	Markov Decision Process
MDS	Medium Data Stream Applications
Me	Medium traffic
MED	Medium-Rate Data
Media	Multimedia
MEMS	Microelectromechanical Systems
MFR	MAC Footer
MHR	MAC Header
MIB	Mote Interface Board
Micro	Micro-Frame
MIM	Message-in-Message
MIMO	Multiple Input Multiple Output
MiXiM	Mixed Simulator
Mob	Mobility adjust
MPDU	MAC Protocol Data Unit
MR	Medium-Rate
MS	Multimedia Streams
MSE	Mean Square Error
MSDU	MAC Service Data Unit
MSB	Most Significant Bit
MS-MAC	Mobility Aware MAC
MSK	Minimum-Shift Keying
MTA	Medium-Term Applications
Multi	Multi-frequency/channel
MWSN	Mobile Wireless Sensor Networks
NaI	Narrow Band Interference
NAMA	Node Activation Multiple Access
NACK	Negative Acknowledgement
NB	Number of Backoffs
Nghb	Neighbour-based
NLoS	Non-Line-of-Sight
NISO	Non-Isochronous traffic
NoB	Node Activation based
NRT	Non-Real Time
NRT-nSDD	Non-Real Time-non Sensitive Delay Demanding Applications
NTC	Negative Temperature Coefficient
NWK	Network
n-Be	Non-Beacon mode
Oh	Reducing Overhearing
OOK	On-Off Keying
OMNeT++	Objective Modular Network Testbed in C++

On	On-demand based
OS	Operating System
Ov	Reducing Overhead
Pack	Packetization
PAMA	Pairwise-Link Activation Multiple Access
PAN	Personal Area Network
PDA	Personal Digital Assistant
PE	Process Estimation
PEDAMACS	Power Efficient and Delay Aware Medium Access Control for Sensor Network
PER	Packet Error Rate
PHR	PHY Header
PHY	Physical
Pigg	Piggybacking Synchronization Information
PLC	Physical Layer Capture
PPDU	PHY Protocol Data Unit
Pre	Pre-defined sets of duty cycles
PrS	Preamble Sampling
pseudo-RNG	Pseudo-Random Number Generator
PS	Protocol Stack
PSDU	Physical Layer Service Data Unit
PSP	Packet Success Probability
PSR	Packet Success Rate
PSSS	Parallel Sequence Spread Spectrum
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
Radio	Wake-up radio
RAM	Random Memory Access
Rang	Range
RBC	Random Backoff Countdown
Rc	Receiver-based
RFD	Reduced-Function Device
RFID	Radio-Frequency Identification
RICER	Receiver Initiated CyclEd Receiver
RL-MAC	Reinforcement Learning based MAC
RN	Repeater Node
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
RT	Real-Time
Rt	Rotative
RT-SDD	Real-Time - Sensitive Delay Demanding Applications
RT-VBR	Real Time-Variable Bit Rate
RX	Reception
Samp	Sampling Duration
Schd	Wake-up schedule
Sched	Schedules Period
SCP-MAC	Scheduled Channel Polling MAC
SD	Superframe Duration

Sensor	Sensor
SER	Symbol Error Rate
SF	Sender First
SFD	Start-of-Frame Delimiter
Sg & Fi	Single CW & Fixed size
Sg & Var	Single CW & Variable size
SHR	Synchronisation Header
SIFS	Short IFS
Single	Single-frequency/channel
SIR	Signal-to-Interference Ratio
SLC	Sender Last, Interferer Clear
Sleep	Sleep Delay
SLG	Sender Last, Interferer Garbled
SMAC	Sensor-MAC
SMS	Short Message Service
SNR	Signal-to-Noise Ratio
SNIR	Signal to Noise-plus-Interference Ratio
SPI	Serial Port Interface
SPX	Simplex
SQL	Structured Query Language
SR	Sampling Rate
St	Static
STA	Short-Term Applications
Stat	Statistical Function
Stag	Staggered based
STEM	Sparse Topology and Energy Management
STEM-B	STEM Beacon
STEM-T	STEM Tone
SWUF	Short Wake-Up Frame
Synch	Synchronization Period
TDMA	Time Division Multiple Access
Tf	Traffic Load
TICER	Transmitted Initiated CyclEd Receiver
ToA	Time of Arrival
ToE	Time of Ending
Tone	Wake-up tone
Tx	Transmission
T-MAC	Timeout-MAC protocol
UBR	Unspecified Bit Rate
ULP	Ultra Low Power
UMPC	Ultra-Mobile PC
Uni	Uniform
USB	Universal Serial Bus
Util	Utilization Function
UWB	Ultra Wideband
Var	Variable
VM	Virtual Machine
VOI	Voice Traffic

WBAN	Wireless Body Area Networks
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WiseMAC	Wireless MAC
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WSAN	Wireless Sensor and Actuator Networks
WUF	Wake-Up Frame
WUS	Wake-Up Signal
WWAN	Wireless Wide Area Network
YANS	Yet Another Network Simulator
ZDO	ZigBee Device Objects
ZDP	ZigBee Device Profile
ZMAC	Zebra MAC
1G	First Generation of WSN
2G	Second Generation of WSN
3G	Third Generation of WSN

List of Symbols

a_i	Time slot
a	Multiplier of the LCG
A_e	Exclusive area of two circles with equal radius
A_i	Slot selection event in CW_1
A_s	Arrangements of the choice of the lowest order slot by exactly one node
$A_t(m)$	Total number of possibilities
$A_s(m)$	Number of possibilities that exactly one node chooses the i -th lowest order slot and the remaining ones choose the subsequent slots
$A_f(m)$	Number of possibilities for the lowest order slot to be chosen by more than one node
A_s	Arrangements for the cases when the lowest order slot is chosen by exactly one node
A_f	Arrangements for the cases of the lowest order slot to be chosen by more than one node
$\widehat{A}_f(m)$	Number of possibilities for the lowest order slot to be chosen by more than one node (unsaturated regime)
$\widehat{A}_t(m)$	Total number of possibilities (unsaturated regime)
c_+	Increment of the LCG
c	Speed of light in vacuum
CW_1	Contention Window 1
CW_2	Contention Window 2
CW_1^{max}	Maximum number of slots in CW_1
CW_2^{max}	Maximum number of slots in CW_2
C_{batt}	Capacity of the battery
C	Capacity of the medium
C_i	Slot selection event in CW_2
d	Distance separation between the transmitter and receiver
d_{fb}	Far-field distance
d_0	Close-in reference distance from near the transmitter antenna
D_{ch}	Slot channel degradation threshold
D	Largest physical linear dimension of the antenna
e_i	Expected theoretical frequency
$E[S]$	Expected number of contending nodes in CW_2
$E[m]$	Nearest integer value of $E[S]$
$\overline{E_{cons\_hg}^{SCP}}$	Upper bound for the energy consumption with piggybacked synchronization
$\overline{E_{cons\_lw}^{SCP}}$	Lower bound for the energy consumption with piggybacked synchronization
$\overline{\overline{E_{cons\_lw}^{SCP}}}$	Lower bound for the energy consumption without piggybacked synchronization
$\overline{\overline{E_{cons\_hg}^{SCP}}}$	Upper bound for the energy consumption without piggybacked synchronization
$\overline{E_{cons}^{SCP}}$	Total energy consumed by the node
$\overline{\overline{E_{multi\_lw}^{SCP}}}$	Lower bound for the energy consumption with piggybacked synchronization in a linear chain topology

$E_{multi\_hg}^{SCP}$	Higher bound consumption with piggybacked synchronization in a linear chain topology
$\frac{E_{listen}^{SCP}}{E_{tx}^{SCP}}$	Energy consumption in node listening process
$\frac{E_{rx}^{SCP}}{E_{poll}^{SCP}}$	Energy consumption in node transmission process
$\frac{E_{sleep}^{SCP}}{\hat{E}[n]}$	Energy consumption in node reception process
	Energy consumption in node polling process
	Energy consumption in node sleeping process
	Expected number of nodes that choose one of the G possible intervals (unsaturated regime)
f_i	Observed number of generation times
f_b	Carrier Frequency
f	Clock skew
F_0	Frame 0
F_1	Frame 1
G	Interval order
G_n	Delivery ratio gains
G_{tx}	Transmitter antenna gains
G_{rx}	Receiver antenna gains
h	Number of hops
H_0	Hypothesis
i_d	Sensor node identifier
i_{dat}	Current to sample sensors
i_{tx}	Current to send a Byte
i_{rx}	Current to receive a Byte
i_{sleep}	Current in sleep mode
ID	Sensor node address
I	Discharge current
I_{tx}	Current in transmitting
I_{rx}	Current in receiving
I_{listen}	Current in listening
I_{poll}	Current in polling
I_{sleep}	Current in sleep
k	Number of the contention window (1 or 2)/index
k^*	Number of trials to deliver packet from PHY to MAC layer
k_{min}^*	Minimum number of trials
l	Subset of nodes
L_{data}	Data packet length
L_{sB}	Piggybacked bytes length
L_{sync}	SYNC packet length
$L_{preamble}$	Length of the frame preamble
L	Side length
LS	System loss factor
m	Number of successful nodes
m_{lcg}	Modulus of the LCG
n_{ngb}	Number of neighbours
n_{hd}	Number of hidden terminals
n	Number of nodes in the network

n_{peuk}	Peukert's exponent
n_{tx}	Total number of nodes per slot
n_{tx_S}	Number of nodes per slot that transmit a data packet and experienced a successfully reception
n_{tx_F}	Number of nodes transmitting a packet involved in a collision
n_{Bits}	Length of the frame
n_{max}	Maximum number of nodes
N	Number of interfering nodes
Nn	Number of time slots
N_{ch}	Available channels
N_d	Total number of different combinations we use the notation
N_c	Probability of the lowest order slot being chosen at least by two nodes
p_i	Probability of choosing a slot i
$P(X_i = l)$	Probability that l nodes choose the slot i
p_n	Probability of at least two of the n people sharing a birthday
$p_{n'}$	Complement of p_n
P_{tx}	Power in transmitting
P_{sleep}	Power in sleeping
P_{rx}	Power in receiving
P_{listen}	Power in listening
P_{poll}	Power in channel polling
P_{node}	Power consumption of the node
P_{c1}	Probability of collision in the CW_1 (saturated condition)
$\widehat{P_{c1}}$	Probability of collision in the CW_1 (unsaturated condition)
P_{Ssuc}	Probability of not choosing the same slot in CW_2
P_{Scol}	Probability of choosing same slot in CW_2
P_{cF}	CW_2 collision probability
$P_{eF}(m)$	Probability of a collision occurring in CW_2 by combinatorics approach
P_{u-G}	Uniformly distributed packet generation probability / probability of a given node to choose one of the G intervals unsaturated
P_{Sidle}	Probability of a slot being idle
P_{sF}	Probability of a successful data packet transmission after i -th transmission
PL	Path loss
$\overline{PL}$	Mean path loss
$\overline{PL}(d_0)$	Reference path loss
P_A	Probability of at least two people in the room having the same birthday
P_{SC}	Probability of nodes choosing the same slot channel
$\widehat{P_{cF}}$	Collision probability in CW_2 (unsaturated regime)
$\widehat{P_{Scol}}$	Probability of choosing same slot in CW_2 (unsaturated regime)
$\widehat{P_{Sidle}}$	Probability of a slot being idle (unsaturated regime)
$\widehat{P_{eF}(m)}$	Probability of a collision occurring in CW_2 by combinatorics approach (unsaturated regime)
Q^2	Chi-square statistic
r_B	Bit rate
r_d	Range
r_{data}	Data packet size
r_{sync}	Sync packet size
r_{dat}	Sensor sampling rate

r	Number of the lowest order slot that is selected by only one node
R_{Flex1}	Flex sensor resistance value
R	Battery hour rating
$RSSI_{F_0}$	RSSI from Frame 0
$RSSI_{F_1}$	RSSI from Frame 1
R_{xval}	Raw value returned by the SHT15 sensor
S_{CW_1}	Set of possible slots in CW_1
S_{CW_2}	Set of possible slots in CW_2
S_{min}	Sensitivity
S_c	Slot channel
t_{wakeup}	node wake-up time
$t_{init_{CS}}$	Time instant to initiate CS
t_{sync}	Time to exchange SYNC packets/ synchronization time
t_{CS}	Duration of the CS
$t_{RX\_SYNC\_pkt}$	Time interval to receive SYNC packets
$t_{init\_CS\_max}$	Maximum time to perform CS
t_{cs1}	Average carrier sense time
t_{p1}	Average time to poll channel
t_{tone}	Duration of the wake-up tone
$t_{to_{ack}}$	Maximum time to receive de ACK packet
t_{node}	Node lifetime
t_{dat}	Time to sample sensors
t_d	Size of data packet (peukert model)
t_{θ_i}	Time instant value for the first data packet generation
$t_{\theta_{max}}$	Maximum time of the interval for the packet generation
t_{start1}	Time instant of first interfering packet
t_{start2}	Time instant of second interfering packet
t_i	Time instants in FC scenarios
t_{tx_sync}	Time instant when the SYNC packet was sent
t_{switch}	Time needed to switch channel
t_F	Duration of the Frame
t_{CS}	Time interval to perform CS
$t_{\varphi}^{CW_1}$	Time instant to initiate the CS
t_{guard}	Time out timer to receive last data packet
t_{sync_max}	Maximum time to disseminate SYNC packet
$t_{simulation}$	Simulation time
T_{subs_slots}	Duration of the remaining time slots
T_{sync}	SYNC packet period
T_p	Channel polling period
T_{poll}	Polling period time
T_{data}	Data packet period
T	Time
T_{tR}	Inter-arrival time value
ToA_i	Time of arrival instant
ToE_i	Time of end instant
$T_{2,n}$	Current time of the child node
$T_{1,n}$	Current time of the parent node (coordinator)
T_n	Total number of possible cases

$\overline{T_{sv}}$	Average MAC service time
T_{min}	Minimum latency time
T_{max}	Maximum latency time
T_x	Average delay per transmission
V_{cc}	Supply voltage
V_{in}	V_{cc} value supplied to the voltage divider
V_{out}	Voltage value output from the voltage divider
V_{drop}	Battery voltage dropping
V_{av}	Average velocity
V_{SO}	Output voltage from RC filter
V_{DD}	Supply voltage for SHT21S
x	X-axis
x_i	Throughput of the node i
X	Geometric random variable
X'_n	Variable of the transmission delays
X_n	Current seed of the LCG
X_{n+1}	LCG generated value
X_i	Random variable
X_σ	Normally distributed random variable with standard deviation σ
y	Y-axis
Y_i	Random variable
α_{exp}	Path loss exponent
α_{add}	Time duration between consecutive Frames
α_{turn}	Turnaround time
α	Level of significance
β	Total number readings performed
Δt	Difference between the arrival times
Δt_{SC}	Time interval in which the parent node switches to each channel
$\Delta \sigma$	CW ₁ time interval
$\Delta \sigma_{max}$	Maximum CW ₁ time interval
$\delta_{preamble}$	Size of the preamble field
δ_{sync}	Size of the sync field
δ_{data}	Size of the data field
δ	Total duration of the packet
δ_1	Delivery reliability 1
δ_2	Delivery reliability 2
δ_{max}	Maximum number of channels
ζ	Retransmissions attempts (collision model)
η_1	Linear fitting constant (IEEE 802.15.6)
η_2	Linear fitting constant (IEEE 802.15.6)
θ_1	Deformation angle of Flex sensor 1
θ_2	Deformation angle of Flex sensor 2
θ	Drift rate
θ_{switch}	Time needed by the sensor node to switch to the chosen channel
$\theta_{PAN\_max\_wait}$	Maximum time that PAN waits to initiate slot channel hopping routine
$\overline{\vartheta_s}$	Achieved throughput
ϑ_{fi}	Throughput fairness index
ι_{ret}	Maximum number of retries

λ	Traffic generation rate
λ_{data}	Data packet rate
λ_{sync}	SYNC packet rate
ν	Ratio between the total number of collision readings
Π_{max}	Highest interval order
Π_{irmax}	IR Sensing range threshold
ρ_{dev}	Maximum allowable deviation time
$\sigma_{current}$	Current time of the node
σ	Standard deviation
ψ	Transmission delay
τ	Probability that a node chooses a given slot i in CW_2
Φ	Asymptotic significance level
γ	Node density
φ_{ch}	Random channel chosen by the sender node
φ_1	Time interval 1 in collision scenario
φ_2	Time interval 2 in collision scenario
φ_3	Time interval 3 in collision scenario
$\varphi_{slot}^{CW_1}$	Time slot choice in CW_1
$\varphi_{slot}^{CW_2}$	Time slot choice in CW_2
φ_{slot}^{SYNC}	Slot choice in SYNC CW
χ^2	Chi-square test
$\psi_{wake-up}$	Next sender node wake-up time
ω	Clock offset
Ω	Monte Carlo significance level

Chapter 1

Motivation and Framework

1.1 Introduction

Although in the past decade there has been a strong research effort on legacy mobile communications and unlicensed wireless systems, several researchers consider that in the next five years, an inversion of the main trends will occur, and the focus will be in interdisciplinary research on Wireless Sensor Networks (WSNs). This interdisciplinary research is stimulating the development of new WSN services and applications to be supported by sensor nodes. Since these sensor networks are starting to take part of our life, more and more applications gradually appear where these smart systems are used. These concepts enable a massive-scale deployment of WSN applied to a wide range of applications and will change the way we interact, live or even work within the surrounding ambient. Nowadays, the need to collect, interpret and act on real-time data gains an increasingly interest. However, to collect data using typical wired sensor networks has always been expensive owing to installation and maintenance costs, and is limited in its range. WSN is a term used to describe an emerging class of embedded communication products that provide redundant, fault-tolerant wireless connections between sensors, actuators and controllers.

WSNs answer the need for nomadicity and mobility in the context of *in situ* event monitoring. The main purpose of this class of networks is to easily and quickly provide access to the information gathered from a set of sensor nodes scattered in an irregular or inaccessible geographical, or even in harsh environments where wired communications are not feasible. Energy efficiency is sought because it increases the lifetime of the network, where nodes are usually battery powered.

Typically a WSN is formed by groups of several sensor nodes, the so-called motes, whose individual constitution is based on actually combining sensor radios and CPUs into an effective robust secure and flexible network, with low power consumption, and advanced communication and computation capabilities, one or more sensors, a communication device (typically a radio), a microcontroller (with memory), and a power supply (battery).

Beyond the hardware description of the sensor node, different protocols are embedded in the sensor node that operate at different layers of the network protocol stack, with the goal of efficient management of his operation modes, dynamic network adaptivity, robust and reliable communications among sensor nodes, while extending the lifetime of the whole WSN.

Due to these capabilities jointly with large scale deployment and low unit cost per sensor node, WSNs offer to researchers great potential of appliance in a wide range of areas. The latter characteristic results undoubtedly in simple architectures, limited processing capabilities and low memory storage capacity in the sensor nodes. Taking into account these constraints in the design of WSNs applications poses significant challenges to overcome these hardware limitations. These systems are spread onto environment and workplaces, facilitating to sense a large variety of phenomena, such as the monitoring of the occurrence of forest fires, enabling rapid emergency response when needed, tracking pedestrian or vehicular traffic in a metropolitan context, structural monitoring and military systems. While these technological advances

takeover, new challenges emerge for information processing in sensor networks. The needs in this framework are novel computational representations, algorithms, protocols, design methodologies and tools which allow for supporting distributed signal processing, information storage and management, networking, and the development of sensor applications.

A WSN is typically a mission-driven services provider, which efficiently delivers services subject to the required Quality-of-Service (QoS), physical and link layer constraints. Since WSNs are service providers they can be modelled at different levels of abstraction, while for each level a set of services and metrics are defined.

Even though there have been a staggering evolution of the hardware and protocols applied in sensor nodes of WSNs, one of the major bottlenecks of the wireless sensor devices performance is the energy limitation faced by the sensor nodes and energy storage. Most of the times, sensor nodes are powered up with batteries and only recently were added energy scavenging capabilities to the sensor nodes. The problem of maintaining these type of networks fully operational without sacrificing the overall performance and delivery of data of the WSN while taking into account the limited energy resource available is a hot topic and the milestone/objective of every researcher in WSNs design. The limited power supply could lead to severe problems of the WSN, namely communication failures, coverage limitations, or even unconnected nodes. The different protocols that operate at different layer of the protocol stack from the sensor node try to guarantee the maintenance of the a energy efficiency of the sensor node. Despite the efforts of the different layer protocols to maintain this efficiency there is always some type of energy waste. Major sources of energy waste are idle listening, packet retransmissions (due to packets collisions), unnecessarily used transmission power, sub-optimal utilization of the available resource, overhearing and control overhead [Sic04, YHE04, BDWL10].

Therefore, these resource limitations impose special challenges that are overcome through design of protocols that guarantee the most efficient use of the energy available while tackling the energy problem in a distributed form. The strict collaboration among sensor nodes allows for overcoming these challenges.

As stated by the authors from [ISH10], the development of applications involving WSNs raise concerns about the hardware capacity, deployment area, type of energy sources available, deployment cost, ambient conditions, energy harvesting possibility, among other issues. Therefore, it is of paramount importance to evaluate the application algorithm (Medium Access Control (MAC), routing, etc) before deploying them into real world. To test the performance of these algorithms and protocols there are some WSN evaluation tools and methodologies, namely analytical modelling, simulation, emulation, testbeds and real deployment. However, in terms of cost-efficiency, simulators, emulators and testbeds are the most effective tools that can be used to evaluate the performance of algorithms and protocols during the design, implementation and development processes.

1.2 Motivation and approach

Nowadays, the user of WSNs is becoming more and more demanding in terms of choice and diversity of applications. As a consequence, as the diversity of applications continues to grow there is a need to identify and classify the set of characterization parameters. These characterization parameters should allow for understanding the differences or similarities, advantages or disadvantages of different WSN applications, facilitating the WSNs applications designer to have a complete insight about the possible application requirements or possible outcomes from

a specific WSN application area.

In fact, the information available in the literature about WSN's application classification is very generalist and does not completely describe specific WSN applications. Nowadays, there is therefore a lack of a taxonomy which gathers several characterization parameters to exhaustively characterize and classify a WSN application. For these reasons, one of the main contributions from this PhD thesis, is a taxonomy for the characterization and classification of WSN applications. This taxonomy fills the gap in the WSN literature by describing the classification and characterization parameters (criteria), and that can be used by other researchers or WSN's applications designers as a tool to better understand the services and requirements of each application. It is centred on the different sets of parameters that have a high impact on a given future WSN application. Furthermore, typical values from related research works are considered as a reference, but in this taxonomy it is proposed inter- and intra-connections among the considered application groups. Based on these connections, new characterization parameters have been added and new application groups have been proposed along with a holistic overview of the WSN application taxonomy performed. To complete the WSN application taxonomy, a chronological comparison is also presented for the projects in all the highlighted areas, along with the evolution path towards new WSN areas and future trends.

Aiming to bridge the frequent gap between theory and practice, three real WSN applications and scenarios are considered and implemented, namely for the health, structure monitoring and precision agriculture areas. This PhD project proposes instrumentation and sensor data dissemination solutions for the foetal movement monitoring, concrete structure integrity monitoring monitoring in the Smart-Clothing and INSYSM projects.

These scenarios are useful to perceive which are the differences/similarities between the theoretical and real requirements of a specific WSN application. Furthermore, these real-world implementations of WSNs were useful to evaluate and observe how the energy efficiency/consumption behaves when considering simple layer protocols in the sensor nodes. Energy efficiency is of paramount importance since it is directly related with the lifetime of the network formed by mostly battery-powered nodes. As soon as the scalability in these WSN applications increases the energy efficiency decreases drastically, due to idle listening, packets collisions, overhearing and control overhead. These sources of energy wastage are already identified in several works in WSN's literature, in which the MAC protocol is a very important component in the normal operation of the sensor node. This protocol is in charge of trying to cope/mitigate or even solve these sources of energy wastage in WSNs. Solving or mitigating these sources of energy wastage naturally leads to an increase of energy efficiency while ensuring a high performance of the network as well as the increase of the network lifetime.

Aiming to fulfil the objective of achieving a better energy efficiency of the WSN we came up with the proposal of an innovative MAC protocol, which explores advanced physical layer and multi-channel techniques (e.g., frame capture). To achieve this goal, different MAC protocols have been analyzed to evaluate the most promising techniques and protocols that are worthwhile to be considered in the design of the new MAC protocol. Based on a taxonomy for the classification of the MAC protocols into different categories, each MAC protocol is characterized not only by the technique employed to access the channel but also considering that one MAC protocol may utilize multiple techniques. Hence, this taxonomy extends the usual classification of WSN MAC protocols for new ones that consider multiple techniques to diminish energy wastage. This analysis identifies that one of the MAC protocols which can be considered as a solid basis for the future development of our own MAC protocol is Scheduled Channel Polling (SCP-MAC). OMNeT++ event driven simulations enable to verify the potential improvements that

may be applied in our new MAC, namely by analyzing the following aspects:

- The impact of piggyback techniques for periodic heavy and light traffic loads in single-hop topology in power and energy consumption performance;
- Throughput performance under periodic heavy and light traffic loads in a single-hop topology;
- Node energy consumption and latency considering a linear node chain and multi-hop scenarios;
- Lifetime analysis while considering piggyback techniques.

The need to explore the behaviour of the associated collision probabilities for the applied two-phase contention window mechanism is identified by implementing and evaluating the performance of the SCP-MAC protocol. This motivates the proposal of a model for the collision probabilities, in which the impact of the consecutive contention windows sizes and number of contending nodes is evaluated whilst considering saturated and unsaturated traffic conditions. The identified stochastic model for the collision probabilities is applied and simple models are proposed for the average MAC service time and achievable throughput. These models can be considered to obtain accurate insights on how and when collisions between nodes occur in a two-phase collision avoidance mechanism and be applied in the routing layer from a real testbed. The model's output can be considered to decide whether to transmit a packet, depending on the number of neighbour nodes.

Another challenge is to analytically compare the benefits/ shortcomings or advantages/ disadvantages of using one or two contention windows in slotted contention based MAC protocols. This objective is demonstrated by a model that is verified by means of simulation.

Improvements in the Physical (PHY) layer include i) the replacement of the algorithm to decide whether a packet is accepted or not by a decision algorithm that ensures the packet delivery to the MAC layer with a certain reliability and ii) the addition of the recently studied frame capture effect capabilities [FXHZ10].

This part of the research leads to the proposal of the Multi Channel Scheduled Channel Polling MAC (MC-SCP-MAC) protocol. This new MAC protocol explores the advantages of multi-channel features in addition to the capture effect present in the recent radio transceivers, the Influential Range (IR) concept (to mitigate the energy losses due to overhearing) and cognitive-based capabilities, such as the channel degradation sensing jointly with opportunistic channel selection. A simulation approach is considered, where different aspects are addressed, namely:

- energy consumption evaluation and comparison (between single and multi-hop topologies) while different traffic generators are considered;
- evaluation of the expected benefits in terms of packet collision ratio from a multi-channel based protocol with a two-phase contention window mechanism;
- analysis of the impact of contention windows sizes while varying the number of channels for different traffic profiles (periodic and Poisson);
- analysis of the impact of the number of channels considered in the energy consumption, delay and aggregate throughput;
- analysis of the impact in the energy consumption, delivery rate and aggregate throughput while varying the sensor nodes density (dense and sparse scenarios);

- analysis of the impact of enabling the IR concept in the MC-SCP-MAC protocol in energy consumption, delay and delivery rate;
- comparison of the performance results for the considered influential range thresholds (for the definition of optimal values);
- energy efficiency evaluation for the scenarios that consider a cluster-based topology;
- evaluation and analysis of the short and long term throughput fairness index;
- comparison and analysis of the energy consumption, delivery rate and aggregate throughput for different network sizes while enabling the frame capture capabilities for different values of the reliability;
- evaluation of the benefits of enabling cognitive-based capabilities.

1.3 Main Objectives

The main goals of this thesis are the following:

- To conduct a study of the state-of-the-art of WSNs applications covering a wide variety of application areas;
- To propose a complete characterization and classification taxonomy of WSN applications, as a mean of providing (to other researchers or WSN applications designers) a tool to better understand the services and requirements of each application;
- To address instrumentation and sensor data dissemination solutions/strategies for real-world WSN applications, mainly in the healthcare, civil engineering and precision agriculture areas;
- To propose a model for the collision probability along with models for the average service time and throughput in a collision avoidance mechanism with two contention windows;
- To validate the proposed models through simulation;
- To propose and implement a decision algorithm, the Enhanced Reliability Decision Algorithm, in the IEEE 802.15.4 compliant physical layer that ensures the delivery of packets to the MAC layer with a certain reliability, as well as the frame capture effect;
- To propose the Multi-Channel Scheduled Channel Polling (MC-SCP-MAC) MAC protocol, which allows for increasing energy efficiency and delivery rate in denser WSNs scenarios with the possibility of supporting the cluster scenario along with cognitive based capabilities;
- To verify the MC-SCP-MAC protocol by means of simulation;
- To disseminate the work developed, through the publication of papers in national and international conferences and journals, and through the publication of a book chapter.

1.4 Contributions

The work presented in this thesis is a significant part of different research European frameworks, such as in the INSYSM Marie Curie IAPP [INS11] and co-operation in the field of Scientific and Technical Cooperation (COST) namely COST2100 [COS06], COST IC1004 [COS11] and COST IC0905 “TERRA” [COS10]. Also some contributions on sensors and MAC layer protocols addressed throughout this thesis have been developed in the framework of the Smart-Clothing [Sma09] and PROENERGY-WSN (PTDC/EEA-TEL/122681/2010) portuguese projects [PRO12]. The participation on these projects suits the purpose of the research for this thesis and the feedback obtained from the experience of sharing knowledge and discussing the developed work with other international researchers or partners has been very rewarding. Some aspects in this thesis have been improved based on the suggestions arising from discussions during some COST2100 meeting. The work from the participation in the aforementioned projects was already disseminated in papers published, accepted for publication or submitted to different conferences, book chapters and journals:

- As a starting point for the research of this thesis a simple real-world application of WSNs to agriculture monitoring was proposed. This research work was published in conferences [BCL07c, BCL07b, BCVL07, BCL07a]. In addition, surveys on WSN applications were also published in conferences with João M. Ferro, a Ph.D. student from our team, [FBVL09, FBVL07a];
- The study of several WSNs applications and scenarios drove the need to understand what is a service in the context of WSNs, as well as what is the definition of application. After establishing these concepts the best way to describe and differentiate the different types of services and applications in WSNs, we identified that different sets of characterization parameters are needed in order to taxonomize the services and applications of WSNs in different classes. The research on characterization parameters that allowed to group and differentiate the different types of applications were published in conferences [BVL08b, BVL09, BVL08a]. Based on these characterization parameters and classes, a taxonomy was build up for WSNs, facilitating to understand which type of applications belong to a certain group with specific characteristics. In addition, a holistic overview of the relations between different groups of characterization, with the same value (or range of values) for a certain set of parameters, is identified and proposed. This work was addressed in [BVL12] a paper to be REVISED and RESUBMITTED to the IEEE Surveys and Tutorials Journal;
- Research work was also performed on instrumentation and sensor data dissemination solutions for real-world WSN applications in the Smart-Clothing and INSYSM projects. The different sensors, and sensor data acquisition and dissemination solutions have been proposed and tested, in order to deliver the sensor data to the user.
 - The main objective of the Smart Clothing for Health Monitoring and Sport Applications (Smart-Clothing) project [Sma09] was to develop easy to wear telemedicine gear that allow for remotely monitoring pregnant women, and count the foetus movements. The participation in this project resulted into the publication of a book chapter [BAL⁺10], several conference papers [BAL⁺08, BBVL09, BLA⁺09], and technical reports [Bor08a, BBVL08, Bor08d, Bor08b, Bor08c];

- Our contribution to the Intelligent Systems for Structures Strengthening and Monitoring (INSYSM) project [INS11] intends to evaluate and assess different parameters inside concrete blocks during the drying (curing) of the concrete, such as moisture, temperature and CO₂. The research of the impact of different sensors embedded in the concrete structure along with different dissemination solutions (wireless and standalone solutions) with Norberto Barroca, another Ph.D. student from our team, and resulted in a technical report in [BBV⁺11] and a paper is accepted for publication with *Major Revisions* [BBV⁺12];
- The criteria considered to choose this simulation tools were analyzed, jointly with João M. Ferro and Norberto Barroca, in a technical report [FBB08];
- The implementation and validation of the Scheduled Channel Polling MAC protocol from [YSH06] in terms of performance metrics (energy, throughput, latency, etc) in the Objective Modular Network Testbed in C++ (OMNeT++) simulator with the Mixed Simulator (MiXiM) framework are published in [BVL11]. In addition, performance evaluation tests for the SMAC protocol [YHE04] have also been performed with Norberto Barroca considering the same simulation tools, which was addressed in [BVF⁺10];
- Cognitive radio aspects in the scope of Medical Body Area Networks (MBANs) have been addressed together with colleagues from COST IC0905 “TERRA” [COS10] in [CSNH⁺12]. Viable architectures solutions of MBANs, with practical Cognitive Radio (CR) features based on the Ultra Wideband (UWB) radio technology are considered. Physical and MAC layer aspects also discussed, in addition to implementation aspects and challenges;
- The packet collision probability in the collision avoidance mechanism with two contention windows in the SCP-MAC protocol was also addressed. A suitable stochastic model for this collision probability for saturated and unsaturated traffic conditions was proposed and evaluated. Using this analytical model, performance metrics such as network throughput and average service time for the successful transmissions have also been derived. This work was addressed in [BVLW12] a paper submitted to the Computer Networks Journal;

Also, contributions were given within the context of regular scientific meetings of the COST Action 2100 (COST2100), as follows:

- A survey on applications of wireless sensor networks, [FBVL07b];
- A taxonomy for the classification and characterization of wireless sensor networks services and applications, [BVL08a];
- A SMAC protocol modelling and simulation for Wireless Body Area Networks (WBAN), [BVFB10];
- The SCP-MAC protocol implementation in the Mobility Framework and the supported modes of simulation considered for this MAC protocol, [BVL10].

1.5 Structure of the Thesis

This thesis is organized into nine Chapters, including this one, and ten Appendices.

The following Chapter presents a survey on the characterization and classification of wireless sensor networks applications. This taxonomy is accomplished via an application-oriented approach in which characterization parameters are divided into different categories (i.e., service,

traffic, communication, service parameters, network, node, and operation environments). A set of characterization parameters is defined for each group of characteristics. A summary of the taxonomy for the characterization parameters is addressed, while thoroughly exploring the different parameters that allow for classifying the WSN applications from each field. A taxonomy is proposed for the classification of WSN applications, where different characterization applications are grouped into sets of applications, depending on the field of application. A holistic overview of the WSN application taxonomy is also given and new WSN applications categories are proposed, in which possible links that may exist between different applications are identified. Finally, a roadmap for WSN applications is proposed and future trends are discussed for all the highlighted WSN areas, from relevant research projects.

Chapter 3 presents the instrumentation and sensor data dissemination solutions proposed and tested in real WSN applications and scenarios. It is divided into three main Sections. Section 3.1 addresses the challenges and experimental apparatus considered for the acquisition and dissemination of the foetal movement in the Smart-Clothing project. Non-invasive sensing techniques have been considered. Then, the different types of sensing belts (based on flex sensors or conductive fabrics) for the pregnant woman that were developed are presented and ends with a discussion about the results obtained. Other solutions considered for sensor data storage and transmission purposes in the project are tackled in this part. In turn, Sections 3.2 and 3.3 address other engineering applications, namely the ones from the INSYSM and precision agriculture [BCL07b] projects. INSYSM addresses instrumentation and acquisition solutions for monitoring the moisture and temperature inside concrete blocks. The objective is to study and assess the state of the concrete structure integrity. Finally, a brief description of the precision agriculture project is analyzed along with the proposed solutions for this outdoor open-field environment.

Chapter 4 is divided into nine Sections that cover the different aspects of the layers in the WSNs protocol stack. The Section 4.1 presents the protocol stack for WSNs as well as the different layers that compose it. Section 4.2 briefly discusses the protocol stack commonly assumed for WSNs while presenting a comparison with other protocol stack models. Section 4.3 describes some basic wireless radio families systems, as well as the evolution of the IEEE 802 standards until the appearing of the IEEE 802.15.4 standard. Section 4.4 briefly discusses the relationship between the IEEE 802.15.4 and ZigBee standards. Section 4.5 presents an overview of the IEEE 802.15.4 standard compliant PHY layer, followed by the Section 4.6, which is dedicated to the MAC layer and its different tasks. Section 4.7 presents the state of the art on MAC protocols for WSNs and proposes a taxonomy for MAC protocols (extra details are given in Section G.3 from Appendix G). MAC protocols are classified into different categories, which depend on the technique employed to access the channel, whilst considering that one MAC protocol may utilize multiple techniques. In Section 4.8, a summary of the MAC characteristics is presented in order to classify and taxonomize the state of the art on MAC protocols for WSNs. Finally, in Section 4.9 conclusions are drawn. Complete details on the IEEE 802.15.4 standard PHY layer are addressed in Appendix F. The MAC protocols comparison tables for the proposed taxonomy are presented in Appendix G. Based on the study performed in the last chapter about the MAC protocols one of them is noteworthy to be more carefully analyzed and elected to be considered in the proposal and design of a new MAC protocol. Chapter 5 therefore describes the Scheduled Channel Polling-MAC protocol [YSH06] in detail, the protocol considered for further research. The motivation to use the SCP-MAC protocol is referred and the various SCP procedures, such as the two-phase contention window mechanism, synchronization phase description are described. A state transition diagram is proposed for the SCP-MAC protocol. This chapter also tackles

the implementation of the SCP in the simulation framework, by discussing the SCP simulator parameters and general definitions.

Chapter 6 presents the SCP protocol implementation in a simulator and its performance evaluation. The chapter starts by showing the simulation results for the performance metrics (e.g., energy consumption, throughput) for single and multi-hop topologies. Heavy and periodic traffic patterns are considered. A lifetime analysis (enabling piggyback synchronization) for the SCP protocol is proposed in this chapter by considering a simple battery discharge model, given by Peukert's equation [JH09]. The remaining of this chapter, addresses one of the novel and major contributions of this work: the proposal of a stochastic model for the collision probability of the SCP protocol (which employs a collision avoidance mechanism with two contention window, one window for a short wake-up tone and the second for data). The saturated and unsaturated regimes are considered. Very promising results are obtained. It is shown that the proposed models can be used to obtain accurate insights into how and when collisions between nodes occur in a two-phase collision avoidance mechanism. Finally, the collision probability model is applied to derive the average MAC service time for a successful transmission, as well as the achieved throughput in the same collision avoidance scheme.

Chapter 7 is an important contribution from this PhD research. The contributions are twofold. Firstly, a new physical layer packet reception decision algorithm is proposed based on a reliability concept. Secondly, the implementation of the frame capture effect feature in the IEEE 802.15.4 compliant physical layer in the MiXiM simulation framework is addressed. After defining the frame capture concept, along with the main reasons to occur as well as its work principles, different frame capture scenarios (corresponding to different frame overlapping situations) are presented. The potential impact of the frame capture effect on MAC protocols is addressed. A description of how the frame capture is implemented in the MiXiM simulation framework is also given. Other novelty from this chapter is the proposal of a formulation based on a reliability concept. The SNIR and the size of the packet are considered in order to guarantee the delivery of a packet received by the PHY layer to the MAC layer with a certain reliability. Finally, the proposed enhanced decider with the frame effect capture and the default decider algorithm are compared.

In Chapter 8, a new MAC protocol based on the SCP-MAC protocol that envisages multi-channel features is proposed. This protocol is refereed as the MC-SCP-MAC protocol. In particular, this chapter describes the new protocol phases, namely the startup, synchronization, discovery and addition to the network ones, medium access control algorithm, packets structure, as well as energy optimization techniques. These techniques comprise the influential range concept and some specific cognitive-based capabilities. The study of the impact of the frame capture effect in the proposed protocol is discussed, as well as the advantages of the extra resolution phase algorithm, useful to mitigate packet losses. Finally, different performance metrics (energy consumption, delay, aggregate throughput, delivery rate and throughput fairness index) are evaluated whilst comparing MC-SCP-MAC with the MC-LMAC, SCP-MAC, CSMA and MMSN protocols, followed by a discussion about the achieved results. Enhancements to be implemented in MC-SCP-MAC are also discussed.

Finally, Chapter 9 presents the conclusions, some final considerations and suggestions for further research. Further detailed information can be found in Appendices. Appendix A discusses the choice of the simulation platform considered throughout this thesis. Appendix B presents the remaining tables for the classification of WSN applications and the characterization parameters considered for the proposed taxonomy in Chapter 2. Appendix C gives a description of other applied solutions in the Smart-Clothing project while Appendix D gives an overview of

the INSYSM project. Appendix E presents the considered radio frequency propagation model (i.e., IEEE 802.15.4 standard indoor and outdoor propagation model), implemented in the simulation framework. Appendix F gives an overview of the IEEE 802.15.4 standard physical layer. Some considerations and specifications about country regulations, frequency bands, data rates, device types and other PHY layer details are discussed. Appendix G presents and describes the IEEE 802.15.4 MAC layer in detail. It includes the superframe structure, interframe spacing, IEEE 802.15.4 MAC frames as well as the remaining MAC protocols considered for the MAC protocol taxonomy and the MAC protocols comparison tables. Appendix H describes how the *Birthday paradox* problem can be applied to solve the collision probabilities in wireless systems. In Appendix I the procedure for the computation of the CW_1 and CW_2 collision probabilities is presented. Appendix J, presents extra results for the MC-SCP-MAC protocol performance evaluation.

Chapter 2

Taxonomies for the Characterization and Classification of WSNs Services and Applications

As the diversity of WSN applications is increasing, there is a need to identify and classify the set of characterization parameters that allows sketching up a taxonomy for WSN applications. This taxonomy is accomplished via an application-oriented approach, identifying the services offered by each application. In this chapter, we fill this gap in the WSN literature by describing the classification taxonomy and characterization parameters. The objective of this chapter attempts to organize a huge amount of information about the entire spectrum of wireless sensor networks. The chapter is organized into three parts. The first part (Section 2.1 to 2.3) introduces the different characterization parameters for WSN applications from each field. This taxonomy is accomplished via an application-oriented approach in which characterization parameters are divided into different categories (i.e., main, traffic, communication, service components, network, node, and operation environments) and where a set of parameters is defined for each group of characteristics. The second part (Section 2.4) addresses a possible taxonomy for the classification of WSN applications, where different applications are grouped into sets of applications, depending on the field of application. A holistic overview of the WSN application taxonomy is also given and new WSN applications categories are proposed, in which possible links that may exist between different applications in this taxonomy are identified. The third part (Section 2.5) presents a WSN applications roadmap and future trends for all the highlighted WSN areas from relevant projects considered for this taxonomy. Conclusions are finally drawn in Section 2.6. Appendix B addresses complete details on the applications areas description for Category 1 and 2 WSNs, as well as the remaining details for the WSN applications taxonomy.

2.1 State-of-the-Art and Motivation

The WSN literature of today offers two types of approaches to analyse and classify the MAC protocols. On the one hand, the traditional Medium Access Control (MAC) protocols classification is done according to the general medium access technique being used, whilst emphasizing their advantages and disadvantages whenever possible. In [YBO09], the specific requirements and design tradeoffs of a typical wireless sensor MAC protocol are discussed. On the other hand, in contrast to traditional surveys, the authors from [BDWL10] provide a classification organized according to the problems dealt by the MAC protocols. These authors address the main focus of the considered MAC protocols, design guidelines, as well as their disadvantages and weaknesses. A more recent survey [HXS⁺12] addresses the evolution of WSN MAC protocols, by surveying papers over the period 2002-2011. The protocols are evaluated in terms of energy efficiency, data delivery performance, and required overhead to maintain protocol's mechanisms. More specific works about the asynchronous WSN MAC protocols are discussed in the survey from the authors of [MDN12], which identifies and studies different aspects of MAC protocols for WSNs. These issues comprise the delay efficiency and their latency. In addition, the authors from this work divide these MAC protocols into six categories.

The most recent surveys on routing protocols available on the literature, such as the one from [SSS10], present a classification of the protocols based on an approach similar to the one from traditional MAC protocols surveys. Their study on the state-of-the-art of routing protocols includes a description of the network characteristics, design objectives and routing issues. These main groups are sub-divided into eight sub-groups: location information, network layering and in-network processing, data centrality, path redundancy, network dynamics, QoS aspects, and network heterogeneity. These classification criteria are summarized into a table where energy efficient routing protocols are compared whilst discussing their strengths and limitations [SSS10]. Other works, such as the one from the authors of [WMRD11], present the evolution of WSN routing protocols in a different perspective. It adds further information regarding the attempt to perform standardization through the Internet Engineering Task Force (IETF) Mobile Ad-hoc Networks (MANET) working group. Different from traditional surveys, this survey presents a chronological organization within the given protocol taxonomy. In each protocol family the authors provide a didactic presentation to the basic concept, a discussion on the enhancements and variants on that concept, and a detailed description of the latest state-of-the-art protocols on such family. Other works go beyond the classification of routing protocols based on the network type and protocol operation and address the security aspects in routing protocols [SPA10], a hot topic in WSNs research. Although the majority of the routing protocols in WSNs have not been designed by considering security requirements, there are important applications that need to be secure (e.g., healthcare, military, personal data). Hence, security requirements need to be introduced to ensure an appropriate data protection level. These protocols aim in securing the multipath routing procedure and are classified into categories, based on the purpose of their adopted security and on the implementation approach. To understand the imminent risks that may arise from the lack of security in certain applications, the reasons that drive the need for security in routing protocols are addressed in [SPA10].

A well-documented survey on security protocols in mission-critical WSN applications was written by the authors from [CMYP09]. This work starts by identifying the threats and vulnerabilities that may affect WSNs, as well as the defence methods applied within the network layer. Their security protocols classification is based on the division of the security issues into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. Moreover, the advantages and disadvantages, as well as countermeasures and design considerations for the security protocols issues, are addressed for the current secure schemes in each category.

Security protocols for static sensor networks represent a large extent of existing works in the literature. There are specific security protocols for Mobile Wireless Sensor Networks (MWSN). A state-of-the-art survey concerning the security aspects in MWSN is given in [ROLG11]. The security requirements taxonomy for MWSN is based on forward secrecy, backward secrecy, data survival, authentication, access control, access privacy, data source location privacy, sink location privacy, key management, intrusion detection and intrusion resilience.

Most of the references on WSNs describe networks whose nodes are static and cannot be replaced when they “die” (due to battery depletion). In a static nodes scenario, the nodes closer to the sink node “die” sooner than the far away nodes. This leads to a disconnection of the sinks from the rest of the network. Mobility based protocols have been developed to mitigate the early energy depletion problem due to the limitations from considering static node scenarios. To give an overview of the available mobility protocols for WSNs, reference [BCP08] delves into the various ways the sensor nodes, some mobile relays or sinks, can become mobile for improving network performance. The mobility protocols are classified based on their pros and

cons, as well as the costs and tradeoffs that result from the use of mobile sensors, mobile relays and moving sinks. Moreover, this work describes two approaches for the mobility: controlled and uncontrolled mobility. Both approaches are compared for networks that use single and multi-hop routing protocols. In the latter cases, packets are routed to a passing relay, or for the case where the sink node is the one that moves through the network (to collect the packets delivered to it, in the context of multi-hop).

Previous milestone surveys have focused on the importance of the different protocols that co-exist in the protocol stack of a sensor node and the interconnection that exist between the different layer protocols, with the goal of achieving a high energy efficiency along with high performance metrics. One characteristic that is commonly addressed in all the surveys is the dependence of the different protocols on the type of application they are going to be applied to. The disperse nature of the WSN applications in the WSNs literature brings additional issues to the attempt of classifying or distinguishing WSN applications according to their main characteristics. Some of these works are surveys about the WSN applications, where applications are classified according to the design space, deployment, mobility, resources, cost, energy, heterogeneity, size, lifetime and QoS [GHIGGHPD07]. Besides these application classifications the survey also compares the technologies and standards employed in WSNs.

Surveys concerning application layer issues [GHIGGHPD07], [KHH05b] are reasonably limited. A comparison of the advantages and disadvantages of the technologies applied in each of the presented applications is addressed in [KHH05b]. The technologies are categorized by the communication mechanism, scalability to large WSNs, fault tolerance, as well as the requirements that must be met before the technology can be used.

2.2 WSN Services and Applications

2.2.1 WSN services

WSNs are mission-driven service providers which efficiently deliver services subject to the required QoS, as well as physical and link layer constraints. As service providers, WSNs can be modelled at different levels of abstraction. For each level, a set of services and a set of metrics are defined. Hence, a service can be defined as a unit of operation upon which the various WSN components are established. A service can be informally defined as an abstraction that encapsulates “an organizational unit” [GEWD05]. The type of service depends on the organizational unit that is encapsulated and on the functionality exposed by the interface. WSNs are typically mission-oriented. It is the mission that guides all the functionality of the sensor network, while sensors collectively deliver services to accomplish the network’s mission, based on their sensing, computing, storage, communication, and energy capabilities as well as on the data that they collect and process.

2.2.2 WSN applications

A WSN application can be defined as the task designed for the sensor network. These devices could tightly either interact with the human user or interact with the surrounding environment where the network is embedded into. The nodes from these networks are equipped with sensing and actuation, to measure/influence the environment.

On the one hand, the application itself can consist of several components integrated (at various places) into the Protocol Stack (PS) without considering a service interface [KW05], as shown

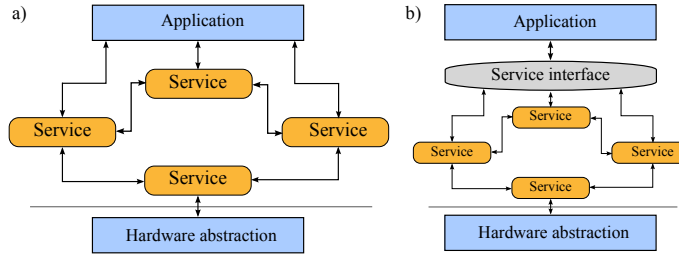


Figure 2.1: Application interface with the protocol stack in the: a) absence or b) presence of a general service interface.

in Figure 2.1 a). The absence of this service interface provides an integrated programming environment, and gives the application designer a very fine-grained control over which protocols (which components) are chosen for a specific task. However, the permission given to the application designer to modify the protocol stack and operating system internals is not prudent. On the other, the presence of a service interface raises the level of abstraction for the interaction between the application and the WSN [KW05], as shown in Figure 2.1 b). Instead of specifying which value to read from which particular sensor, it might be desirable to provide an application with the possibility to express sensing tasks in terms of the application semantics. It is actually possible to face the service interface as a middleware, since it only gives easy access to certain components in a standardized way. Conceptually, WSN services are located between the application and the hardware, and each application is characterized by a set of characterization parameters.

2.3 Taxonomy for the Characterization Parameters

Nowadays, many applications are being created. However, in this survey we only cover a set of meaningful WSN applications from the ones that exist in the literature. By identifying different types of characterization parameters, the proposed taxonomy distinguishes between the functional and technical requirements for the classification of WSN services and applications, as shown in Table 2.1. Depending on the values of the different parameters that identify/characterize WSN applications, these characterization parameters can be organized into seven groups: service, traffic, communication, service components, network, node, and operation environment(s) [FV05, VC02].

The node characteristics is a set of parameters that help to distinguish the type of nodes and the characteristics that the nodes present in a specific WSN application. A set of characterization parameters is defined for each WSN application that covers essentially the node hardware description, as well as the sampling rate of the external sensors that are attached to the node. Finally, the operation environment characteristics define the context in which the WSN applications are deployed. This group of parameters is sub-divided into three sub-groups: i) WSN scenarios, ii) WSN framework, and iii) deployment scenarios. The first sub-group distinguishes between the single-hop, multi-hop, and mobility scenarios. From the basics of radio communication and the inherent power constraints, radio communications are limited by the feasible distance between the sender and receiver. Note that the simple direct communication (single-hop), between source and sink is not always possible owing to the result in coverage difficulties. The second sub-group is the operation framework: i) public or ii) private. The third one (deployment scenarios) is going to be further described to provide an overview of the environments for WSN applications deployment.

Table 2.1: Characterization parameters for WSN applications.

Categories	Characterization Parameters
Service	Delivery requirements
	Directionality
	Communication symmetry
	End-to-end behaviour
	Interactivity
	Delay tolerance
	Criticality
Traffic	QoS
	Bit rate
	Latency/delay
Communication	Synchronization
	Class of service
	Modulation
	Communication direction
Service components	Type of traffic
	Packet delivery failure ratio
	Data acquisition & dissemination
Network	Lifetime
	Scalability
	Density
	Sensing range
	Self-organization
	Security
	Addressing
	Programmability
	Maintainability
	Homogeneity
	Mobility Support
Node	Microprocessor
	Radio transceiver
	Overall energy consumption
	Sampling rate
	Type of function
	Communication range
	Power supply
Operation environment	Sensor network scenarios -Single hop versus multi-hop -Multiple hop sinks and sources -Mobility scenario
	Framework -Public: Urban, Road, Rural, Commercial -Private: Emergency dedicated
	Deployment scenarios -Offices, Industry, Home, Military, Civil, Metropolitan

2.3.1 Service Parameters

Table 2.1 presents the service parameters for WSN applications. The **service** characterization parameters include the delivery requirements of the WSN applications, how the communications

are established among WSN nodes, how the application reacts or behaves to different packet priorities, the quantity of packets in the data stream in both directions, and the way the application reacts to simple interaction between nodes.

In terms of delivery requirements, a WSN application is either in Real-Time (RT) or Non-Real-Time (NRT) [KW05]. On the one hand, RT packets are transmitted as soon as possible, with no waiting in the queue [PCKC05], as they are sensitive to the aggregation latency. On the other, NRT packets wait in the queue until the number of accumulated packets is equal to the maximum aggregation limit. So, RT applications may provide a quick result but at higher energy costs, e.g., by forcing nodes to wake up earlier than they would wake up anyway, or, alternatively, provide it slowly but at reduced energy cost.

WSNs communications can be unidirectional or bi-directional. Unidirectional applications can only send data from the sensor nodes to the sink node. However, a bi-directional communication is more efficient and allows for the sensor nodes to send data to the sink node, while receiving control data from the sink node (e.g., topology change, schedule information, slot allocation and routing paths).

Bi-directional communications can be either symmetric or asymmetric. In symmetric links the data rate or volume is the same in both directions, averaged over time. In asymmetric links the data rate or volume averaged over time differs in the two communication directions.

WSNs may require to fulfil end-to-end or non-end-to-end performance. The end-to-end parameter characterizes the trust relationship in a network that is established between the sender and the receiver [PCKC05].

Interactivity characterizes the type of support for WSN simple request/response interactions, retrieving a measured value from some sensor node or setting a parameter in some sensor nodes. If the interaction pattern is synchronous, then the result (or possibly the acknowledgement) is expected to be immediate. Otherwise, asynchronous event notifications can be supported, e.g., where a requesting node collects information on the occurrence of a certain event.

WSN applications may be delay tolerant or not. If they are not delay tolerant they are usually classified as real-time applications.

The criticality is another relevant parameter which characterizes the entire WSN application. The application may be mission-critical or non-mission-critical. It does not depend on the network itself, but exclusively on how the network is used. For example, an application whose sensor nodes are used for patient heart rate monitoring is more critical than another that monitors regular exercise activities.

2.3.2 Traffic Parameters

Traffic characterization parameters include the accurate description of the QoS performance metrics of a WSN application. Supporting QoS in WSNs is still a largely unexplored research field. However, in the last years several works have addressed different protocols for applications in which QoS constraints are considered in their design [GHIGGHPD07]. The traffic parameters are a specific group that provides a perspective of how the application handles the different performance metrics. Two perspectives can be identified for QoS in WSNs:

- i) **Individual QoS** - Applications impose specific requirements on the deployment of sensors, in the number of active sensors, in the measurement precision of sensors and so on [MKPS01];
- ii) **Collective QoS** - From the network QoS perspective, the application that is actually carried out by itself is not so important, but more important is how the data is delivered to the

Table 2.2: Application requirements in a WSN network with QoS support [CV04].

Parameters	Class		
	Event-driven	Query-driven	Continuous
End-to-End	×	×	×
Interactivity	✓	✓	×
Delay tolerant	×	query-specific	✓
Criticality	✓	✓	×

sink and how the corresponding requirements are fulfilled.

Furthermore, from the QoS perspective, there are four basic data delivery models for the sensor network [TAGH02, Jur07]:

- i) **Event-driven** - Event-driven WSNs applications are interactive, delay intolerant (real-time), mission critical and non-end-to-end ones. As a consequence, the event detection sensors are very important to the success of the application. The data that flows from these sensors may be highly correlated, which leads to a high level of data redundancy. Besides, the data traffic generated by a single sensor may be of very low intensity, but with the possibility of supporting bursty traffic phenomena. The actions that occur in response to the detected event may need to be distributed to sensors or actuators as quickly and as reliably as possible;
- ii) **Query- or Demand-driven** - Most of query-driven applications are interactive, query-specific delay tolerant, mission critical, and non-end-to-end ones. In order to save energy, queries can be sent on demand. The query-driven delivery model it is similar to the event-driven model, except that in this one the data is pulled by the sink, while the data is pushed to the sink in the event-driven model (e.g., if the sink wants to upgrade the firmware on the sensor nodes);
- iii) **Continuous based** - In the continuous based model, sensors send their data continuously to the sink at a pre-specified rate. In this type of data delivery model, different types of traffic can coexist. However, different types of requirements must be fulfilled. On the one hand, real-time voice, image, or video data are non-end-to-end delay-constrained applications, whose packet losses can be tolerated. On the other, for non-real-time data, the delay and packet losses are both tolerated;
- iv) **Time-driven** - In time-driven networks, sensor nodes collect and report data from the physical environment periodically. The period between two consecutive data packets from a particular sensor node is referred to as the “data sampling rate”. Time-driven sensor networks are represented by a simple model in which nodes mostly report data and perform minimum data processing, while the sink node is where all the data processing takes place.

The aforementioned delivery models are deeply related with the service characterization parameters shown in Table 2.2 (end-to-end, interactivity, delay tolerant, and criticality).

The authors from [CV04] address all the above requirements. Application requirements are summarized in Table 2.2, which shows that there are some differences between WSNs and traditional networks in terms of application requirements. One of these differences is the end-to-end QoS parameter. The WSN application itself is not end-to-end, because one peer of the application is the sink, while in the other end there is not always a single sensor node but a group of sensor nodes (within the area in the range of the event). When the WSN communication is between a single node and a sink node, then the application is end-to-end. In this particular

case the end-to-end parameter is mentioned in the Table 2.2 to show that, in the majority of the WSN applications, there is a set of sensor nodes that are scattered over an area that collectively work to sense such event and report to the sink. In [CV04], as it is considered that these end-to-end network QoS parameters are insufficient to measure the QoS support in WSNs, some collective QoS parameters have been proposed, such as i) collective latency, ii) collective packet loss, iii) collective bandwidth, and iv) information throughput.

The traffic characterization parameters of a WSN application are also specified by its traffic generation pattern and the average duration. The traffic generation in WSNs is often assumed as CBR, on-off, Poisson, or exponentially distributed [CWGD10]. The bit rate (given in bits per second) associated to the generation process is the rate the modulator can support for transmission of the binary data.

The latency or end-to-end delay is also one of the key QoS parameters [CV04]. For some WSN applications, such as real-time monitoring or emergency response networks, performance guarantees (e.g., delay) are required. Two important aspects related to delay are the following: i) data freshness (how recent is the reported data) and ii) response time (the network capability to respond to environmental events or user queries within a given time interval).

2.3.3 Communication Parameters

Communication parameters are related with some of the previous characterization parameters from different groups (namely service and traffic groups). Each type of service has a particular communication constraint that has to be satisfied for the communication to be effective. For example, voice or video are delay sensitive. The service class needs to be identified for each type of traffic [GBH⁺03]. The key communication parameters of a WSN application include classes of service, synchronization (service traffic) and modulation. There are many types of services in a WSN (i.e., communication tasks, routing, localization, or the localization of a data sink for sensor data during the initialization of a node [GBH⁺03]).

Since WSNs are gradually becoming similar to legacy communications networks, to support more demanding WSN applications, the classes of service can be viewed from the QoS or ITU-T service traffic perspective. Based on the QoS parameters, two classes of services are identified:

- i) **Best-effort delivery (no QoS)** - It is addressed with ABR class of service, where the traffic is processed as quickly as possible [Sto06];
- ii) **Real-time delivery of time-based information** - It can be CBR or VBR with time requirements. In the WSN literature, CBR data traffic is commonly employed [CMGL05]. There are also a few works that consider VBR (e.g., Poisson distributed [MHA04]) data sources. For VBR [MRX08], based on QoS parameters, some authors consider an application with a VBR class of service as soft QoS one [VCB⁺02].

The data traffic is mapped into four specific classes of service:

- i) **CBR** - The monitoring values produced by the CBR WSN application are transmitted at a relatively constant bit rate. Nodes are served with a constant bit rate agreed during the initial setup of the WSN [HJB03];
- ii) **RT-VBR** - The bit rate varies between zero and a peak value agreed during the connection setup phase [MC05];

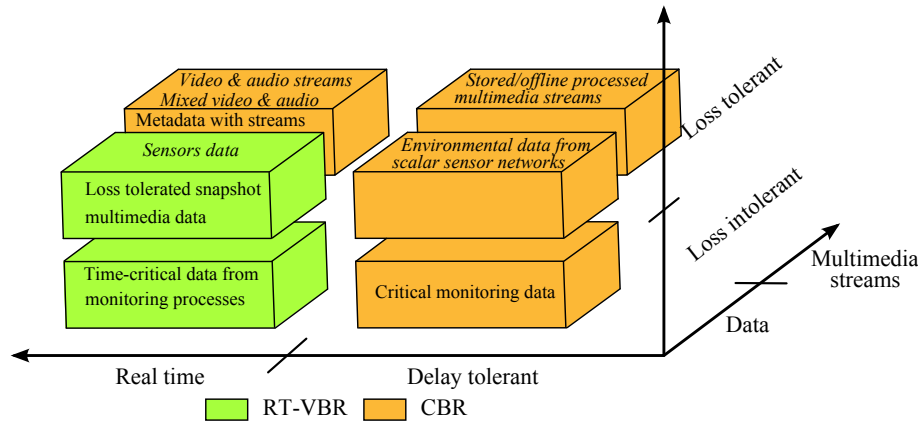


Figure 2.2: Definition of the service classes within communication parameters.

Table 2.3: Definition of the acronyms for the traffic classes.

Traffic classes	Acronym	Description
Type of delivery	RT	Real Time
	DT	Delay tolerant
Type of information	Data	Data
	MS	Multimedia streams
Data loss	LI	Loss intolerant
	LT	Loss tolerant

iii) **ABR** - it is a class in which a minimum data rate is guaranteed by the system for non-real time applications and ensures the delivery of data;

iv) **UBR** - It is a best effort service without performance guarantees. UBR is used for WSN applications that require mobility [SRJB03].

Figure 2.2 graphically presents examples for each type of service. The type of sensor data is presented inside of each box. The different axes are associated with the type of delivery (RT or NRT), type of information (Data or MS) and data loss (LI or LT). The authors from [SRS12] categorize the mission-critical applications into four different applications classes. The application classes are based on network-driven performance (i.e., the data loss and the type of delivery). Relatively to reference [SRS12], in Figure 2.2, a third dimension is added to the graph, i.e., the type of information. It shows the different types of data that may appear in WSNs, such as multimedia-related types of traffic. Table 2.3 presents possible attributes or values for the type of delivery, type of information, and data loss.

According to ITU-T terminology, the service traffic may be classified into two classes of service:

- i) **Isochronous traffic (ISO)** - Isochronous traffic includes the ability to simultaneously transport different data types (voice, video, and data), across the same system and includes the capability to dynamically allocate bandwidth as the application needs. When there is no other traffic but the sensor data in the network, the traffic of sensed data is typically isochronous (or synchronous) [KLJ⁺06];
- ii) **Non-isochronous traffic (NISO)** - Non-isochronous traffic is classified by message streams which are generated by their sources on a continuing basis but the delivery to the respective destination is not based on a continuous delivery (packet delivery fragmentation scheme).

The choice of the modulation to be used by the radio transmitter is another communication characteristic. The choice of the digital modulation scheme as well as the choice of radiated

power (within the legal constraints) can significantly influence the Signal-to-Noise Ratio (SNR). The range for the SNR evidently depends on the maximum transmission power, the antenna characteristics, and the path loss. The latter depends on the carrier frequency, the modulation/coding scheme, and BER one is willing to accept at the receiver. The BER describes the probability for a bit delivered to a higher layer to be incorrect and is an indicator of link reliability. It also depends on the quality of the receiver, essentially characterized by its sensitivity. The choice of the modulation scheme is crucial in WSN design and involves the following aspects: the required/desirable bit rate and symbol rate, the implementation complexity, the relationship between the radiated power and target BER, as well as the expected channel characteristics. The higher the offered bit rate by a transceiver/modulation is, the smaller the time needed to transmit a given amount of data. Consequently, if sleep modes are allowed the energy consumption is lower.

The power consumption derives from a modulation scheme which directly depends on the symbol rate rather than on the bit rate [KW05]. In WSNs applications, the most common modulation schemes are the following:

- **Binary Phase-Shift-Keying (BPSK)** - The use of a BPSK signal in WSN environments is more realistic than the consideration of impulse signals, as it occupies and utilizes a finite amount of bandwidth instead of an unlimited wide band [Gol05];
- **Frequency-Shift Keying (FSK)** - The FSK modulation may consider two different carrier frequencies to represent the zero and one. In WSNs, the FSK modulation is associated with modulation technique Direct-Sequence Spread Spectrum (DSSS), which allows for the signal to occupy the full bandwidth of the transmission frequency range by considering more than two frequencies to increase transmission rates [Gol05];
- **Gaussian Frequency-Shift Keying (GFSK)** - GFSK is a sub-type of the FSK modulation that employs a Gaussian filter to reduce the spectral width [Gol05] and mitigate positive/negative frequency deviations;
- **Amplitude-shift keying (OOK/ASK)** [WPW⁺07, AR05] - On-Off Keying (OOK) modulation is the simplest form of ASK modulation and is the only available modulation scheme that uses a single channel and frequency. In OOK, phase synchronization is not required. The disadvantage of OOK modulation arises in the presence of an undesired signal [LDBO⁺05]. The ASK modulation schemes offer the advantage of being more immune to interfering signals than OOK. ASK is easier to implement at a lower cost than FSK. However, FSK performs better in the presence of interfering signals;
- **Direct Sequence Spread Spectrum Offset Quadrature Phase-Shift Keying (DSSS-O-QPSK)** - The offset quadrature phase-shift-keyed (O-QPSK) modulation scheme is a derivation of traditional Quadrature Phase-Shift Keying (QPSK), which is more efficient because it requires less power than similar schemes, while achieving the same or higher throughput. It is usual within the 2.4-GHz band devices, (e.g., ZigBee transceivers). It enables devices to achieve a bit rate of up to 250 kb/s in a reasonably power-efficient manner [Gol05].

Finally, in terms of directionality, communications can be either uni-directional or bi-directional. While uni-directional communications are simplex ones, bi-directional communications can be either half-duplex or full-duplex:

- **Simplex (SPX)** - It corresponds to a system, in which the communication occurs only in one direction;

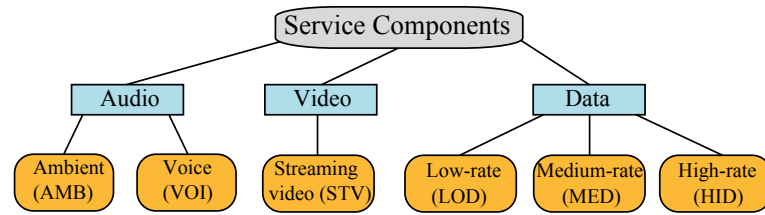


Figure 2.3: Basic service components.

Table 2.4: Service components versus type of information.

Types of information	Service Components					
	Audio		Video	Data		
	VOI	AMB	STV	LOD	MED	HID
Sensor Data	–	–	–	✓	✓	✓
Sound	✓	✓	–	–	–	–
Video	–	–	✓	–	–	–
Moving pictures and sound	✓	✓	✓	–	–	–
Snapshot images	–	–	✓	✓	✓	✓

- **Half Duplex (HDX)** - A half-duplex system supports communication in both directions. However, only one party or device (i.e., radio transceivers) can communicate at a time (not simultaneously);
- **Full Duplex (FDX)** - This type of systems, composed by two parties or devices to communicate, allows for each one to simultaneously communicate with another one in both directions.

2.3.4 Service Components and Data Acquisition/Dissemination

Basic service components for WSNs are audio, video and data. The service components and the type of information can be grouped as in Table 2.4. With the wireless sensor nodes coming of age, a new albeit nascent field of research has sprung up, namely exploration of the possibility of use of video/acoustic sensors to set up multimedia WSNs, to monitor and convey data in the form of only video, only audio, or both video and audio streams. Moreover, audio can be subdivided into Voice (VOI) and Sound Ambient (AMB), video can be supported by Streaming Video (STM), whereas data can be Low-Rate (LOD), Medium-Rate (MED) or High-Rate (HID), as shown in Figure 2.3.

Data acquisition and dissemination of data can be event-based, demand-based, continuous-based or time-based [Jur07], as mentioned in Section 2.3.2. These data dissemination models for sensor networks are not mutually exclusive and can be combined to provide a richer set of data dissemination options.

The packet delivery failure ratio is the average percentage of data packets lost during the data dissemination through node transmissions. This parameter is evaluated in terms of lost packets percentage and is very important. Lost packets lead to the degradation of the QoS of the WSN application, energy consumption inefficiency, and overall performance reduction.

2.3.5 Network Parameters

The **network** parameters group facilitates to characterize the different sensor node protocols (in the protocol stack). These parameters include self-organization, security and mobility support. Moreover, this group has parameters related to the application of the WSN network, such

as the lifetime, scalability, density, sensing range, addressing, programmability, and maintainability. All these parameters are inherent to the network as a whole.

The lifetime of the network is an essential characteristic in WSNs. The precise definition of lifetime depends on the application at hand. A simple option is to define network lifetime as the time until the first node fails (or runs out of energy), time until the network ceases to be fully operational. For this taxonomy this parameter is given in hours.

The ability to support a high amount of sensor node devices is known as the scalability of the network. Scalability is enabled by the employed architectures and protocols [PCKC05].

The number of nodes per unit of area gives the density of the network, which is another important characteristic that needs to be defined for the WSNs. The density of the nodes for an application also depends on the coverage area.

Different applications require different degrees of sensing coverage, which is characterized by the sensing range, the monitoring quality provided by a sensor network in a specific region. Sensor coverage may assume different ranges depending on the type of phenomena being sensed.

The self-organization is defined as the sensor nodes capability to find appropriate paths to establish the best communication among them and with central node (coordinator node), checking the received power level every time a configuration is built up. It is worthwhile to note that the self-organization of a network can be established either for the entire network or a part of the network.

The security of a WSN is determined by the protection policies associated with the data and WSN application requirements. As the level of security increases the energy consumption also increases, due to strong security policies that are associated to these highest levels. Since security is a vast area, only data encryption is considered in this taxonomy. According to [RY06, dOdON08], the level of security in WSNs can be classified as:

- **Low** - No security component is enabled and data fusion protocols may be used to reduce energy consumption;
- **Medium** - The security components will add security overheads to the data that is transmitted while performing data fusion. In this level, the security components do not interfere with the network operation;
- **High** - For the highest security level, cryptography algorithms are employed, preventing in-network processing. In this case, data aggregation protocols replace the data fusion ones.

The addressing scheme is another parameter of the network components group. These identifiers make each sensor node in the network unique, helping to setup routing paths when configuring the WSN. From all the addressing schemes currently being used in WSNs, the ones that are mostly used are the following ones:

- **Data-Centric** - A sensor node may not need an identity, e.g., an address. Rather, applications will focus on the data generated by sensors. In this case, all the data from the sensor nodes are named by attributes. This facilitates a more robust application design [EGHK99];
- **Attribute-based** - It is often seen as the most ideal scheme for wireless sensor networks. To use this addressing scheme in WSNs, it is worthwhile to guarantee the data-centricity (the sensor network that can be modified to the sensing task at hand [IM04]) and

the application-specificity. A particular node is not likely to be redundant for a specific information, rather a certain region;

- **Geographic addressing** - Frequently, WSNs are deployed randomly in remote and inaccessible terrain. Geographic addressing will use spatial coordinates. Therefore, localization techniques are essential to work with geographic addresses [KW05];
- **Address-centric** - In traditional networks like the Internet or ad hoc networks, nodes or stations are named and addressed as well as the data hosted by them. The address-centric scheme assigns to sensor nodes an unique ID (or name/label) based on low-level network topology information [KW05];
- **Spatial IP** - Each sensor constructs its spatial Internet Protocol (IP) address by taking the (x, y) coordinates of the node location as the two least significant octets in the Internet style IP address. It allows supporting geographic routing as well as routing based on network topology independently of geographic location [AU04];
- **Address-free** - One of the advantages of address-free WSNs is the possibility to randomly select a unique identifier for each transaction and spatial and temporal locality, rather than using static addresses [FLQ07].

The programmability from the wireless sensor nodes is a characteristic that does not only enables to process information but also to facilitates their flexible reaction to the changes in their tasks. The devices that constitute the WSN are either programmable or not programmable. The nodes programming must be changeable during operation when new tasks become opportune. Since the WSN and their environment continuously change (e.g., depleted batteries, failing nodes and new tasks), system adaptation is needed. The maintainability of a WSN represents this adaptive behaviour which a WSN application may have. The network [RMC02] has to maintain itself, being able to interact with external maintenance mechanisms whilst ensuring an extended operation at a required service quality.

The homogeneity of the network characterizes how similar to the capabilities of a sensor node are in comparison to the other ones that coexist in the same WSN. The network is homogeneous if all the WSN nodes present the same capabilities in terms of processing, energy and communication resources. A network is heterogeneous if, additionally to these sensor nodes, there are nodes with increased capabilities relatively to the majority of nodes [ZK03].

The last network parameter is the mobility support in a WSN application. Normally, the WSN sensor nodes applications are static. However, in the real-world, the nodes may be moving. Therefore, the protocols from different layers of the WSN must be aware of the sensor node mobility, in order to establish new paths between nodes, as the nodes move on the field. The support of mobility requires additional processing capability from the sensor node.

2.3.6 Node Parameters

The sensor node hardware is composed by several modules that jointly form a device with communication capabilities. Since these modules can be chosen from a wide variety of manufacturers, the classification of the sensor node hardware can be categorized based in a set of parameters.

The node characteristics is a set of parameters that help to distinguish the type of nodes and the characteristics that the nodes present in a specific WSN application. A set of characterization parameters is defined for each WSN application that covers essentially the node hardware

description, as well as the sampling rate of the external sensors that are attached to the node. This set of parameters defines the operation of the sensor jointly with their different communication protocols and the associated control of the sensor nodes hardware. Each one of the hardware components has to operate properly, while balancing the trade-offs between low energy consumption and high efficient operation (to fulfil the assigned tasks).

Different applications require different levels of processing capabilities. This processing is handled by the microprocessor/ microcontroller. The microprocessor/microcontroller is the main component of the sensor node. It is responsible to process all the relevant data and is capable of executing arbitrary code in the sensor node while coordinating the interaction with neighbouring nodes. In our taxonomy, we distinguish the type of microprocessors in terms of manufacturer.

In a WSN, a sensor node is a device with communication capabilities. The radio transceiver enables that each sensor node is identified as a unique entity in a WSN and is of paramount importance. The radio transceiver is the key component that allows for sensor nodes to communicate wirelessly with other sensor nodes over a wireless channel. In our taxonomy we distinguish the radio transceivers, by the manufacturer and respective transceiver model. For the sake of energy efficiency its choice must be energy aware.

The overall energy consumption also plays an important role in WSN along with the need for a longer lifetime, and on the WSN application. In our taxonomy we define pre-established intervals for the maximum achievable lifetime, where the WSNs are grouped into each one of the following intervals: a) [24, 720] h, b) [721, 25920] h, and c) >25920 h.

The Sampling Rate (SR) corresponds to the number of samples taken from the sensed event signal and reported as data packets to the sink node [AA07]. Since the sensor nodes have different types of sensors attached to them, the SR can be different for each of them [HLBW08]. We classify the sampling rates into three categories:

- **Low SR** - varies between 0.001 Hz and 100 Hz;
- **Medium SR** - varies between 100 Hz and 1 kHz;
- **High SR** - higher than 1 kHz.

The role of the WSN entities depends on the processing capabilities and how sensor nodes themselves take on specific functions and behaviours in the network. If the application supports heterogeneous nodes, these roles are assigned according to various sensor node properties (e.g, location, type of sensors and actuators). In our taxonomy we define the roles of WSN device as:

- **Sensor node** - It comprises the microprocessor/microcontroller, radio transceiver, and sensors; and facilitates to measure the physical quantities.
- **Sink node** - It can be a sensor node but with extended data processing capabilities, since it receives data from all the sensor nodes of the WSN, while it manages the network;
- **Sensor and actuator node** - It comprises the same basic sensor node components plus actuators;
- **Anchor node** - Node with known localization, which supports the remaining sensor nodes in the localization process;
- **Cluster head** - Sensor node to whom all nodes in the cluster (group of nodes, created according to: geographical area, type of sensor, type of phenomenon, task, etc) send the

collected data; the cluster head is then responsible for sending the received data to the sink node. It also delivers data coming from outside the cluster (commands, queries, etc.) to the cluster members;

- **Gateway node** - It is a node responsible for the connection and delivery of data to other communication networks from other technologies (e.g., Wi-Fi, fixed access to Internet or WiMAX).

It is worthwhile to mention that, in the perspective of [dB11], [dBRP08], [RPBS11], collaborative WSNs are managed by a software tool whose user (person) interacts with the WSN, querying the network, visualizing data, etc. The user customizes the work of the sensor nodes; the data collected by sensor nodes is used by the user's application. As the radio transceiver is the key component in a sensor node, the range of each sensor node depends on the choice of the radio transceiver. Besides, trade-offs between the maximum range of the sensor node and the network lifetime maximization is always a critical decision.

The range depends on the radio output power and comprises two components: the fixed and variable components. The first one corresponds to the minimum acceptable power of the radio transceiver while the second one is related with variation of the output power until the maximum allowable output power. The IEEE 802.15.4-compliant devices should be capable of transmitting at a minimum of -3 dBm. Its maximum output power needs to comply with the local radio spectrum regulations. The communication range of each sensor node in a WSN application depends on which type of radio transceiver the sensor node uses and on the trade-offs to render network lifetime maximization in battery-powered nodes.

Finally, different types of power supply can be used in the WSN nodes. In our taxonomy, we distinguish between three energy sources: i) battery, the most common way to power up sensor nodes, ii) harvesting device, which collects energy from the surrounding environment (e.g., vibrations, solar, heat or electromagnetic energy), and iii) local supply by means of an uninterrupted power supply.

In addition to the aforementioned node parameters, several surveys have been published concerning the hardware aspects on the different Wireless Multimedia Sensor Networks (WMSNs) sensor nodes [KKK11, CCH12, KKJ11]. Other works, such as the ones from [HLBW08, SR11, TBZBO12, AGZAKMP10, AMC07] [AMC08], characterize the hardware of the typical WSN sensor nodes, in which the hardware is simpler. Based on all these works we propose System on a Chip (SoC) characteristics for a specific microcontroller in Tables 2.5 and 2.6, jointly with the reference to the sensor node platform that employs the microcontroller. By knowing the characteristics of a specific microcontroller in detail, it is possible to better plan the usability of its functions for a WSN application. These tables present not only the SoC characteristics of the microcontrollers but also other important features that are not present in the referenced papers such as the clock speed, type of power management, number of available timers and ADC resolution.

Table 2.5: System on a chip characteristics of microcontrollers.

Microcontroller	Architecture	Clock speed	Memory		Peripherals		Power management	Platform
			RAM	Flash	Timers	ADC		
ATmega 128L	8-bit	8 MHz	4 KB	128 KB	4	10-bit	Six sleep modes Software selectable clock frequency	Mica2/Mica2Dot/ MicaZ; Cyclops; CSIRO ICT'S FleckTM-3
ATmega 103L	8-bit	6 MHz	4 KB	0.125 KB	3	10-bit	Four sleep modes	Mica
AT90LS8535	8-bit	8 MHz	0.512 KB	8 KB	3	10-bit	Three sleep modes	Rene
ATmega 163	8-bit	8 MHz	1 KB	16 KB	3	10-bit	Four sleep modes Power-on reset	Rene2 , Dot
ATmega 1281	8-bit	8 MHz	8 KB	128 KB	6	10-bit	Programmable brown-out detection; Six sleep modes;	Firefly
ATmega 8	8-bit	16 MHz	1 KB	8 KB	3	10-bit	Power-on reset Programmable brown-out detection; Six sleep modes;	BTnode
PIC18LF4620	8-bit	4-8 MHz	1 KB	64 KB	4	10-bit	Power saving idle and sleep modes	TUTWSN
MSP430F1611	16-bit	8 MHz	10 KB	48 KB	2	12-bit	Supply voltage supervisor with programmable level detection	TelosB Tmote Sky
MSP430F449	16-bit	8 MHz	2 KB	60 KB	2	12-bit	Supply voltage supervisor with programmable level detection	WSN430
MSP430F149	16-bit	8 MHz	2 KB	60 KB	3	12-bit	Five power-saving modes	BSN
Xetal II	16-bit	84 MHz	10 MB	N.A.	N.A.	N.A.	Controlled by power management chip	WiCa
MSP430F1612	16-bit	1-11 MHz	5 KB	55 KB	2	12-bit	Supply voltage supervisor with programmable level detection	Freie Universitat's ScatterWeb
OKI ML 67Q5002	32-bit	57.6 MHz	32 KB	256 KB	1 (8 ch.)	10-bit	Power tracker, supervisor, Controlled clock divider peripherals switch on/off	Yale's XYZ
INTEL Xscale (PXA255)	32-bit	100-400 MHz	64 MB	32 MB	4	4x10-bit	No support for network wake-up; battery monitoring utility; power management unit.	UC Berkeley's Stargate

Table 2.6: System on a chip characteristics of microcontrollers (cont.).

Microcontroller	Architecture	Clock speed	Memory		Peripherals		Power management	Platform
			RAM	Flash	Timers	ADC		
INTEL Xscale (PXA270)	32-bit	500 MHz	N.A.	N.A.	1	12-bit	Power management chip; Supply voltage reduction; Four low-power modes; Dynamic voltage and frequency management	NIT-Hohai Node
INTEL Xscale (PXA271)	32-bit	13-416 MHz	32 MB	32 MB	1	12-bit	Power management chip; Supply voltage reduction; Four low-power modes; Dynamic voltage and frequency management	Crossbow's Imote2/ Stargate 2
Atmel AT91SAM7S (ARM 7TDMI)	32-bit	55 MHz	64 KB	256 KB	3	10-bit	MCU power management; Software controlled phase locked loop	Stanford's MeshWye; WiSN motes; Imote; MeshEye;
Freescale Coldfire MCF5282	32-bit	66-80 MHz	64 KB	512 KB	12	10-bit	Fully-static operation with processor sleep; Wake-up with external interrupts; Clock enable/disable for each peripheral;	Coldfire MCF5282 ZigBee ready Demo kit
AT91RM9200	32-bit	180 MHz	16 KB	128 KB	6	10-bit	Slow clock operating mode software power optimization capabilities	SUN spot
TI-TMS320 VC 5509A	32-bit	108 MHz 144 MHz 200 MHz	192 KB	128 KB	2	10-bit	Programmable low-power control of six device functional domains	-
PHILIPS NXP LPC2106	16/32-bit	1 MHz 30 MHz 60 MHz	64 KB	128 KB	2x32-bit	N.A.	Two low power modes; Processor wake-up from via external interrupt	CMUcam3
ADSP-BF537 Blackfin	16/32-bit	600 MHz	32 MB	4 MB	8x32-bit	12-bit	Dynamic clock up to 600 MHz	CMU's DSPCam

2.3.7 Operation Environments

The operation environment characteristics define the context in which the WSN applications are deployed. This group of parameters is sub-divided into three sub-groups: i) WSN scenarios, ii) WSN framework, and iii) deployment scenarios. The first sub-group distinguishes between the single-hop, multi-hop, and mobility scenarios. From the basics of radio communication and the inherent power constraints, radio communications are limited by the feasible distance between the sender and receiver. Note that the simple direct communication (single-hop) between source and sink is not always possible owing to the resulting coverage difficulties. The second sub-group is the operation framework: i) public, or ii) private. The third one (deployment scenarios) allows for shedding light on the environments for WSN applications deployment.

Before describing the operation environments where the WSN can be deployed in, it is worthwhile to define what source and sink nodes are. A source is any entity in the network that can provide information, i.e., typically a sensor node and it could also be an actuator node that provides feedback about an operation. A sink, on the other hand, is the entity where information is required. Figure 2.4 presents these three main types of sink nodes in a case with single-hop communication. Figure 2.4 a) considers the sink as a normal sensor node in the network (with no extended capabilities); Figure 2.4 b) assumes the sink node as sensor node with extended capabilities; and Figure 2.4 c) considers a sink node, which is a gateway, with extended capabilities and connected to the higher layers networks in the hierarchy [KW05].

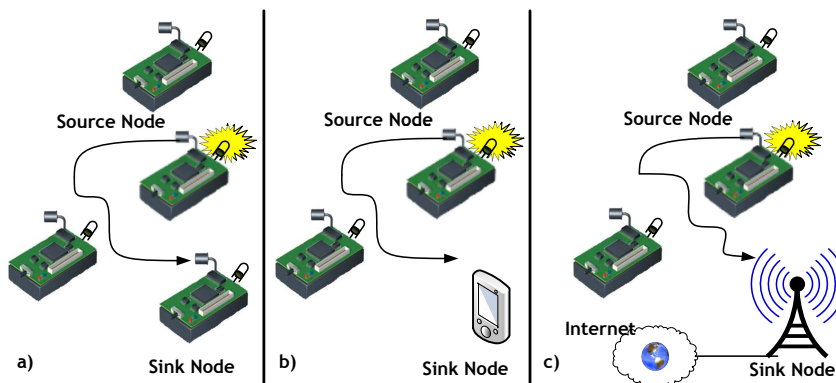


Figure 2.4: Main types of sinks with single-hop communication.

For much of the remaining discussion, the distinction between the various types of sinks is actually irrelevant. It is however important to know whether sources or sinks are able to move. However, what sinks and sources do with the information is not a primary concern of the networking architecture. In the context of the most common sensor network scenarios, the first distinction is between single-hop and multi-hop networks. From the basics of radio communication and the inherent power constraints, radio communications have a limitation on the feasible distance between a sender and a receiver. Because of this limited distance, the simple direct communication between source and sink is not always possible, as shown in Figure 2.5, specifically in WSNs, as they are intended to cover broad areas (e.g., in environmental or agriculture applications), operating in difficult radio environments with strong attenuation (e.g., in buildings). To overcome such limited distances, an obvious solution is to use relay stations, with the data packets taking multi hops from the source to the sink. This concept of multi-hop networks, shown in Figure 2.5, is particularly attractive for WSNs, as the sensor nodes themselves can act as such relay nodes, eliminating the need for additional devices.

While multi-hopping is an evident and working solution to overcome problems with large dis-

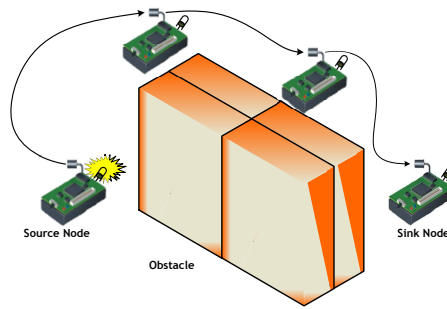


Figure 2.5: Multi-hop network.

tances or obstacles, it has also been claimed to improve the energy efficiency for the communications.

In fact, the authors from [MC03] classify the misconception that multi-hopping saves energy as the number one myth about energy consumption in wireless communication. Great care should be therefore taken when applying multi-hopping aiming to improve the energy efficiency. In such a network, a node has to correctly receive a packet before it can forward it somewhere else. In alternative, innovative approaches attempt to exploit even erroneous reception of packets. For example, they explore the cases when multiple nodes send the same packet and each individual transmission could not be received, but collectively, a node can reconstruct the full packet, e.g., by applying the frame capture effect [FXHZ10] from Chapter 7.

Another scenario is the multiple sinks and sources one. Besides only networks with a single source and a single sink, in many scenarios, there are scenarios with multiple sources and/or multiple sinks. In the most challenging case, shown in Figure 2.6, multiple sources that should send information to multiple sinks are present. Either all or some of the information has to reach all or some of the sinks.

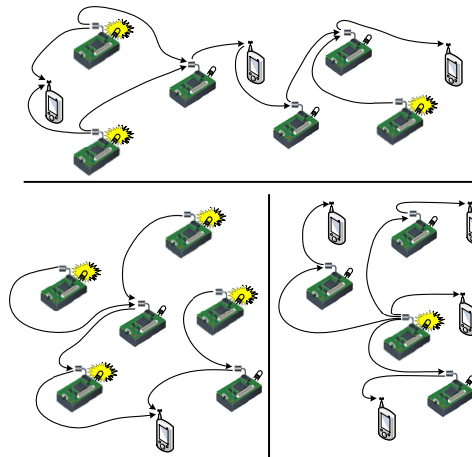


Figure 2.6: Deployment scenarios with multiple sources and/or multiple sinks.

A third scenario is the mobility one [SSJ01]. Although in the scenarios discussed above all participants were stationary, one of the main virtues of wireless communications is its ability to support mobile participants. In WSNs, mobility can be presented in three main forms:

- **Node mobility** - The wireless sensor nodes themselves can be mobile. The meaning of such mobility is application dependent. In examples like environmental control, node mobility should not happen; in livestock surveillance (sensor nodes attached to cattle, for

example), mobility is the common rule. Because of node mobility, the network has to reorganize itself frequently enough, to be able to properly operate. It is clear that there are trade-offs between the frequency and speed of node movement, on the one hand, and the energy required to maintain a desired level of functionality in the network, on the other hand.

- **Sink mobility** - In Figure 2.7, the information sinks can be mobile. While this can be a special case of node mobility, the important aspect is the mobility of an information sink that is not part of the sensor network, for example, a human user requested information via a PDA while walking in an intelligent building. In a simple case, such a requester can interact with the WSN at one point and complete its interactions before moving on. Other case considers a mobile requester which is particularly interesting. However, if the requested data is not locally available the requester would likely communicate only with nodes in its vicinity in order to retrieve the data from some remote part of the network. The network, possibly with the assistance of the mobile requester, must make provisions that the requested data actually follows and reaches the requester despite its movements [SSJ01];

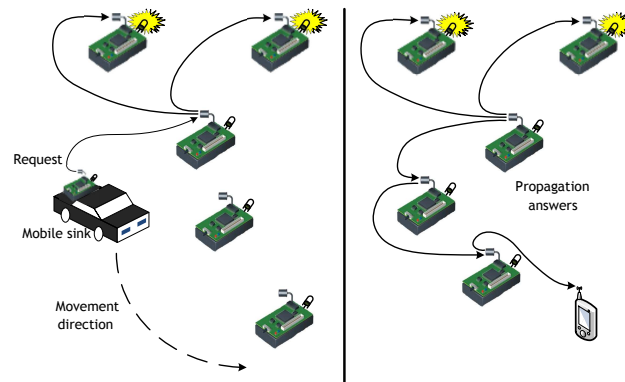


Figure 2.7: Deployment scenario with the presence of a mobile sink.

- **Event mobility** - In applications like event detection, in particular tracking applications, the cause of the events or the objects (to be tracked) can be mobile. In such scenarios, it is important that a sufficient number of sensors permanently covers the observed event. Consequently, sensors will wake-up around the object, and will be engaged in higher activity to observe the present object. Only then they will go back to sleep. As the event source moves throughout the network, it is accompanied by an area of activity within the network. The authors from [SGAP00] named this effect as the “Frisbee” model (which also describes algorithms for handling the “wake-up wavefront”). This notion is described in Fig. 2.8.

Besides the sensor network scenarios themselves, to perform a complete definition of the operation environment it is worthwhile to define the framework, which is divided into main two subsets [GPS⁺06]:

- **Public** - Urban, roads, rural or commercial zones;
- **Private** - Emergency dedicated.

In terms of mobility, the devices or entities present typical average speed (V_{av}) values that can be taken into account to design new WSN applications with mobility support. The scenarios

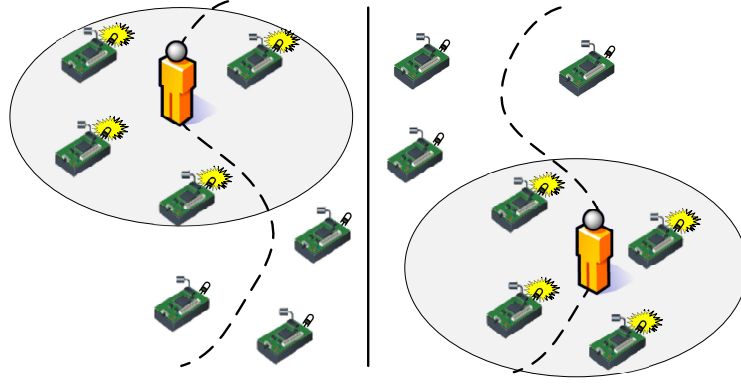


Figure 2.8: Event mobility in wireless sensor and actuator networks.

Table 2.7: Typical values for the average velocity from WSN entities.

Telemedicine	Entity	V_{av}	Article(s)
	Mobile WSN node	0.1 ms^{-1}	[SNVW07]
		0.42 ms^{-1}	[ZCLP07]
	User (fastest human)	10 ms^{-1}	[SW04a]
	Mobile sink	$1\text{-}10 \text{ ms}^{-1}$	[SW04a]
	User (walking)	2 ms^{-1}	[HK03]
	Car (normal speed)	10 ms^{-1}	
	Car (high speed)	20 ms^{-1}	

of mobility can be characterized by a triangular distribution for the velocity of the mobile elements of a mobile WSN. These typical values are summarized in Table 2.7.

The deployment scenarios are defined by the set of services/applications operating simultaneously in the WSN. The typical geographical areas/zones of operation are the following ones: Offices, Industry, Home, Military, Civil, Metropolitan and Rural.

2.4 Range of Variation for the Characterization Parameters

The wide diversity of WSN applications motivates the need for their classification. Hence, the most suitable solution to organize the different types of applications is to taxonomize sensor networks and systems into two categories, Category 1 WSNs (C1WSNs) and Category 2 WSNs (C2WSNs) as presented in [SMZ07a]. In the C1WSNs category, WSNs are mainly multi-hop, supporting massive data flows, with dynamic routing and high density network. In turn, in the C2WSNs category, WSNs are mainly single-hop, with static routing, a low/medium density network, supporting source-to-sink applications and suitable for applications in confined short-range spaces. A more detailed description of each application area is given in Appendix B. Their characteristics are presented in Table 2.8. This list of parameters facilitates to compare the differences and similarities between both categories. In Table 2.8 we define a node as Repeater Node (RN) if it supports communications on behalf of other sensor nodes. If a node forwards the packets it is referred as a Forwarder (FN).

On the one hand, if a node forwards information from other node it is a cooperative node. On the other, if a node only handles its own information, then it is a non-cooperative node. In Table 2.8, dynamic routing is a mechanism that has the same function as static routing except it is more robust, since it finds the best route from a wider set of paths.

Besides the division of WSNs into these two categories (C1WSNs and C2WSNs), the applications

that belong to these two categories fall into two different user requirement classes: Event Detection (EDe) and spatial and time random Process Estimation (PE), [CRU06]. For the sake of convenience, the attributes for each characteristic that allows for comparing both these classes are summarized in Table 2.9. One characteristic of the ED class that is not presented in Table 2.9 is the network coverage, deeply related with the nodes' sensing range and event type.

If the sink nodes utilize a demand-driven data acquisition scheme to periodically query the nodes, the periodicity of queries must be chosen so that the event is detected and the data is delivered to the sink nodes on time. For the PE class, a good example for the periodic estimation of a given physical phenomenon is the modelling of the atmospheric pressure by a bi-dimensional random process.

2.4.1 Holistic Overview of the WSN Applications Taxonomy

The large amount of work that has been produced over the last 10 years on the different areas of WSNs allows us for identifying the different parameters of our proposed application taxonomy. We have classified key WSN applications for the different areas, as well as analyzed the WSN applications evolution over the years. The time stamps on the publications of different projects also allow us to observe how the different areas have appeared chronologically for the past 10 years, facilitating to foresee the future trends. After gathering all the information from different projects, in this work we have summarized it in tables (whilst considering the different areas). However, since it is difficult to present all the comparison tables for all the groups of parameters, we will opt for presenting tables with a subset of parameters. These tables are a representative sample of all the work performed by us on the taxonomy for the characterization and classification of WSNs.

By combining the C1WSNs and C2WSNs categories with the ED and PE classes we were able to organize the main WSN applications areas and the corresponding sub-applications of each area. The applications from the C1WSNs and C2WSNs categories are presented in Tables 2.10 and 2.11, respectively. Since it is not feasible to present all the classification tables the identification of

Table 2.8: Comparison of the C1WSNs and C2WSNs characteristics.

Characteristics	C1WSNs	C2WSNs
WSN scenario	≥ 1 -hop away from (RN) or (FN)	1-hop away from FN
WSN topology	Multipoint-to-point	Point-to-point Multipoint-to-point
Radio link range	Measured in thousands of meters	Measured in hundreds of meters
Sensor node repeater function	Wireless router	Wireless router
Forwarding node supported mechanisms	Dynamic routing > one physical link to the network Data processing	Static routing one physical link to the terrestrial network
Nodes behaviour	Cooperative & non-cooperative	Non-cooperative
Network density	Large-scale systems	Simple and short-range wireless systems
Data flow characterization	Massive data flows	Transaction-based data flows
Sensor node capabilities	Repeater & Forwarder	Non-repeater & Forwarder
Applications examples	Environmental monitoring National security systems	Residential systems Confined short-range spaces, e.g., home, factory, building

Table 2.9: Comparison of the ED and PE classes.

Characteristics	ED	PE
Data acquisition	Event-driven Demand-driven Not time-driven	Periodic estimation of physical phenomenon Demand-driven
Signal processing capabilities	Simple compare with threshold & send to sink	Data gathering & forwarding to sink(s) sink collects & handles packets from nodes
Node density	Enough to guarantee a given event detection probability	Enough to ensure the process is accurately estimated
Efficient mechanisms support	Distributed localization algorithms	Sampling frequency allow event tracking
Connectivity issues	Alarm packets arrive with high probability & in a short time	Process estimation error < threshold
Main issues	Coverage Connectivity Distributed localization Ensure low packet losses and delays	Signal processing Connectivity Time synchronization Ensure low process estimation error
Application requirements	Min. probability of coverage Max. localization error Min. probability of connectivity Max. packet loss probability Max. packet delivery delay	Max. estimation error Max. localization error Min. probability of connectivity Max. packet loss probability

Table 2.10: Characterization of Category C1WSNs applications. †- PE; ♪- PE&ED; ‡- ED

Applications Area	Applications
Metropolitan Operation [†]	1 - Highway monitoring [CV07, MYT ⁺ 06] [†]
Military [♪]	2 - Condition-based-monitoring [JR07] [†] 3 - Surveillance [GM05] [‡] 4 - Borders Monitoring [SBI] [‡]
Civil Engineering [‡]	5 - Structural Integrity Monitoring [BEOiRTUE07] [‡]
Environmental Monitoring [♪]	6 - Monitoring Volcanic Eruptions [WALJ ⁺ 06] [♪] 7 - Habitat Monitoring [MCP ⁺ 02] [♪] 8 - Water Monitoring [Aqu, dGLM ⁺ 07] [♪] 9 - Weather Monitoring [JM06] [♪] 10 - Forest Fire Detection [ASSDGC08, ASSdGC06] [♪] 11 - Precision Agriculture [BDO ⁺ 05, MID04] [♪]
Logistics [♪]	12 - Target Tracking [HKL ⁺ 06, DHJ ⁺ 06] [‡] 13 - Warehouse Tracking [EHK ⁺ 07] [♪]
Position & Animals Tracking [‡]	14 - Immersive Roam [LEM] [‡] 15 - Real-Time Relative Positioning System [JKLK08] [‡] 16 - Wild-Life Tracking [JOW ⁺ 02, Hog, Lor04] [‡]
Transportation [†]	17 - Smart Roads [Mar04, Ast] [†]
	18 - Automobile [ESVS ⁺ 09] [†]
	19 - Sensor & Robots [DRS ⁺ 05] [♪]
	20 - Reconfigurable WSN [HKWW06] [‡]
	21 - Nanoscopic Sensors [‡]

the most common attributes or values for the corresponding parameters is followed by a brief discussion on the achieved results for each group of parameters:

- **Service parameters** - the majority of the analysed applications requires real-time delivery, all have a bidirectional communication, present a symmetric communication, do not need end-to-end connection, are mostly interactive and are mission critical. Moreover, all the identified applications are delay tolerant except for the water monitoring, automobile, telemedicine and smart office applications. These four applications are not delay tolerant. Besides, the delay parameter depends on the delivery requirement parameter,

Table 2.11: Characterization of Category C2WSNs applications. †- PE; ™- PE&ED; ‡- ED

Applications Area	Applications
Industrial Automation™	22 - Commercial Spaces™
	23 - Smart Factory [WLH ⁺ 08]™
Health™	24 - Pre-Hospitalar [LMFJ ⁺ 04]™
	25 - In-Hospitalar Emergency Care [KLC ⁺ 10]™
	26 - Telemedicine [ZC05]™
	27 - (Tele)Rehabilitation [IKKV08]™
Mood-based Services†	28 - Personal Coaching [e-S]†
Entertainment‡	29 - Dynamic Spaces‡
	30 - Gaming [MGN ⁺ 05]‡
	31 - Gesture/body Tracking [Ayl06]‡
	32 - Smart Office [RML05]‡
	33 - Sports [KGG ⁺ 09]‡
	34 - Building Automation [PWVW08]‡
	35 - Home Control [FFR09]‡

which, in turn is related with the QoS class. Other parameters, like the class of service and traffic class, are influenced by the characterization parameters from this group. Since, in the majority of the WSN applications, the delivery requirement is real-time, the traffic class (from the communication parameters group) is frequently real-time.

- **Traffic parameters** - the majority of the applications follow an event-driven data delivery model, related to the attributes chosen in the service parameters described above. Event-driven applications are defined as interactive, non delay tolerant, mission critical, real-time, and non-end-to-end ones. Most of the applications present a bit rate that varies up to 57.6 kbps. However, nowadays there is a significant number of applications that work at a bit rate higher than 115.2 kbps. For a considerable number of applications, the minimum acceptable delay for data delivery varies between 0 and 250 ms, while the maximum acceptable delay varies around 250 ms and 1000 ms. Nonetheless, there are some applications with a maximum delay that varies around 1 and 10 s, or even 63 s, depending on the deployment scenario (n.b., harsh environment allows for higher delays tolerance).
- **Communication parameters** - nearly all applications need a synchronized platform for nodes to work. Only the structural integrity monitoring, wild-life tracking and gaming do not require a synchronized platform. However, the sports application may require or not a synchronization scheme, depending on the type of sport being monitored. In terms of delivery requirement the majority of the WSN applications are in real-time. Since the communication parameters, namely the class of service and traffic classes, are influenced by the parameters from the service parameters group, the most common service traffic is the Real Time & Loss Tolerant & Data (RT&LT&Data), while the most prominent classes of service are the Isochronous & Real Time-Variable Bit Rate (ISO&RT-VBR) and Isochronous & Constant Bit Rate (ISO&CBR). The packet delivery failure ratio (PDFR) for some applications varies between 1 and 10 %, although this aspect is not well described in some of the studied projects. The types of modulation scheme employed in the applications are the FSK (DSSS) and DSSS-O-QPSK, with half-duplex communication capabilities. The latter correspond to an IEEE 802.15.4 compliant radio transceiver. In terms of service components, the most usual ones are the HID, MED and LOD. These applications areas are more suitable for the event-driven delivery model. However, some applications present a combination of STV+HID or STV+LOD+MED+HID service components. The most prominent model for data acquisition & dissemination is the event-driven one, followed by demand and event driven

combination models. These models are deeply related with the QoS parameter from the traffic parameters group, as well as with the delivery requirement and delay tolerance parameters (from the service parameters group). Depending on the delivery requirement and the delay tolerance of the WSN application, the QoS model that is assumed by the application must fulfil the requirements from the service group and from the acquisition & dissemination model (closely related with the QoS model).

- **Network parameters** - this group is the one with the vastest variety of parameters (from all the groups of parameters). First, the lifetime of the analysed applications mainly varies between 29 and 720 h, i.e., most of them are short-term applications. Besides, applications present a deployment of no more than 50 sensor nodes in real-scenario deployments, while covering an area larger than 100 m² in the majority of the applications. Only the density of nodes in indoor applications differ from this value (i.e., less than 10 m²). Building divisions impose special attention to the propagation phenomenon and sensor nodes deployment. This shows that high scalable deployments are still not fully feasible. As sensor hardware does not allow for long sensing range, the sensing area is limited to 10 m² for all the applications. Hence, the WSN applications are cooperative and limited in the sensing of the phenomenon. This sensing restriction allows for reducing the redundancy of the sensed data. From the studied applications, almost all have a self-organization procedure. Only border monitoring, precision agriculture and (tele) rehabilitation applications consider mechanisms to organize only a part of the network. The habitat and weather monitoring applications do not consider any type of mechanism to organize the network automatically. Besides, there is a lack of security mechanisms in the majority of the applications. Only in some applications (e.g., military) the security (medium or high) is considered. In practice, in the WSN applications, the addressing is performed mainly in two ways: i) MAC address or ii) node ID. *In situ* node reprogramming without the need for suspending all the network operation is not usual in more than half of the analysed applications. Nonetheless, there are some applications that allow for sensor node reprogramming.

The use of mechanisms to ensure the maintainability of the sensor nodes is common in the majority of the applications. The WSNs are composed by different devices that together form the network itself. In the studied applications, it is typical to observe a heterogeneous nature in terms of WSN network composition. Finally, the mobility support feature is employed in nearly half of the applications from the different areas.

- **Node parameters** - microprocessors are mostly ATMEL, TI or DustNetworks ones, while the most used radio transceivers are the CC1000 and the CC2420 ones. The studied WSN applications use hardware commercially available that already incorporate these radio transceivers. In addition, the former is IEEE 802.15.4 standard non-compliant and the latter one is compliant. If we wish to change the radio transceiver only experts are capable of changing the radio transceiver. In terms of overall energy consumption, with sensors attached, the majority of the applications present an energy consumption less or equal than 50 mA, and few applications require an energy consumption of around 51 and 100 mA (considering a power supply of 3.3 V). The applications that present a higher consumption are typically the ones that have a higher sampling rate. The most common reporting frequencies in the studied applications are the medium and low sampling rates. Regarding the type of function that is performed by the different devices in WSNs, the majority of the applications are composed by sensor and sink nodes and always a user. Some applica-

tions have already started to have a gateway, allowing the WSN to connect to the Internet and disseminate the gathered data. Other applications also possess actuators connected to the sensor nodes, in order to execute the commands given by the central node. The communication range is related with the type of radio transceiver, the transmission power and the signal propagation environment where it is inserted. The majority of the applications achieve a range of at least 50 m. Finally, the power supply used by the WSN devices is mainly formed by batteries. In some cases, however, batteries are combined with an energy harvesting device (e.g., solar panel).

2.4.2 New WSN Applications Categories

Based on the previous holistic overview of the WSN applications taxonomy, we are able to identify some common features between characterization parameters, enabling to propose a new classification of the applications, based on the combination of the parameters' attributes.

Table 2.12: Categories for time related applications.

Parameters	Category		
	LTA	MTA	STA
Lifetime	> 25920 h	[721; 25920] h	[24; 720] h
Scalability	> 400 nodes	[51; 400] nodes	≤ 50 nodes
Maintainability	Maintainable	Maintainable	Maintainable
Sampling rate	Low/Medium	Medium	High
Acquisition & dissemination	Low event/ demand-driven	Medium event/ time-driven	High event/ time-driven

The first group of the three categories is related with the time related constraints of applications, which relates the lifetime, scalability, maintainability, sampling rate, power supply and acquisition & dissemination classes parameters. This time related application group considers that all the WSN applications that present the same attributes for the respective parameter belong to the corresponding category, as shown in Table 2.12. The three possible categories are: the Long-Term Applications (LTA), Medium-Term Applications (MTA), and Short-Term Applications (STA). In Table 2.12 (time related applications categories) the parameters considered to group the different WSN applications into one of the three categories are sufficient. For these categories, the time is a very important issue and allows for easily identifying the WSN applications that last longer or are supposed to present a longer usable lifetime. Therefore, the lifetime parameter for these categories is essential in order to provide a time basis in which different periods of time (in hours) correspond to long, medium and short term deployment of WSN applications. The sampling rate parameter is related with the lifetime parameter. On the one hand, a WSN application with higher sampling rate generally has a shorter lifetime. On the other, low sampling rates lead to a longer lifetime. Another characterization parameter deeply related with the lifetime and sampling rate is the acquisition and dissemination. This parameter represents how the data acquisition is performed during the lifetime of the sensor nodes. By being aware of the type of acquisition the WSN application has, it is possible to infer which type of acquisition and dissemination schemes are common in certain application areas. To complement the grouping of WSN applications in one of the three categories, the maintainability parameter is also related with the lifetime, since it contributes to save energy (when the WSN application is maintainable), and consequently to increase the lifetime. The size of the network is another parameter that influences the lifetime of the WSN application.

Table 2.13: Aggregation of WSN applications for time related categories.

Applications	Lifetime (h)	Scalability (nodes)	Parameters			Positive matches ratio	Belongs to the category
			Maintainability	Sampling rate	Acquisition & dissemination		
LTA	Range of variation	> 25920	Maintainable	Low/Medium	Event/demand-driven	5/5	Yes
	Border Monitoring	72000					
	Target Tracking	2640		Low	Event-driven	4/5	Y/N
	Highway Monitoring	70090 - 96360	Maintainable	Medium		5/5	Yes
	Precision Agriculture	5208		Low	Demand-driven Time-driven	3/5	No
MTA	Structural Integrity Monitoring	26280		High	Event-driven Time-driven	3/5	No
	Range of variation	[721; 25920]	Maintainable	Medium	Event/time-driven		
	Water Monitoring	168		Low	Time-driven	3/5	No
	Smart Factory	30000		Medium	Event-driven Time-driven	3/5	No
	Forest Fire Detection	N.A.		Low		3/5	No
STA	Gaming	12648	Maintainable		Event-driven	2/5	No
	Dynamic Spaces	17520		Medium		4/5	Y/N
	Habitat Monitoring	5208		Low-Medium-High	Demand-driven Time-driven	4/5	Y/N
	Range of variation	[24; 720]	Maintainable	High	Event/time-driven		
	Personal Coaching	600		Low	Demand-driven Event-driven	3/5	No
STA	Weather Monitoring	1680			Demand-driven	3/5	No
	Monitoring	168		Medium	Demand-driven Event-driven	4/5	Y/N
	Volcanic Eruptions	72	Maintainable			4/5	Y/N
	Surveillance	1220		High	Event-driven	4/5	Y/N
	Condition-based Monitoring	179				5/5	Yes
STA	Wild-life Tracking	3					
	Range of variation	[24; 720]	Maintainable	High	Event/time-driven		
	Personal Coaching	600		Low	Demand-driven Event-driven	3/5	No
	Weather Monitoring	1680			Demand-driven	3/5	No
	Monitoring	168		Medium	Demand-driven Event-driven	4/5	Y/N
STA	Volcanic Eruptions	72	Maintainable			4/5	Y/N
	Surveillance	1220		High	Event-driven	4/5	Y/N
	Condition-based Monitoring	179				5/5	Yes
	Wild-life Tracking	3					
	Range of variation	[24; 720]	Maintainable	High	Event/time-driven		

For larger network sizes the networks are more robust and therefore aiming at long-term WSN applications. Tables 2.13, 2.15 and 2.17 consider the positive matches ratio corresponding to the WSN application for a specific category (i.e., how many parameters correspond to the attribute or value for such application category). Another column (i.e., the right hand side column) shows if the WSN application belongs (or not) to the respective category. Apart from “Yes” or “No”, this column presents the attribute “Y/N”. This attribute means that the WSN application nearly fulfils all the necessary attributes to belong to the category.

Table 2.13 presents different WSN applications organized among the LTA, MTA and STA categories, which aggregate the WSN applications with common parameters. It is noticeable that, for the LTA category, both border monitoring (military area) and highway monitoring (metropolitan area) share the same attributes and values. Even though these applications are from different areas, the combination of these parameters envisages a long-term solution application.

For the MTA category, the aggregation of WSN applications has not resulted in full positive match of the parameters. However, dynamic spaces (entertainment area) and habitat monitoring (environmental area) are applications which almost fulfil all the requirements of medium-term applications. Again, different application areas belong to the same time related category but each application envisages different purposes.

In the STA category, wild-life tracking (position and animals tracking area) positively matches all the characterization parameters attributes and values from this category, and is a typical short-term application. This is due to limited lifetime and small scalability of the hardware attached to the animal, being tracked along with the high reporting data rate. Other WSN applications, such as monitoring volcanic eruptions, surveillance and condition-based monitoring do not fully match the attributes and values for the parameters from this category. However, these applications can be assumed as nearly short-term ones.

The second group of three categories considers the data stream related constraints of applications. In this group, the service components, and data rate parameters are combined, enabling to form up the three new categories. The applications can be classified as High Data Stream Applications (HDS), Medium Data Stream Applications (MDS), and Low Data Stream Applications (LDS), as shown in Table 2.14.

The objective of Table 2.14 is to organize the WSN applications into one of the three categories, which are relate to the data stream in WSNs. In this table, it is enough to consider only two parameters. With this categorization, the intention is to help on the quick identification of the set of WSN applications whose primary concern is the bit rate. By identifying the intended WSN application, it is possible to analyse in detail a project that may serve as a basis for further research work. The service components parameter enables to distinguish the types of traffic that are expected to be present in a WSN application (depending on the application area). The most bandwidth demanding WSN applications consider the types of traffic with the widest requirements in terms of bandwidth, such as the Data-HID, Video-STV and Audio-VOI. In turn, the lowest bit rates are associated to the types of traffic with the lowest requirements in terms of

Table 2.14: Categories for data stream related applications.

Parameters	Category		
	HDS	MDS	LDS
Service components	Data-HID/ Video-STV/ Audio-VOI	Data-MED	Data-LOD
Bit rate	High Bit rate ≥ 115.2 kbps	Medium Bit rate [57.6; 115.2] kbps	Low Bit rate ≤ 57.6 kbps

Table 2.15: Aggregation of WSN applications for data stream related categories.

		Parameters		Positive matches ratio	Belongs to the category
	Applications	Service components	Bit rate (kbps)		
HDS	Range of variation	HID/STV/VOI	High bit rate (≥ 115.2)		
	Immersive Roam	STV-HID	Low bit rate	1/2	No
	Smart Roads	HID		1/2	No
	Real-Time Relative Positioning System		High bit rate	2/2	Yes
	Telemedicine			2/2	Yes
	Dynamic Spaces			2/2	Yes
	Highway Monitoring	STV-LOD MED-HID		2/2	Yes
MDS	Range of variation	MED	Medium bit rate ([57.6; 115.2])		
	Border Monitoring	MED	Low bit rate	1/2	No
	Habitat Monitoring			1/2	No
	Sensor & Robots			1/2	No
	Forest Fire Detection	LOD	Medium bit rate	1/2	No
	Gaming	MED		2/2	Yes
Personal Coaching	High bit rate		1/2	No	
LDS	Range of variation	LOD	Low bit rate (≤ 57.6)		
	Smart Office	MED	Low bit rate	1/2	No
	Weather Monitoring	LOD		2/2	Yes
	Precision Agriculture			2/2	Yes
	Warehouse Tracking			2/2	Yes
	Automobile			2/2	Yes
	Smart Factory	HID		1/2	No

bandwidth. The bit rate is related to the service components parameter, which also defines the category in Table 2.14. Hence, low, medium and high bit rates correspond to the LDS, MDS and HDS categories from Table 2.16, respectively. The addition of more parameters to Table 2.14 might help the reader but we consider that these two WSN characterization parameters are the most prominent and essential ones in terms of data stream.

Table 2.15 considers data stream related categories for different WSN applications and the relations among different applications areas. Typically, high data stream applications require higher bandwidth than other applications. Therefore, the real-time relative positioning system, telemedicine, dynamic spaces and highway monitoring applications are associated to the high data stream category. All these applications share the high bit rate and high demanding bandwidth traffic classes.

In the medium data stream category, the most common WSN applications are the ones related with monitoring events or associated to the user. These applications are medium bit rate applications and are associated to regular traffic sensor service components, i.e., MED. Note that the gaming application fulfils all the requirements of the medium data stream category. However, the remaining MDS applications from Table 2.15 only present one of the attributes. Either they present a MED service component or a medium bit rate. Low data stream applications present low bit rate jointly with low traffic sensor service components, i.e., LOD. Since the majority of the WSN applications use high reliability short packets of information, weather monitoring, precision agriculture, warehouse tracking and automobile applications present all the attributes from the low data stream category. Many of the WSN applications that belong to the MDS or LDS category are also part of the LTA and MTA categories from Table 2.12. This is due to the close relation between the attributes from the characterization parameters. Low event report and short packets lead to long or medium-term applications.

The third group is subdivided into two categories and refers to the delivery requirements and delay sensitivity of the applications. These categories include the interactivity, end-to-end connection, criticality, QoS, class of service, and traffic classes parameters. This group is subdivided into the Real-Time & Sensitive Delay Demanding Applications (RT-SDD) and Non Real-Time & non Sensitive Delay Demanding Applications (NRT-nSDD) categories, as shown in Table 2.16. To group WSN applications into one of the two categories from Table 2.16, the considered parameters are sufficient. These parameters have been chosen because timeliness issues must be addressed in the considered parameters for the delivery and delay sensitivity related categories. For these categories, the delay is an important issue. The provision of delay guarantees in WSNs is challenging due to sensor nodes' limitations in terms of energy supply, as well as computational and communication capabilities. The delay is the most critical delivery requirement parameter. Depending on the real-time (or non-real-time) nature of the WSN application, the QoS class parameter is also related to the delivery requirement. In real-time event-driven applications, the event needs to be reported to a sink node as soon as possible. In demand and periodic-driven WSN applications, real-time delivery may not be required. The end-to-end connection parameter is needed to identify if the WSN application presents a cooperative (non-end-to-end) or point-to-point (end-to-end) relationship among nodes. To assess if the WSN application is mission critical, the following two essential network performance metrics arise from the criticality parameter: delay and reliability. These metrics are discussed within the traffic class parameter from subsection 2.3.2. In addition, the class of service parameter is necessary to verify if the WSN applications adapts its bandwidth or not (ISO or NISO, respectively) and what type of data traffic is exchanged among nodes. This parameter is closely related with the QoS and traffic class parameters. The parameters considered in Table 2.16 are therefore enough to group WSN applications into one of these new categories.

Table 2.17 aggregates WSN applications according to timeliness aspects, which, in turn, are described by the assigning attributes or values to different parameters within the RT-SDD and NRT-nSDD categories. For the real-time and sensitive delay demanding category, the essential requirement is real-time delivery modelling. Additionally, WSN applications must be mission critical and non-delay tolerant. From the considered WSN applications, the border monitoring, personal coaching and gaming fulfil all the requirements from the RT-SDD category. However, other applications, such as (tele) rehabilitation, pre-hospitalar and immersive roam applications do not fully fulfil the requirements of this category, as they are nearly RT-SDD. Although the applications do not fully belong to the RT-SDD category, conclusions can be extracted regarding the similarities between applications from different areas that do and do not comply all the characterization parameters in a specific category.

Table 2.16: Categories for delivery and delay sensitivity related applications.

Parameters	Category	
	RT-SDD	NRT-nSDD
Delivery requirement	Real-time	Non real-time
End-to-End connection	End-to-end	Non end-to-end
Delay tolerance	Non delay tolerant	Delay tolerant
Criticality	Mission critical	Non mission critical
QoS	Event/Continuous/Demand driven	Query driven
Class of service	ISO&RT-VBR	ISO&CBR NISO&ABR NISO&UBR
Traffic classes	RT&LT&Data RT&LI&Data	DT&LI&Data DT&LT&Data

Table 2.17: Aggregation of WSN applications for delivery and delay sensitivity related categories.

Parameters										Positive matches ratio	Belongs to the category
Applications	Delivery requir.	End-to-end connection	Delay tolerance	Criticality	QoS	Class of service	Traffic classes				
RT-SDD	Range of variation	RT	End-to-end	Non delay tolerant	Mission critical	Event/ continuous/ demand -driven	ISO&RT-VBR	RT&LT&Data RT&LI&Data	7/7	Yes	
	Border Monitoring (Tele)	RT	End-to-End	Mission Critical	Event-driven	ISO&RT-VBR	RT&LT&Data	RT&LT&Data	6/7	Y/N	
	Rehabilitation		Both		Query-driven				RT&LI&Data	6/7	Y/N
	Pre-Hospitalar		End-to-end		Query & event-driven					7/7	Yes
	Personal Coaching		End-to-end		Event-driven				7/7	Yes	
	Gaming		Non End-to-End			RT&LT&Data	6/7	Y/N			
Immersive Roam					RT&LI&Data						
NRT-nSDD	Range of variation	NRT	Non End-to-end	Delay tolerant	Non mission critical	Query-driven	ISO&CBR NISO&ABR NISO&UBR	DT&LI&Data DT&LT&Data			
	Weather Monitoring	NRT	Non End-to-end	Delay tolerant	Mission critical	Query-driven	ISO&CBR	DT&LT&Data	6/7	Y/N	
	Condition-based		End-to-end		Non mission critical	Event-driven	ISO&CBR	DT&LT&Data	5/7	No	
	Monitoring		End-to-end		Mission critical	QoS-driven			4/7	No	
	Water		Both		Mission critical	Query & event-driven			6/7	No	
	Precision Agriculture	RT	Non End-to-end		Mission critical			DT&LI&Data	6/7	No	
	Forest Fire Detection		End-to-end						5/7	No	
	Wild-life Tracking	Both	End-to-end		Non mission critical	Event-driven	NISO&ABR	-	4/7	No	

The non-real-time and non-sensitive delay demanding category aggregates WSN applications that are not characterized by a real-time delivery model. Instead, these applications are based on a delivery model that relies on queries. This allows the WSN applications to be assumed as delay tolerant and tolerant to packets losses. In Table 2.17, there is no application that fulfils all the requirements for this category. However, weather monitoring positively presents all the requirements, except criticality, as it assumes the application is mission critical instead of non-mission critical. The remaining applications in the NRT-nSDD category do not fulfil all the requirements for this category. However, being non real-time is one of the main characteristics for this category.

On the one hand, the majority of WSN applications from the NRT-nSDD category are associated to the LDS category from Table 2.15. On the other, the WSN applications from the RT-SDD category are associated to the MDS and HDS categories from Table 2.15. This is due to the real-time nature from the RT-SDD category, which is usually related to wider bandwidth requirements.

2.4.3 Example for the WSN Applications Taxonomy

In order to better understand how the taxonomy can be applied, in this section, we present a description of twelve applications from different areas and categories. The remaining taxonomy tables for all the WSNs applications of Tables 2.10 and 2.11 are presented in Appendix B.

metropolitan, military, environment monitoring, position & animal tracking, industrial automation, health, civil engineering, environmental monitoring, logistics, transportation, automobile, and sports. Real-world WSN implementations of the presented applications are the highway monitoring, condition based monitoring, monitoring of volcanic eruptions, immersive roam, smart factory, telemedicine, structural integrity monitoring, forest fire detection, target tracking, smart roads, automobile and sports, respectively.

Table 2.18: Service characterization parameters of WSN applications (I).

Application Area	Metropolitan	Military	Environmental monitoring
Project	Traffic Dot [CV07]	WiBeaM [JR07]	Reventador volcano [WALJ ⁺ 06], [WAJR ⁺ 04]
Application	Highway monitoring	Condition based monitoring	Monitoring volcanic volcanic eruptions
Delivery requirements	RT & NRT	NRT	RT
Directionality	Bid	Bid	Bid
Communication symmetry	Sym	Sym	Sym
End-to-end connection	Non end-to-end	End-to-end	Non end-to-end
Interactivity	Interactive	Interactive	Interactive
Delay tolerance	Non delay tolerant	Delay tolerant	Delay tolerant
Criticality	Mission critical	Non mission critical	Mission critical

Tables 2.18, 2.19, 2.20 and 2.21 present the values for the attributes for the studied applications, whilst considering the service classification parameters, from our proposed taxonomy. In terms of service parameters the applications are organized as follows:

- **Delivery requirements** - All presented applications need a real-time delivery demand, except for the condition based monitoring, since it is not critical to have the data from the sensors available in a continuous mode. Highway monitoring also presents non-real-time delivery in some types of data (e.g., counting cars).

Table 2.19: Service characterization parameters of WSN applications (I) (cont.).

Application Area	Position & animals tracking	Industrial automation	Health
Project	LEMe Room [LEM]	Anshan [WLH ⁺ 08]	MEDiSN [KLC ⁺ 10]
Application	Immersive room	Smart factory	Telemedicine
Delivery requirements	RT	RT	RT
Directionality	Bid	Bid	Bid
Communication symmetry	Asym	Sym	Asym
End-to-end connection	Non end-to-end	End-to-end	End-to-end & Non end-to-end
Interactivity	Interactive	Interactive	Interactive
Delay tolerance	Non delay tolerant	Delay tolerant	Non delay tolerant
Criticality	Mission critical	Mission critical	Mission critical

Table 2.20: Service characterization parameters of WSN applications (II).

Application Area	Civil engineering	Environmental monitoring	Logistics
Project	Sustainable Bridges [BEOiRTUE07]	FireBug [ASSDGC08], [ASSdGC06]	VigilNet [HKL ⁺ 06]
Application	Structural integrity	Forest fire	Target tracking
Delivery requirements	RT & NRT	RT	RT
Directionality	Bid	Bid	Bid
Communication symmetry	Sym	Sym	Sym
End-to-end connection	Non end-to-end	Non End-to-end	Non end-to-end
Interactivity	Interactive	Interactive	Interactive
Delay tolerance	Delay tolerant	Delay tolerant	Non Delay tolerant
Criticality	Mission critical	Mission critical	Mission critical

Table 2.21: Service characterization parameters of WSN applications (II) (cont.).

Application Area	Transportation	Automobile	Sports
Project	AstroRoads [Mar04], [Ast]	Intelligent Tires [ESVS ⁺ 09]	DexterNet [KGG ⁺ 09]
Application	Smart Roads	Automobile	Sports
Delivery requirements	RT & NRT	RT	RT
Directionality	Bid	Bid	Bid
Communication symmetry	Sym	Sym	Asym
End-to-end connection	Non end-to-end	End-to-end	Non end-to-end
Interactivity	Interactive	Non interactive	Interactive
Delay tolerance	Non delay tolerant	Delay tolerant	Non delay tolerant
Criticality	Mission critical	Mission critical	Non mission critical

- **Directionality** - All the applications presented in Tables 2.18, 2.19, 2.20 and 2.21 are bidirectional.
- **Communication symmetry** - In terms of communication symmetry parameters, both categories C1WSNs and C2WSNs have applications that share the same attribute for this parameter. Highway monitoring, condition based monitoring, monitoring of volcanic eruptions, smart factory, structural integrity monitoring, forest fire detection, target tracking, smart roads and automobile applications are symmetric, whereas, immersive room, telemedicine and sports are asymmetric applications. This asymmetry is caused by fluctuations in the data quantities that may occur during the execution of the application.

- **End-to-end connection** - The military and industrial automation areas from different categories (C1WSNs and C2WSNs, respectively) share the need for an end-to-end guarantee. Also, in telemedicine an end-to-end connection may also be needed or not, depending on the type of data being sent by the nodes. In turn, the highway monitoring, monitoring of volcanic eruptions, immersive roam, structural integrity monitoring, forest fire detection, target tracking, smart roads, automobile and sports applications do not require an end-to-end connection, in order to fulfil the requirements of the application.
- **Interactivity** - All the presented applications are interactive, except for the automobile application. In this application the data is reported almost continuously.
- **Delay tolerance and criticality** - The delay tolerance and criticality parameters are deeply related with each other. By observing Tables 2.18, 2.19, 2.20 and 2.21, the majority of the presented applications that are non delay tolerant are also mission critical. Only a few applications, like smart factory, monitoring of volcanic eruptions, structural integrity monitoring and forest fire detection are simultaneously delay tolerant and mission critical ones. Usually, the demand for non delay tolerance is a characteristic of real-time applications, while the mission criticality relies on the importance of the data being sent aiming at meeting a certain application requirement.

The traffic characterization parameters of the presented applications are shown in Tables 2.22 and 2.23. Details are as follows:

- All the presented applications employ a stand-alone event-driven data delivery model or a hybrid model that combines two schemes (e.g., event-driven and query-driven hybrid model) for QoS parameter.
- The bit rate parameter characterizes the application demand for high or low data packets transmission. All the applications have low bit rates in common, except telemedicine, either due to energy restrictions or to a pre-established optimal working point stated by its designers. These low bit rates guarantees an efficient tradeoff between the energy and data delivery.
- The volcanic eruptions monitoring application presents the highest maximum delay, as shown in Table 2.22, and is delay tolerant. However, although the condition based monitoring is tolerant to delays too, its maximum allowed delay is lower than the previous one. This is explained by the surrounding environment where the application is going to be deployed. Despite the seemingly harsh volcanic environment, it is comprehensive the presented maximum delay value of the monitoring of volcanic eruptions application.

Tables 2.22 and 2.23 presents the communication parameters for the considered WSN applications. Details are as follows:

- **Synchronization** - All the presented applications require synchronized communications, except for the structural integrity monitoring applications which does not requires synchronized communications. The sports application considers both synchronized and asynchronized communications, since it depends on the type of sport being monitored.
- **Class of service** - The class of service and traffic classes are related with the delay tolerance. Figure 2.2 sheds light on how the different service classes are assigned to the corresponding application. Since the immersive roam, telemedicine and sports applications present fluctuations in the data packet transmission and have a real-time delivery

requirement, the class of service is ISO&RT-VBR. Although the structural integrity monitoring application does not presents an asymmetric characteristic it assumes the class of service ISO&RT-VBR. For the remaining applications, the class of service is ISO&CBR, as shown in Tables 2.22 and 2.23.

- **Traffic class** - All the WSN applications transmit the data traffic class. The differences among the applications rely on the delay and loss tolerance. The highway monitoring, immersive roam, telemedicine and target tracking applications are real-time applications. However, only the telemedicine and target tracking applications are packet loss intolerant. This is because of the importance of the data being transmitted. The remaining real-time applications are loss tolerant except for the forest fire detection and automobile applications, since either data can be retransmitted or the reporting frequency is high enough to guarantee a reliable data delivery. The forest fire detection and automobile applications are delay tolerant and loss intolerant. The condition based monitoring, monitoring volcanic eruptions, smart factory, forest fire detection and automobile applications are tolerant to delay. Despite this fact, only the first two aforementioned applications are packet loss tolerant.
- **Modulation** - The most common modulation in the applications addressed in this work is the FSK(DSSS) one, because it is easily supported by simple radio transceivers. However, in the condition based monitoring and target tracking applications, the applied modulation scheme is DSSS-O-QPSK, which is IEEE 802.15.4 compliant.
- **Communication direction** - The communication direction depends on the number of radio transceivers used. If the sensor nodes of the application utilize more than one radio transceiver (if they support full duplex), all the addressed applications are half-duplex, since only one radio transceiver is used in each sensor node.

Tables 2.22 and 2.23 present the service components for the considered WSN applications. Details are as follows:

- **Type of traffic** - The applications addressed in this work exchange HID traffic, except for the condition based monitoring, forest fire detection, target tracking and automobile applications which only exchange LOD traffic as shown in the rows for the service components from Tables 2.22 and 2.23. Besides, the highway monitoring application includes the three types of traffic (LOD, MED, HID) and STV in which highway surveillance is supported by video streaming. The telemedicine application also includes this type of traffic (STV), since video streaming can also be transmitted.
- **Packet delivery failure ratio** - The packet delivery failure ratio QoS parameter is of paramount importance. All the applications present values lower than 10% for the PDFR parameter.
- **Data acquisition and dissemination** - All the studied applications from the acquisition and dissemination classes are event-driven or a combination of event-driven with another class. Only the telemedicine application corresponds to a demand-driven and time-driven class. Telemedicine only transmits data on demand (or by following a defined reporting frequency).

The network parameters presented in Table 2.22 and 2.23 facilitate to understand the impact of the choice of certain attributes or values for the parameters from Tables 2.18, 2.19, 2.20 and 2.21. Details are as follows:

Table 2.22: Traffic, Communications, service components, network and node parameters for WSN applications (I).

Application Area	Metropolitan	Military	Environmental monitoring	Position & animals tracking	Industrial automation	Health
Project	Traffic Dot [CV07]	WiBeAM [JR07]	Reventador volcano [WALJ ⁺ 06], [WAJR ⁺ 04]	LEMe Room [LEM]	Anshan [WLH ⁺ 08]	MEDISN [KLC ⁺ 10]
Application	Highway monitoring	Condition-based monitoring	Monitoring volcanic eruptions	Immersive roam	Smart factory	Telemedicine
QoS	Collective QoS (Event-Driven)	Collective QoS (Event-Driven)	Collective QoS (Event-Driven)	Collective QoS (Event-Driven)	Collective QoS (Event-Driven & Query-driven)	Collective QoS (Event-Driven)
Bit rate (kbps)	≤ 57.6	≤ 57.6	≤ 57.6	≤ 57.6	≤ 57.6	≥ 115.2
Latency	$T_{min} = 1$ s $T_{max} = 2$ s	$T_{max} = 0.00867$ s (per packet)	$T_{max} = 63$ s (per hop)	$T_{max} = 3$ ms	$T_{min} = 80$ ms $T_{max} = 250$ ms	$T_{max} = 7-8$ ms
Synchronization	Sync	Sync	Sync	Sync	Sync	Sync
Class of service	ISO&CBR	ISO&CBR	ISO&CBR	ISO&CBR	ISO&CBR	ISO&CBR
Traffic classes	RT&LT&Data	DT&LT&Data	DT&LT&Data	RT&LT&Data	DT&LT&Data	RT&LT&Data
Modulation	FSK(DSSS)	DSSS-O-QPSK	FSK	FSK(DSSS)	GFSK or MSK/OOK	FSK
Communication direction	Half-duplex	Half-duplex	Half-duplex	Half-duplex	Half-duplex	Half-duplex
Type of Traffic	STV; LOD MED; HID	LOD	HID	HID	HID	STV; HID
Packet delivery failure ratio	1%	9%	4.96%	N.A.	$\leq 10\%$	6.3%
Acquisition & dissemination classes	Event-driven	Event-driven	Demand-driven & event-driven	Demand-driven & event-driven	Event-driven & time-driven	Demand-driven & time-driven
Lifetime (h)	≥ 25920	[721; 25920]	[24; 720]	[24; 720]	≥ 25920	N.A.
Scalability	[51; 400] nodes	≤ 50 nodes	≤ 50 nodes	≤ 50 nodes	> 400 nodes	≤ 50 nodes
Density	N.A.	N.A.	3 km ²	450 m ²	3000 m ²	N.A.
Sensing range	N.A.	Local	Local	2 m ²	< 1 m ²	local
Self-organization	Entire network	Entire network	Entire network	Entire network	Entire network	Entire network
Security	Low	Low or none	Low	Medium	None	None
Addressing	Address-centric: MAC address	Address-centric: MAC address	Address-centric: MAC address	Address-centric: node ID	Address-centric: node ID, group ID, cluster ID	Address-centric: address number
Programmability	Not programmable	Not programmable	Not programmable	Programmable	Not programmable	Not programmable
Maintainability	Maintainable	Maintainable	Maintainable	Not maintainable	Maintainable	Not maintainable
Homogeneity	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous
Mobility support	No support	No support	No support	Support	No support	Support
Microprocessor	ATMEL (ATmega 128L)	TI (MSP430F1611)	ATMEL (ATmega 128L)	ATMEL & Microchip (ATmega 128L) & (PIC16F872)	ATMEL (ATmega 128L)	TI (MSP430F1611)
Transceiver	CC1100	CC2420	CC1000 (433 MHz)	CC1000 (900 MHz)	CC1000 (900 MHz)	CC2420
Overall energy consumption	0.01044 A	0.0612 A	0.038 A	0.0520 A	0.072503 A	0.040955 A
Sampling rate	[100; 1000] Hz	> 1 kHz	[100; 1000] Hz	> 1 kHz	[100; 1000] Hz	[0.001; 100] Hz
Type of function	Sensor & sink	Sensor & sink	Sensor & sink	Sensor & sink	Sensor & sink + gateway	Sensor & sink
Communication range	5.5 m	10 m	10.7 m	305 m	400 m	> 5 m
Power supply	Battery	Battery	Battery	Battery & local supply	Battery	Battery

Table 2.23: Traffic, Communications, service components, network and node parameters for WSN applications (II).

Application Area	Civil engineering	Environmental monitoring	Logistics	Transportation	Automobile	Sports
Project	Sustainable Bridges [BEOiRTUE07]	FireBug [ASSDGC08], [ASSdGC06]	VigilNet [HKL ⁺ 06]	AstroRoads [Mar04], [Ast]	Intelligent Tires [ESVS ⁺ 09]	DexterNet [KGG ⁺ 09]
Application	Structural integrity monitoring	Forest fire detection	Target tracking	Smart roads	Automobile	Sports
QoS	Collective QoS (Event-Driven)	Collective QoS (Event-Driven & Query-Driven)	Collective QoS (Event-Driven)	Collective QoS (continuous) individual specific	Hybrid model	Collective QoS (Event-Driven)
Bit rate (kbps)	≤ 57.6	[57.6; 115.2]	≥ 115.2	≤ 57.6	≤ 57.6	≥ 115.2
Latency	$T_{min} = 400$ ms $T_{max} = 1500$ ms	$T_{min} = -$ $T_{max} = 2$ s	$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = 130$ s	$T_{min} = -$ $T_{max} = 2.9$ s	$T_{min} = -$ $T_{max} = -$
Synchronization	Async	Sync	Sync	Sync	Sync	Sync and Async
Class of service	ISO&RT-VBR	ISO&CBR	ISO&RT-VBR	ISO&RT-VBR	ISO&CBR	ISO&RT-VBR
Traffic classes	RT&LT&Data	DT&LT&Data	RT&LT&Data	RT&LT&Data	DT&LT&Data	RT&LT&Data
Modulation	FSK(DSSS)	FSK	DSSS-O-QPSK	FSK(DSSS)	FSK(DSSS)	DSSS-O-QPSK
Communication direction	Half-duplex	Half-duplex	Half-duplex	Half-duplex	Half-duplex	Half-duplex
Type of Traffic	HID	LOD	LOD	HID	LOD	HID
Packet delivery failure ratio	-	-	1%	0.1%	4%	-
Acquisition & dissemination classes	Event-driven & Time-driven	Event-driven & Time-driven	Event-driven	Event-driven & event-driven	Event-driven & time-driven	Event-driven
Lifetime (h)	≥ 25920	[24; 720]	[721; 25920]	N.A.	[24; 720]	N.A.
Scalability	N.A.	≤ 50 nodes	> 400 nodes	≤ 50 nodes	≤ 50 nodes	≤ 50 nodes
Density	-	3 km ²	50 km ²	N.A.	0.17 m ²	16 m ²
Sensing range	10-52 m ²	Local	200 m ²	N.A.	< 1 m ²	< 1 m ²
Self-organization	Entire network	Entire network	Entire network	Entire network	Entire network	Entire network
Security	Low	Low	None	None	None	None
Addressing	Address-centric: MAC address	Address-centric: MAC address	Address-centric: MAC address	Address-centric: node ID	Geographic addressing scheme	Address-centric: node ID
Programmability	Programmable	Not programmable	Programmable	Programmable	Not programmable	Programmable
Maintainability	Maintainable	Maintainable	Maintainable	Maintainable	Maintainable	Maintainable
Homogeneity	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous
Mobility support	No support	No support	No support	No support	Support	Support
Microprocessor	TI (DSP 8-bit)	ATMEL (ATMega 128L)	TI (MSP430)	ATMEL & Microchip (ATMega 128L)	ATMEL (ATMega 128L)	ATMEL (ATMega 8)
Transceiver	CC2420	CC1000	CC2420	CC1000	CC1000	CC2420
Overall energy consumption	0.053 A	0.036 A	0.0351 A	0.045 A	0.0346 A	0.0289 A
Sampling rate	> 1 kHz	[100; 1000] Hz	[0.001; 100] Hz	N.A.	N.A.	[0.001; 100] Hz
Type of function	Sensor & sink	Sensor & sink	Sensor & sink + gateway	Sensor & sink + actuator	Sensor & sink	Sensor & sink + gateway
Communication range	10-30 m	10.7 m	125 m	305 m	140 m	10 m
Power supply	Battery	Battery	Battery Solar panel	Battery	Battery	Battery

- **Lifetime** - Highway monitoring, smart factory and structural integrity monitoring present the longest lifetime, even though presenting a real-time delivery, which can be misleading to assume the ones with the highest energy consumption. These applications present a long lifetime because of the low reporting frequency (i.e., ultra low duty cycles). The remaining applications present short or medium lifetime, due to the high or medium reporting frequency. These higher reporting frequency correspond to more energy drain.
- **Scalability** - Outdoor applications (e.g., highway monitoring and target tracking) present the highest level of scalability, while the ones related with indoor environments present the lowest scalability. Despite this fact, some indoor deployments applications present high scalability, in order to better cover the indoor environment.
- **Self-organization and homogeneity** - The self-organization and homogeneity parameters are equal in all the presented applications.
- **Security** - The applications shown in Tables 2.22 and 2.23 present minimum security level or even no security. This is justified by the increased complexity that is added to the WSN when a security mechanism is considered (along with the increase of the energy consumption). Only the immersive roam application presents medium security level, since it is a recent application.
- **Addressing** - All the applications consider an addressing scheme based on ID's, except the automobile application, which relies on geographic addressing.
- **Mobility support** - There are applications that require an adaptive mechanism (mobility support) to handle changes in the network due to the sensor or coordinator nodes movement. From the analyzed applications, immersive roam, telemedicine, automobile and sports applications include mobility support, since the devices can move around within the environment.

Finally, Tables 2.22 and 2.23 also mention important values and attributes for the node parameters, such as the type of microprocessor, type of power supply and radio transceiver, and gives an appropriate range of possible attributes or values that are expected for each application. The overall values presented for the energy consumption for the corresponding hardware and parameter configuration of an application are only indicative. Details are as follows:

- **Microprocessor** - In off-the-shelf sensor node solutions, the microprocessors more commonly used are the ones from the ATMEL brand but Texas Instruments (TI) microprocessor are also considered. Details are given in Tables 2.5 and 2.6 from section 2.3.6.
- **Transceiver** - As aforementioned, the chosen modulation depends on the type of radio transceiver used in the envisaged application. Applications that use the CC2420 radio transceiver are compliant with IEEE 802.15.4, while the remaining ones are non-compliant.
- **Sampling rate** - Since the sampling rate is deeply related with the application lifetime, higher sampling rates generally correspond to applications with short lifetime. On the other hand, the ones with low sampling rate may lead to longer lifetime (note however that the sampling rate is not the only parameter that influences the lifetime of a sensor node).

- **Type of function** - In these projects, the sensor nodes perform mainly simple sensor and sink tasks. In some cases, there is a sink with extended capabilities that allows for connecting the network to the Internet. In the smart roads application the sensor node can also actuate a device, beyond the normal tasks of sensing and reporting data to the sink node.
- **Communication range** - The communication range considerably depends on the type of radio transceiver, the transmission power and frequency band. The applications that utilize a radio transceiver with a low frequency band have a wider communication range.
- **Power supply** - All applications use batteries as the power supply for the sensor nodes, except for the sink node with extended processing capabilities (e.g., immersive room). In target tracking, the sensor nodes use energy harvesting devices (i.e., solar panels jointly with batteries).

2.5 WSN Applications Roadmap and Trends

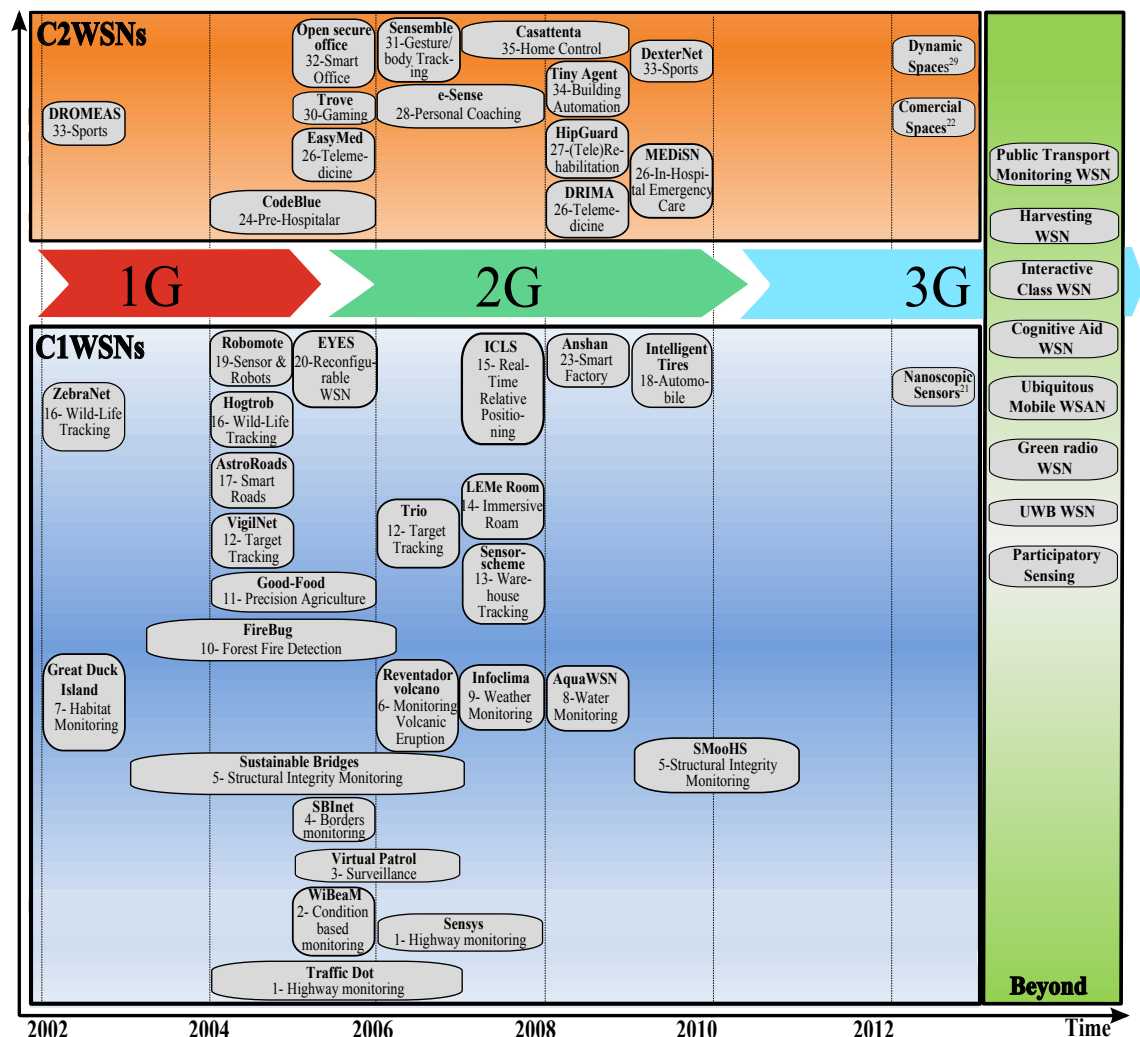


Figure 2.9: WSN applications roadmap and future trends.

This section discusses the chronological evolution for all the highlighted WSN areas for the past 10 years. Key approaches from relevant projects are addressed. The intention is to provide a

significant evidence of the usefulness of WSNs in various areas. In fact, it is difficult to identify one application area that cannot benefit from the WSN technology. In addition, the evolution path towards new WSN application areas is discussed together with future trends. Figure 2.9 organizes the considered WSN applications from Tables 2.10 and 2.11 in a chronological manner. The WSN projects considered in from this taxonomy are ordered by their duration (X axis) and category, either CW1WSNs or CW2WSNs (Y axis). It is worthwhile to note that the majority of the surveyed WSN projects occurred between 2004 and 2008. In addition, Fig. 2.9 allows for observing that there are few recent WSN projects. However, the new trends in WSN applications will allow the development of more WSN projects beyond the state-of-the-art. By analyzing Fig. 2.9 and the different parameters in Tables 2.18, 2.19, 2.20, 2.21, 2.22 and 2.23, it is possible to divide WSN applications into three generations.

The first generation (1G) of WSNs is characterized by applications that are considered as isolated and self-contained systems with a WSN gateway (i.e., sink node) as the only node that interacts with the user. In other words, the network centralizes all the data to a central node which delivers the information to the user. The main requirements for the 1G of WSN applications are the following ones:

- Non real-time delivery is required;
- Non end-to-end connection;
- Mission critical absent;
- No QoS support;
- Simple interaction;
- Low data rate;
- No security;
- Reduced scalability;
- Reduced lifetime;
- No mobility support;
- Mainly event or time-driven data acquisition model;
- Simple hardware.

The habitat monitoring application (from the environment monitoring area) is a representative example.

As the market needs and technology continue to evolve, new challenges have been posed to the field of WSNs, and the second generation (2G) of WSNs emerged. 2G is characterized by heterogeneous WSNs, whose sensor networks are seen as service providers. Additionally, the interaction over Internet is enabled, in order to offer a richer and more complex set of services and information to the end users [AHS06],[GBM⁺08],[KS09]. The main requirements for the 2G of WSN applications are the following ones:

- Support of real-time applications;
- Need for more robust system operation;
- Support for heterogeneous networks;

- Inclusion of security support and mechanisms;
- Privacy;
- Control and actuation;
- Support of different types of traffic sources;
- QoS support;
- Mission criticality support;
- End-to-end connection support;
- More complex, and more efficient hardware;
- High data rate support;
- Interaction with feedback (when actuation is involved).

As the years pass by, the popularity of WSNs and Machine-to-Machine (M2M) communications has been growing. This evolution has brought up this new class of network traffic[PP11]. WSNs benefit from the increase in the mobile network penetration over the world as well as the increase in the complexity of the mobile devices. This is achieved by extending the functionalities of each mobile phone, allowing for sensing and gathering information from the environment surrounding the mobile phone user[BEH⁺06],[GSB⁺09],[SHB⁺06]. The M2M communication can be used to connect individual machines and devices over Internet and mobile networks. As such, mobile network operators may offer services that facilitate the use of M2M over mobile networks, while generating additional profit. Until the second generation of WSN applications, the networks did not have suitable openness to the common user. Only experts were able to manipulate and change the WSN behaviour and functionalities. Currently, there is a need for new WSN applications to open up WSNs. This need motivates the creation of macroprogramming frameworks, in order to provide a set of standardized interfaces solutions, services and protocols that allow for an easier interaction between devices in a heterogeneous network, whilst facilitating the role of the applications designer. By opening up WSNs a more reliable and easier integration of WSNs with higher layers networks in the hierarchy will be possible. This integration facilitates the creation of new services whilst enhancing solutions for smart cities, smart homes and smart roads. This new class of network traffic corresponds to the third generation of WSNs (3G), in which the term *things* is introduced, referring to different devices with a unique identification. The communication between *things* drives the need of having traffic characteristics different from the traditional human-centric communications. It is expected, as stated before, that M2M and WSNs services use other higher layers mobile networks (e.g., 3G, LTE) as a backhaul. This conceptual scenario is known as the Internet of *Things* (IoT)[oro09]. The IoT delivers one of the most important and envisioned novelties of 3G applications: the inclusion of context information awareness about the surrounding environment, whilst making it available to all users in a traditional manner, like the nowadays Internet services availability. These new WSN applications will be connected with *things* to the Internet, by means of mobile network technologies, which serve as a backbone. Since the new WSN applications will be more Internet-dependent via mobile networks, the operators should reinforce their mobile structures in order to support the new kind of traffic class generated by WSNs, machines and, in general *things*. This is an important aspect since the number of *things* is expected to grow significantly[ERI],[CIS], and soon will exceed the number of mobile phone human subscribers.

The 3G of WSN applications (compared with the previous ones) includes all the requirements from 2G plus the new features that have been highlighted before.

Examples of third generation WSN applications also include the heating, ventilation and air-conditioning control (HVAC) applications. HVAC encompasses the monitoring and control of industrial and residential buildings over Internet. These applications are part of smart cities, a 3G scenario in WSN applications. In smart cities, mobile networks work as the backbone that allows for remotely monitoring and controlling buildings with no fixed communication link.

The educational application is another 3G WSN area, more specifically the Interactive class room application. This type of application typically sends periodic updates containing a small amount of data[Sen].

Other types of WSN applications are related with cognitive radios. A cognitive radio is able to behave, in a certain manner, as a cognitive system, meaning that it has, at least, capabilities of observing, decision making, and adapting. Since, the licensed spectrum allocation approach is regarded as old fashioned, due to the static resource allocation, which leads to spectrum inefficiency, cognitive radios improve spectrum utilization by seeking and opportunistically utilizing radio resources on a real-time basis in the time, frequency, and space domains. The emergence of the cognitive radio technology results in numerous advantages for WSNs, including economic benefits, as well as solving coexistence, interference management and interoperability issues. Several works have addressed cognitive radio issues in the context of WSNs, including spectrum sensing, coexistence mechanisms, environment awareness, etc. An example of a WSN application with cognitive capabilities is the cognitive aid WSN application. It senses all the traffic from a higher network layer system (e.g., 3G network) and transmits the sensed data to the base station, in order the mobile network is able to tweak its quality parameters. Here, the WSN alleviates the base station in terms of traffic quality assessment, increasing the efficiency of all the mobile network whilst reducing the energy consumption from the base station.

Another 3G WSN application area is the ubiquitous mobile WSN. This application area enables WSNs with sensing and actuation capabilities to interact with ubiquitous computing, leading to a variety of applications with pervasive physical world instrumentation requirements (e.g., environment monitoring, logistics, smart buildings, etc). In order to support the required sustainability, mobility, scalability, and dynamic adaptation of the application, several domains that are common in the first generation WSN are now re-modelled or re-designed.

Green radio communications will facilitate an efficient energy utilization in Information and Communication Technology (ICT) platforms (e.g., Internet or mobile or wireless technologies) that support 3G WSNs. Associated to green radio communications is the harvesting WSN applications that employ harvesting devices in the sensor nodes to scavenge for energy from different types of sources (e.g., solar, thermal, kinetic, etc).

Participatory sensing is also a new type of WSN application which makes use of everyday mobile devices (such as mobile phones), to form an interactive and participatory sensor networks, by enabling public and professional users to collect, analyze and share knowledge from a specific location. The objective is to allow people to be more aware of the surrounding environment where they are inserted in, while allowing participation at a personal, social and urban scales. This leads to a higher public concern about a certain subject and a higher conscious awareness [GSB⁺09],[SHB⁺06]. The five main applications areas of participatory sensing are the following ones: urban planning, public health, cultural identity and creative expression, and natural resource management.

Although the different WSN applications are spreading to new areas, the market for short-range, low power RF technologies in the 2.4 GHz ISM band is far from achieving maturity. As a conse-

quence, the new WSN applications are limited to the constraints imposed by the short-range transceivers hardware. The authors from [ERI] foresee that healthcare and personal fitness are going to be the areas where the low energy chips will be more frequently used. In the context of the Internet of *Things*, tiny Ultra Low Power (ULP) transceivers allow for thousands of devices to communicate while increasing the usefulness of each device. The authors from [Uni05] propose four enablers to the Internet of *Things*:

- **Tagging things** - enables real-time wireless/contactless identification and tracking;
- **Sensing things** - enables detection of environmental status and collection of varied data on physical parameters (velocity, presence of foreign objects, temperature, moisture);
- **Shrinking things** - smaller but smarter devices facilitates building intelligence into the edges of the network, and even in materials themselves;
- **Thinking things** - makes possible the networking of smaller and smaller objects.

Embedded intelligence (such as smart cities, homes, and so on), real-time monitoring (medical applications and environmental management), augmented reality and new Internet (Web 3.0) are certainly the major complimentary technologies to look forward to [Uni05]. In a context of convergence among different wireless communication technologies (RFID, GSM, 3G, WLAN, WiMAX, LTE), product identification solutions (barcodes, RFID), process control (sensor networks, home automation) and network interconnection (Ethernet, Internet) will be a reality.

2.6 Summary and Conclusions

The available information about the classification and characterization parameters of WSN applications in different areas has been put together enabling to obtain insights about possible applications requirements or possible outcomes from a specific WSN application area.

A taxonomy has been proposed for application characterization parameters, which are divided into main, traffic, communication, service components, network and node parameters. Typical values from related research works are considered as a reference. The proposed taxonomy for classification of the applications is centred on the different sets of parameters that have a high impact on a given future WSN application. A holistic overview of the relations (links) between different groups of classification, with the same value for a certain set of characterization parameters has been identified. These inter- and -intra-connections among the applications groups facilitate to understand how different WSN applications from different areas may share the same parameters values/attributes. Moreover, this holistic overview allow for understanding that other WSN applications which do not share the same parameters values are assumed as different among all the aforementioned WSN applications.

Based on the different inter- and intra-connections three new groups of applications characterization parameters can be defined. The first group is based on the time related constraints of the application (e.g., lifetime, scalability). Three possible categories are Long Term Applications (LTA), Medium Term Applications (MTA) and Short Term Applications (STA). The second group considers the data stream related constraints of application, such as service components and bit rate. It can be classified as High Data Stream Applications (HDS), Medium Data Stream Applications (MDS) and Low Data Stream Applications (LDS). The third group is related to the delivery requirements and delay sensitivity of the applications (e.g., QoS, criticality, interactivity). It is sub-divided into Real Time & Sensitive Delay Demanding Applications (RT-SDD) and Non

Real Time & non Sensitive Delay Demanding Applications (NRT-nSDD). Our review indicates that some of these new application categories are deeply related with each other. Many of the WSN applications that belong to the MDS or LDS category also belong to the LTA and MTA categories. Consequently, low event report and short packets lead to long or medium term applications. On the one hand, the majority of WSN applications from the NRT-nSDD category are associated to the LDS category. On the other, the WSN applications from the RT-SDD category are associated to the MDS and HDS categories. Note that it is a worth nothing that the real-time nature from the RT-SDD category is usually related to higher bandwidth requirements.

To complete the WSN application taxonomy, by characterizing WSN projects over the period of 2001-2011, a chronological comparison is presented for existing projects in all the highlighted areas, along with the evolution path towards new WSN application areas and future trends. Based on the vast fields of WSN applications as well as the proposed taxonomy, have been identified three generations. The first generation is characterized by applications within isolated and self-contained systems with a sink node. The second generation is characterized by heterogeneous WSNs, where sensor networks offer a richer and more complex set of services and information to the end users. This new class of network traffic gives the ground to bring to light the third generation of WSN, along with communication between *things*, with traffic patterns different from the traditional human-centric communications. This is known as the Internet of *Things*. With 3G, new fields of applications are appearing, such as interactive class room, cognitive aid WSN, ubiquitous mobile WSN, “green radio communications”, harvesting WSN and WBAN applications, as well as participatory sensing. With the Internet of *Things*, tiny Ultra Low Power (ULP) transceivers allow for thousands of devices to communicate among them while increasing the usefulness of each individual device.

Chapter 3

WSN Real World Applications and Scenarios

This chapter presents the instrumentation and sensor data dissemination solutions proposed and tested in real WSN scenarios and is organized into three parts: Section 3.1 is dedicated to the foetal movement monitoring application (Smart-Clothing), Section 3.2 addresses the concrete structural integrity application (INSYSM Project), while Section 3.3 presents the precision agriculture application (InterNodal Network). Sections 3.1.1 to 3.1.3 starts by presenting the challenges followed by the experimental apparatus considered for the acquisition and dissemination of the foetal movement in the Smart-Clothing project. Finally, a summary and conclusions regarding the achievements of the project Smart-Clothing is presented in Section 3.1.4. The second part of this chapter regards the concrete structural integrity application in which the main goal is to develop an WSN-based automatic measurement system allowing for monitoring the temperature and humidity within civil engineering structures (Sections 3.2.1 to 3.2.6). The objective is to study and assess the concrete structure integrity. Some limitations and challenges for the INSYSM project are also discussed (Section 3.2.8), followed by summary and conclusions (Section 3.2.9). The third part of the chapter presents the precision agriculture application. The conception of an entire WSN for precision agriculture monitoring is discussed. The objective is to measure physical parameters (such as temperature, CO₂ level, moisture level and wind speed) from the surrounding environment in a vineyard, while triggering devices that are attached to sensor nodes. Experimental results are discussed in Sections 3.3.1 to 3.3.5 for outdoor and indoor scenarios, and finally, some conclusions are presented (Section 3.3.6). Appendices C and D address in depth some details regarding the aforementioned projects.

3.1 Smart Clothing for Foetal Movement Monitoring Application

3.1.1 Challenges

The Smart Clothing for Health Monitoring and Sport Applications (Smart-Clothing) project [Sma09] was an iCentro project approved by CCDR-C with FEDER funding. The methodological specifications applied in this project enables to quantify the precision of the experimental measurement with a new device for signal acquisition, develop algorithms to extract the parameters that show clinical relevance and to establish strategies for efficient data mining in the context of medical diagnostic of foetal health in pregnant women. From the conventional sensor and data acquisition and storage circuit's point of view, the objective is to develop a set of electronic microcircuits associated with textile materials that enable to measure relevant biomedical and biomechanical parameters through an easy-to-use telemedicine gear, e.g., a belt. One example of how the theme of pregnancy monitoring is gaining importance in the research community is mentioned by the authors from [EKP⁺06], which describes an innovative, remote monitoring decision support system, employed in the early diagnosis of pregnancy complications, through the effective and non-invasive monitoring of maternal and foetal electrocardiograms. A hierarchical communication system, as shown in Figure 3.1, is needed to deliver the data from the WBAN that is attached to pregnant woman. Note that, although the main focus of the Smart-Clothing

is to produce the sensors integrated into the clothes and to integrate them into the WBAN, the consideration of aspects of data aggregation, routing and MAC protocols were also important, as they facilitate the integration of WSNs into the hierarchical network. New algorithms and protocols were developed to optimize the trade-off between energy consumption/processing and communication capabilities, namely in the MAC layer [BVF⁺09]. Hierarchical communications can be a solution to obtain a network of networks, e.g., by using IP. A bottom-up architecture formed by i) WSNs, ii) Wi-Fi, and iii) Ethernet (or WiMAX) was explored to facilitate healthcare monitoring anyway, anywhere and anytime.

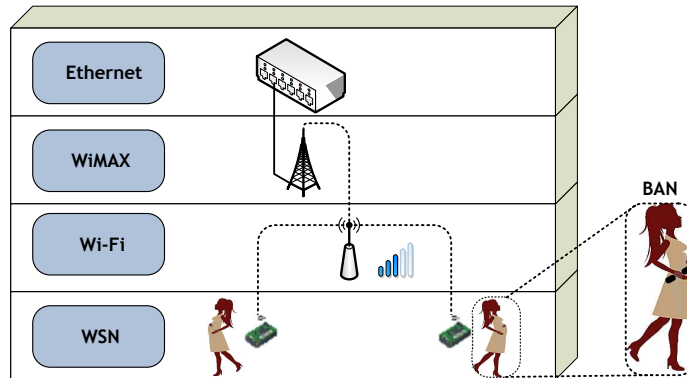


Figure 3.1: Hierarchical network considering the WBAN and other communication networks.

The majority of foetus fatalities in the end of pregnancy occur in the low risk pregnancies group. The main area addressed by the Smart-Clothing project is obstetric tracing, enabling to identify sudden changes in the foetus health, by monitoring its movements and the Foetal Heart Rate (FHR). In low risk pregnancies, in the periods between medical sessions (that occur weekly during the last five weeks of pregnancy), the objectively monitoring of the foetal health based in traditional protocols for counting the foetal movements felt by the mother is very important [EKP⁺06, GJ05]. Although the maternal perception is a relevant characteristic for the evaluation of the foetal health, the monitoring is hard to accomplish and may induce into error, e.g., due to the mother's anxiety or lack of concentration. In the Hospital, the foetal monitoring is done by using a Cardiotocograph, which records the FHR and the uterine contractions. The FHR is determined by means of an ultra-sound Doppler sensor (operating at a frequency $f = 1$ to 3 MHz), while the uterine contractions are detected with a pressure sensor (dynamometer). The foetal monitoring can be done by the pregnant woman at home, counting the foetus movements (the pregnant woman feels 80 % of them), which should be registered by herself in a form for posterior analysis of the physician. There is in the market low cost portable equipments based on the Doppler technology, which allow for foetal heart sounds hearing and the foetal movements detection, to be performed by a pregnant woman [BAL⁺08]. They can be used beyond the 12 weeks of pregnancy and allows for recording the cardiac sounds. The possible effects over the foetus due to the use of equipments based on the ultra-sound technique raise some concerns but their effects, although not well known, are probably unimportant when applied intermittently. Frequently pregnant woman does not show the same accuracy in detecting the foetus movements as it is done by the health services. Smart-Clothing is motivated by the need to conceive an automatic harmless remote monitoring device to the purpose of foetal movement monitoring.

The main Smart-Clothing scenario is presented in Figure 3.2. It consists of four main actors: the WBANs, WSN, gateway and remote agents. Each WBAN is attached to the pregnant woman and collects the data from the Electrocardiogram (ECG) and the foetal movement sensors. The

WSN is itself responsible by the aggregation of the data collected by the WBAN, and its accurate delivery to the gateway. The gateway has got a decision system that chooses the better way to deliver the data to the gateway located in the Hospital. The Hospital gathering system has the same decision system and is used for the interconnection of a WSN with remote agents through a geographical network, to collect, aggregate and eventually pre-process data received by the WSN.

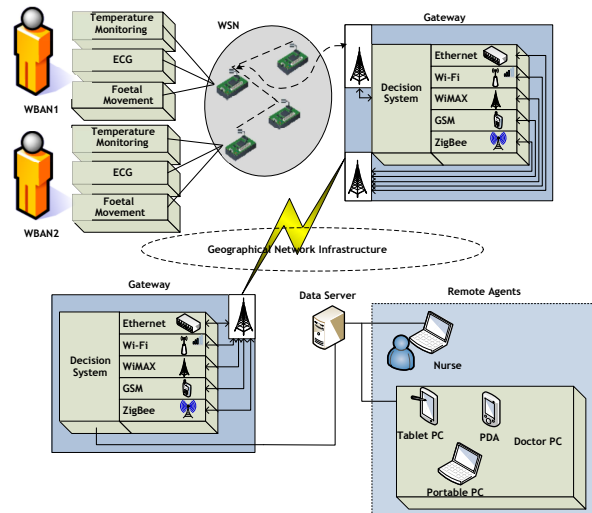


Figure 3.2: Smart-Clothing main healthcare scenario.

Finally, the remote agents can be either a collector of information (through a server where the information is stored and could be accessed later on) or a nurse that monitors the foetus in the pregnant women as well as a doctor that closely monitors the foetus by using his/her Personal Digital Assistant (PDA), or his/her laptop or even his/her tablet PC or Ultra-Mobile PC (UMPC).

3.1.2 Experimental Apparatus

Flex Sensor based Belt

After the application scenarios had been defined [BAL⁺08], the next step was to identify which types of sensors would be incorporated into the Smart-Clothing belt. To achieve this goal, several belts were made, tested and compared to see which sensors were capable of better detecting the foetal movements [BAL⁺08]. One of the Smart-Clothing belt prototypes is based on the Flex sensor, while another one incorporates a piezoelectric sensor. The first version of the Flex sensor belt incorporates eight Flex sensors, as shown in Figure 3.3. A simple voltage divider, associated to a temperature compensated voltage reference, generates the input signal. The manufacturer proposes a correspondence of standard values of the flexion angle to a certain value of resistance.

The acquisition system diagram is presented in Figure 3.4. For the sake of simplicity just one Flex sensor is presented. Besides the Flex sensor a button was incorporated in the system to be pressed by the pregnant woman (when she feels or detects foetal movement). The recording of these events is very useful for comparison purposes, as they enable a comparison of personal detected movements with the movements automatically detected by the belt. A microcontroller was used for data acquisition and communication. For practical reasons, in a preliminary experimental context, we supplied the V_{cc} voltage to the voltage divider by using external pin from the MSP430 microcontroller (MSP430-F449STK2 module) and read the

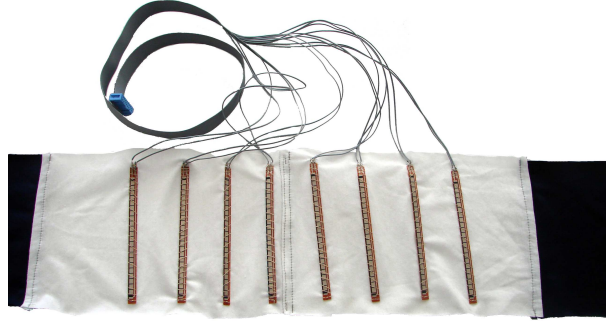


Figure 3.3: Flex sensor belt.

voltages from the voltage dividers using the Analog-to-Digital Converter (ADC) inputs of the microcontroller.

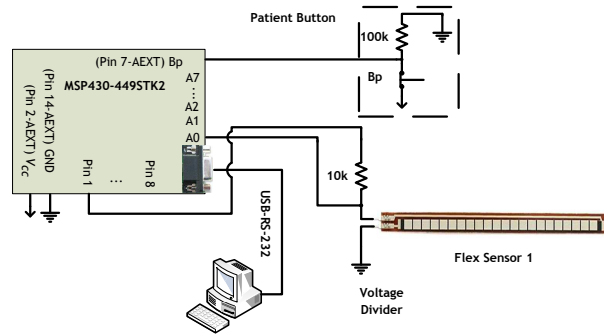


Figure 3.4: Flex sensor belt acquisition system diagram.

To compute the resistance value from the Flex sensor one uses the voltage divider formula as follows

$$R_{Flex1} = R_1 \times V_{out} / (V_{in} - V_{out}) \quad (3.1)$$

where R_{Flex1} is the resistance value, R_1 is equal to 10 k Ω , V_{in} is the V_{cc} value supplied to the voltage divider, and V_{out} is the voltage value from the voltage divider. The V_{cc} voltage supplied to the voltage divider is measured periodically by a routine that is located in the microcontroller, in order to compensate the battery losses during the system operation. This enables a better accuracy for the values extracted from the Flex sensors.

Two formulas were used for the conversion of the resistance value to the angle value, as follows

$$\theta_1[^{\circ}] = (R_{Flex1} - 10 \times 10^3) / 44.44 \quad (3.2)$$

$$\theta_2[^{\circ}] = (R_{Flex1} - 6001) / 88.88 \quad (3.3)$$

where θ_1 and, θ_2 are the angles for the corresponding Flex sensor resistance value. This enables to extrapolate the angle values.

Equation 3.2 is used when the resistance value is between 10 k Ω and 14 k Ω while Equation 3.3

is used when the resistance value is between 14 k Ω and 22 k Ω . We have made a calibration curve to identify the broad range resistance characteristic for the sensor. The Flex sensor manufacturer states that a resistance value of 10 k Ω matches an angle of 0° while values of 14 k Ω and 22 k Ω match angles of 90° and 180°, respectively.

These formulas were based on the theoretical and calibration curves for the Flex sensor, as shown in Figure 3.5. The theoretical line is based on the resistance values and corresponding deflection angle supplied by the flex sensor manufacturer. The calibration curve results from an experiment where the flex sensor was bent from 0° to 90° and the resistance value measured with a protractor was registered at each 10° of bending increment.

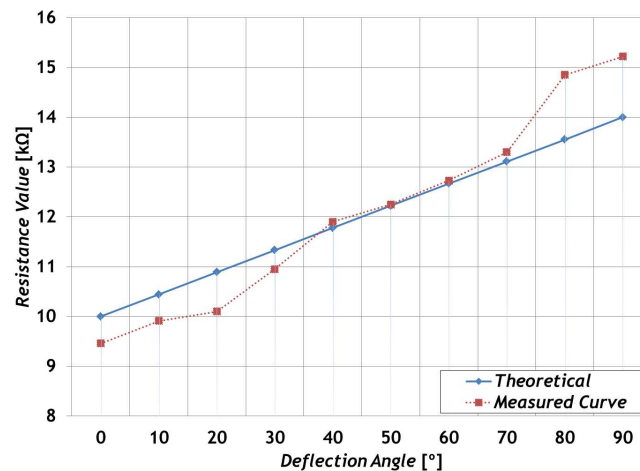


Figure 3.5: Theoretical and calibration curves for the Flex sensor.

The MSP430-F449STK2 module, after acquiring the values for each Flex sensor, sends all the data to the computer (where several values for the correspondence between resistance and angles are presented), and automatically counts the movements above a preset threshold.

The algorithm from Figure 3.6, used in the acquisition module, begins with the reset option, (applied to all system). If the reset option is not chosen then the algorithm will measure the voltage from the power supply, in order to compute later the corresponding voltage to a flexion angle. Then if button B1 (located in the acquisition module) is pressed a timer (of 100 ms) is set. After 100 ms, the algorithm starts reading all Flex sensors. First, the Flex sensor 1 voltage divider is powered up. Then, the algorithm waits 10 ms so that the ADC can read properly the voltage value from the voltage divider. Then, it computes the flexion angle depending on the read voltage value and extracts the state of the patient button (if the patient pressed the button it records the time and add one unit to the counter). This procedure is repeated for the other seven Flex sensors. However, in the last one the data from all the Flex sensors and patient counter is aggregated enabling to build the data packet while sending it to the computer. The Flex Sensor View program running presents the values of the different angles for each Flex sensor.

The final version of the standalone Flex sensor belt uses only one data packet to transmit the deformation angles of the eight Flex sensors, according to the packet protocol established between the computer and the acquisition module. This data packet is sent at the end of the routine controlled by a timer in the microcontroller only, in order to maintain a constant data flow between the acquisition module and the computer. Besides, a calibration routine was implemented in the microcontroller. Each calibration packet is sent from the program running in the computer to the acquisition module and has the ability to calibrate all the (eight) Flex

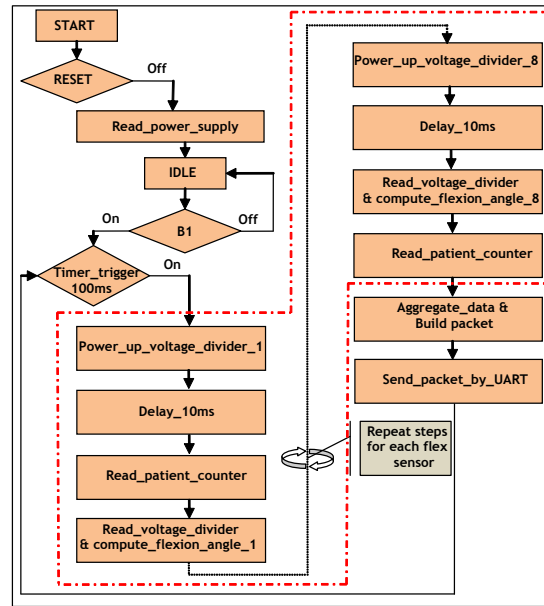


Figure 3.6: Algorithm diagram for the flex sensor acquisition system.

sensors (or only one).

Considering the preliminary work performed in the first version of the Flex sensor belt, a belt with only five Flex sensors was integrated with a WSN device. Each of the five Flex sensors is connected to an ADC channel, in order to convert the voltage (given by each Flex sensor voltage divider) to the corresponding deformation angle.

This device consists of an IRIS mote from Crossbow, a small battery and a set of Flex sensors. A hybrid communication system is employed in order to deliver the data through the WSN. The system detects the foetal movement based on the flexion angle of the sensors while the IEEE 802.15.4 network delivers all the data collected by the motes to our Centralised Management of Resources (CMR) identity.

An application that manages the WSN (and saves the information) was developed and is located at the CMR, by using a Structured Query Language (SQL) database. Figure 3.7 shows a simplified block diagram for the monitoring system. The WSN management application is also responsible to present the data to the user (nurse/doctor). As an option, it is possible to transmit the data via Wi-Fi. The information can be shared or accessed by other authorized users. The foetal movements are monitored while data is being transmitted wirelessly to a Mote Interface Board (MIB) directly connected to our CMR, as shown in Figure 3.7. The CMR is formed by a personal computer, an application which displays and saves the measured data into the database, and a Wi-Fi module to transmit data through the Wireless Local Area Network (WLAN) [BVF⁺09, SMZ07b].

There are two different possibilities to receive and send information. One uses an IEEE 802.15.4 network, while the other one considers two protocol layers (IEEE 802.15.4 and 802.11 ones). If the priority is to collect as much data as possible from the patient, some questions like energy consumption arise. Tradeoffs between energy consumption and processing and communication capabilities are relevant [BVF⁺09].

The IEEE 802.15.4 standard was chosen because of its unique characteristics that lead to energy-efficient MAC protocols. It also facilitates the development of our application according to the patient needs, while ensuring an integrated and complete solution for sensor networking based applications, including analog-to-digital conversion. One possible scenario for this small

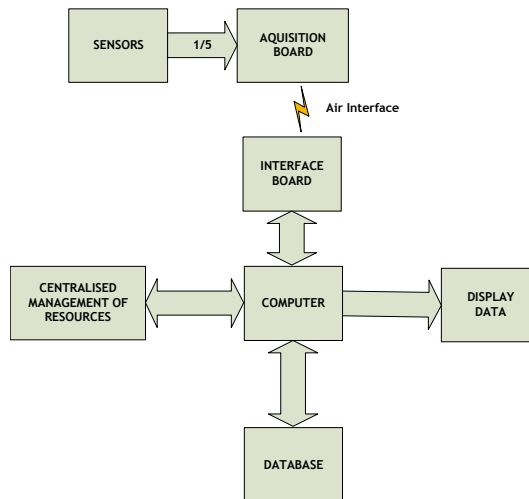


Figure 3.7: Block Diagram for the acquisition system.

scale wireless flex sensor belt network is a waiting room of the health centre or clinic, where pregnant women wait to visit the obstetrician.

In the second solution for this belt, another communication layer was considered that allows for sending and receiving information that was collected from the IEEE 802.15.4 network through an IEEE 802.11 wireless network, as shown in Figure 3.8. This solution was chosen because it constitutes a practical and interesting solution for network connectivity while offering some mobility, flexibility, and low cost of deployment. An example is transmitting the data from our CMR to any computer that is in its range and has an IEEE 802.11 (Wi-Fi) connection capability. In this scenario the CMR identity may be controlled and monitored by a nurse that looks up for anomalies in the Flex sensor belt data.

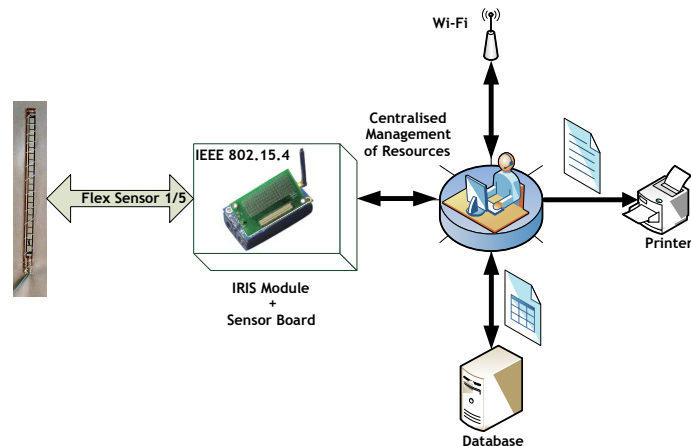


Figure 3.8: Patient monitoring and IEEE 802.15.4 wireless networking.

Belt with Piezoelectric Sensors

We developed a belt incorporating piezoelectric sensors. This type of sensor transduces the force to voltage (and vice-versa) and present high sensitivity. They proved to be an appropriate choice to detect mechanical movements such as those originated from foetus in a pregnant woman. Furthermore, the sensors could be very small, they respond to a broad frequency range, do not react to static forces and are cheap.

In this belt, we used plastic pre-encapsulated piezoelectric sensors with a BNC connector (to

drive the electrical voltage signal to the signal processing circuit). This type of sensor, Figure 3.9, is used by PowerLabs data acquisition system from ADInstruments [MLT09], at Health Science Faculty from Universidade da Beira Interior.



Figure 3.9: Piezoelectric sensor MLT1010 (ADI Instruments).

Other healthcare monitoring devices are based in piezoelectric film sensors, commonly used for the detection of biological signals. This sensor is placed against the abdomen of the pregnant woman in order to detect slight surface deformations caused by the movements of the foetus. Compared with other sensors this one presents a high sensitivity, reduced dimensions and does not need power supply to operate.

Figure 3.10 shows the signals captured by the sensor above, during an experiment where the pregnant woman also holds a pressure switch that should be pressed when perceiving a foetal movement. In this experiment, only one sensor was used several times, placed in several positions in order to detect the foetal movements. Besides the detection of the foetal movement, the mother's breath movement is also as well as the movements due to the displacement of the sensor (motion artifacts). These movements represent an interference signal that should be eliminated [VPM⁺07], and are represented upon the curve in Figure 3.10.

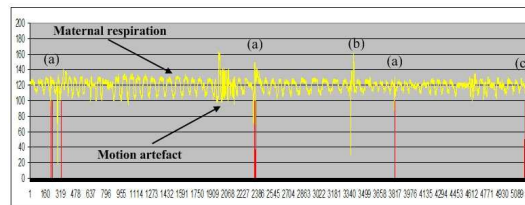


Figure 3.10: Foetal movement curves (upper=belt, lower=mother): (a) detected by mother and belt, (b) detected by belt only, and (c) detected only by the mother.

3.1.3 Experimental Results and Conclusions

Flex Sensor Belt

Some initial results were extracted from the Flex sensor belt with a patient that was not a pregnant woman. The objective of this test was to verify if the respiratory movements or other type of motion artefact influence the angles of each Flex sensor in the belt. It was verified that the respiration movements were slightly felt. Besides, if the patient moves quickly the sensors may detect the deformation from the belt.

After these preliminary tests, the Flex sensor belt was tested in a pregnant woman, in order to detect foetal movements and compare these occurrences with those signalled when the pregnant woman presses the button. A good idea that can be extracted from these initial tests is to implement a routine which automatically defines the value for a detection threshold-trigger whose values will be tuned.

The Flex Sensor View software was incorporated and its final version is presented in Figure 3.11. Examples are the capability to simultaneously show eight angles from the Flex sensor, the patient counter and the option to save the data in a log file (for later treatment). This version

enables the communication between the computer and the acquisition module by using a single interface a packet for all Flex sensors.

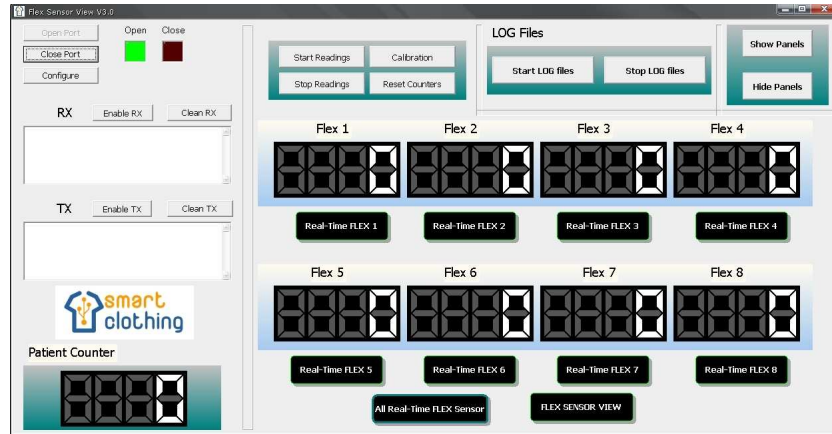


Figure 3.11: Main window for Flex Sensor View application.

Figure 3.12 presents the real-time view chart plot for the Flex sensor, extracted from the application to display the deformation angles. For each sensor, an independent threshold trigger can be defined individually or a unique threshold value can be defined (as a whole) for all the sensors.

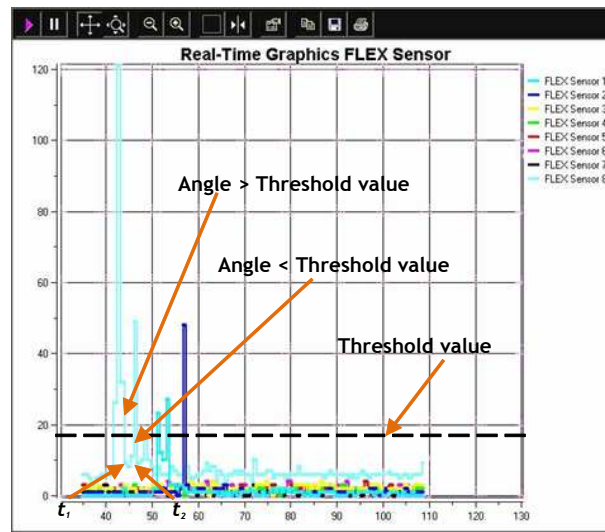


Figure 3.12: Real-time view chart plot for the Flex Sensor.

When considering this threshold-trigger, even if the sensor detects some motion artefact, a boundary can be established in order to tune when the application should count the deformation angle as a foetal movement.

In Figure 3.12, the value used for the global threshold is equal to 15° (angle deformation). This threshold was established by analysing the experimental data. This means that the automatic counter from each Flex sensor counts a flexion as a movement when the instant value of the Flex sensor angle is larger than the threshold value at one time instant and smaller at the next time instant. As an example of how the automatic counter works, considering Flex sensor 8 in the view chart at time instant t_1 the angle value is equal to 28° . Hence, the counter will count a foetal movement if this value decreases at the next time instant. In time instant t_2 the angle value is equal to 8° ; so, the automatic counter will add one unit to the counter of the Flex

sensor 8.

Some tests were made in a pregnant woman. During the test, the patient was sitting in a chair most of the time. A calibration of the flex sensors is made in the belt circuit before any test. A test was also made on how curves vary if a sudden change of the pregnant woman position happens, as shown in Figure 3.13.

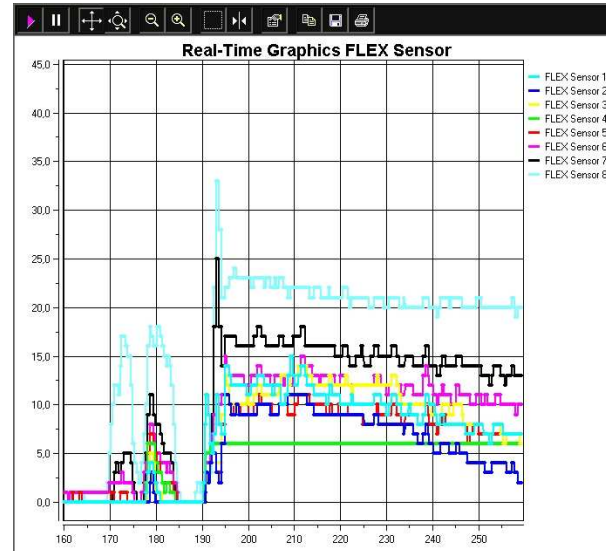


Figure 3.13: Results when patient stands up at time $t = 190$ s.

One may verify that the change of position occurred approximately at the time instant 190 s. There was a lot of artefact movement detected during the change of position, which causes the loss of the initial calibration.

Another test was made while the patient was sitting in a chair. Two different foetal movement occurrences were detected. In this case, instead of presenting all the flex sensors in the same window we enabled the software option to show separate windows for each flex sensor. The movements were detected in the flex sensor 1, at time instants ≈ 420 s and ≈ 460 s, as shown in Figure 3.14. A motion artefact was detected after the time instant 500 s, probably due to the mother respiration movements.

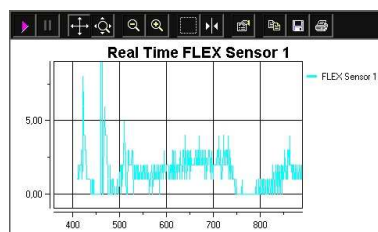


Figure 3.14: Results from Flex sensor 1 when patient is sited.

Simultaneously, the window that monitors the Flex sensor 2 shows two peaks, whose amplitude is larger than the other peaks in the chart, one at the time instants ≈ 420 s and another at time instant ≈ 460 s, as shown in Figure 3.15. The movements detected by Flex sensor 1 caused a deformation angle larger than the one from Flex sensor 2. Hence, because the Flex sensors are placed side by side (and separated by 8 cm) we may conclude that the movements detected were nearer Flex sensor 1.

Another test was made when the patient was sitting in a chair, as presented in Figure 3.16. A movement was detected by the system, while the patient claims to have detected two foetal

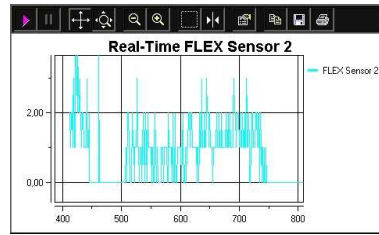


Figure 3.15: Results from Flex sensor 2 (Patient sited).

movement occurrences. The time instant when the system and the patient detected the foetus movement simultaneously was ≈ 910 s. The system detected the movement at the Flex sensors 1, 2, 3, 4, 5 and 6, with a stronger intensity in the Flex sensor 3. The other movements the pregnant woman claimed to have felt a foetus movement was at time instant ≈ 895 s. However, the system did not detect any foetal movement. At the instant ≈ 925 s the system detected a foetus movement but it was considered a false positive, as the patient did not feel it.

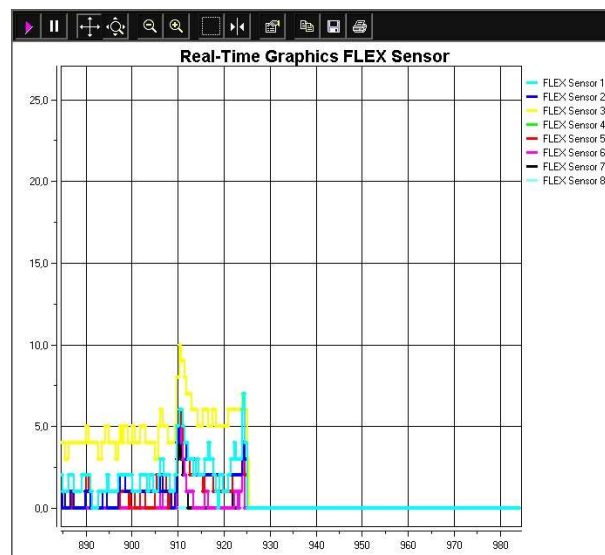


Figure 3.16: Results when patient is sited.

Piezoelectric Sensor Belt

All the tests of the piezoelectric sensor belt were performed in Centro Hospitalar da Cova da Beira. A woman in her 38th week of pregnancy wore a belt that incorporates three piezoelectric sensors (one central sensor and two on both sides), adjusted to the abdomen by an elastic belt. The signals obtained from the sensors were combined into only one signal, amplified, filtered and applied to an ADC converter, and then sent to the computer via USB. At the computer, the signals were processed and graphically presented to the medical team. The pregnant woman had a manual event marker (patient button) to mark the foetal movements when she felt it, for redundancy purposes. Another device was also used, called RespiSense [res09] and usually applied to detect the baby breathing. The signals of the event marker and RespiSense were compared with those extracted from piezoelectric sensors. Figure 3.17 shows a block diagram of the circuit to acquire the signals from the sensors.

Figure 3.18 shows the Hospital environment in which the tests were performed, as well as the pregnant woman. The belt covers only a small part of the pregnant patient belly, contributing for non-ideal results. We plan to use more piezoelectric sensors in a future version of the belt.

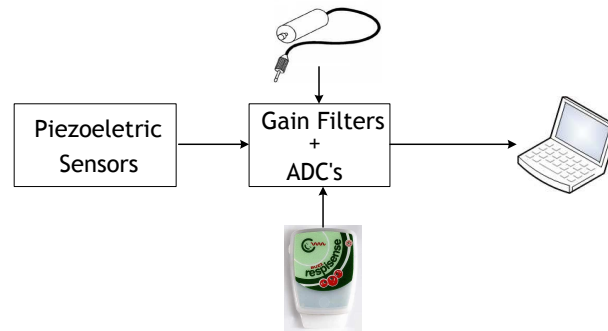


Figure 3.17: Diagram for the circuit to acquire the signals from the sensor.



Figure 3.18: Field tests for foetal movements' detection.

Figure 3.19 shows the experimental results. Different signals can be observed, distinguished by different colours:

1. Red - original signal (piezoelectric sensors);
2. Blue - filtered signal (finite impulse high-pass response filter);
3. Brown - event marker;
4. Green - detected foetal movements.

Figure 3.19 presents a screenshot from the program developed to display the signals from the sensors. It shows the a) multiple foetal movements simultaneously detected by the mother and sensors, as well as b) some discrepancies caused by patient movements (like speaking, tossing), by the event marker detection forgotten by the patient, and due to the reduced number of piezoelectric sensors included.

From the experimental results, we can conclude that the system has a high potential to detect foetal movements, isolating them from external interferences. However, weak foetal movements are easily hidden by signals with larger amplitude, such as maternal walking, speaking and even breathing.

Filtering and interference reduction will be important topics that need further research. Also, using more piezoelectric sensors inside of the belt, to cover a broader area of the pregnant woman abdomen, is one suggestion for future developments. As a suggestion, it may be possible to use sensors built with polymer films (Polyvinylidene Fluoride) [pol09] in the future.

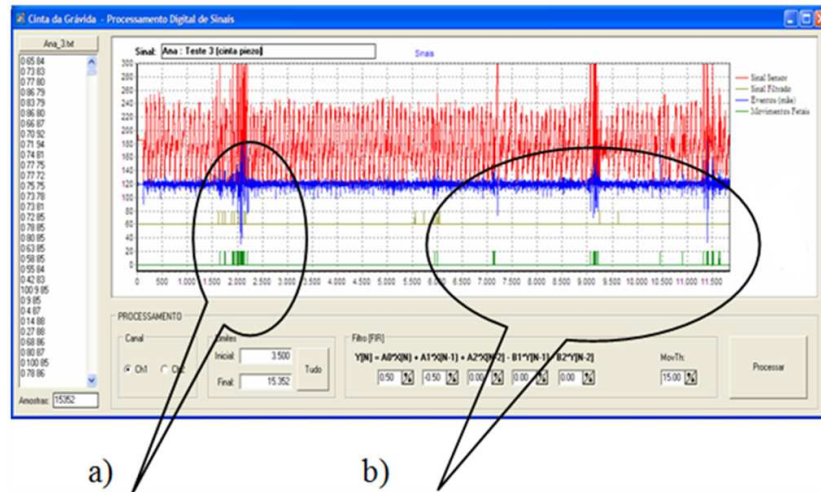


Figure 3.19: Test results for foetal movements' detection.

3.1.4 Summary and Conclusions

This Section presents two main versions of prototype sensor belts produced within the Smart-Clothing Project, which aim at counting the movements of the foetus in a pregnant woman. Besides the standalone solution for the Flex Sensor belt, where data can be saved into a memory card, we developed a wireless Flex sensor belt network based on the IEEE 802.15.4 standard. A hierarchical wireless network with a Wi-Fi layer on top of the sensor network will allow for extra flexibility in data communication. The system guarantees real-time and continuous foetal monitoring while creating effective interfaces for querying sensor data and store all the medical record (which can later be accessed by health professionals). Another developed belt has piezoelectric sensors incorporated onto it. The system has a high capacity to detect foetal movements, isolating them from external interferences. As future work, we propose to implement other types of communication systems that may work together with the existing ones. For example, create a webpage where we can scroll through all the data produced in real time while sharing the information with other medical institutions. Another proposal is to implement algorithms for signal source separation, noise and motion artefact signal suppression, as well as to implement advanced algorithms for data treatment and aggregation. Further work is needed to upgrade the signal conditioning circuitry, the processing soft-ware (to accomplish a real time filtering) and statistical techniques to detect the foetal movements in the piezoelectric belt. The data collected from the belt contains signals from the mother and foetus. An alternative approach to distinguish the different signals detected with the belt may be based on a spectral analysis instead of time domain analysis, facilitating the separation of the different signals, such as the mother respiration, foetus movements, mother's heart beat and motion artifacts. Other techniques may be based on the Fast Fourier Transform (FFT), which detects a peak from a signal composed by signals with different frequencies, or blind source separation.

3.2 Concrete Structural Integrity - INSYSM Project

3.2.1 Introduction

It is now recognized that integrated monitoring systems and procedures have an important and promising role to play in the total management of concrete structures. Monitoring deterioration would provide an early warning of incipient problems enabling the planning and scheduling of maintenance programmes, hence minimizing relevant costs. Furthermore, the use of data from monitoring systems together with improved service-life prediction models leads to additional savings in life cycle costs [Bue08, MV04].

Sensors and associated monitoring systems to assess materials performance form an important element in the inspection, assessment and management of concrete structures. There are more than fifty different types of sensor whose deployment into practical devices facilitates long-term monitoring of structural changes, reinforcement corrosion, concrete chemistry, moisture state and temperature [MV04].

The development of new sensor concepts allows for a more rational approach to the assessment of repair options, and scheduling of inspection and maintenance programmes in different civil engineering structures. Currently, there is a growing number of recent studies for the development of sensors in concrete structures, to monitoring from earlier-age parameters to environmental conditions that can cause deterioration processes, some of which may be highlighted. The authors in [PL11] studied an early-age concrete strength development miniaturized sensor system. The idea is to characterize the condition of the fresh concrete at very early stages. It consists of a reusable transducer being strong enough to easily detach from the hardened concrete structure, and to monitor the concrete strength development at early ages and initial hydration stages.

The monitoring of temperature and moisture level will provide crucial information about the hardening and setting process of concrete as well as the progress of deterioration mechanisms such as corrosion of steel reinforcement, freeze-thaw cycles, carbonation and alkali-aggregate reaction. A new technique to monitor the moisture level and temperature has recently been proposed in [NSR08]. This innovative technique uses nanotechnology/Microelectromechanical Systems (MEMS) to measure temperature and internal relative humidity by using microcantilever beams and a moisture-sensitive thin polymer. Based on the obtained results, it was found that the proposed MEMS survived the concrete corrosive environment, as well as to internal and external stresses. Also it was found that the MEMS output reflects the change in the concrete properties and can be used to effectively measure moisture content and temperature, with high sensitivity. However, serious issues, such as long-term behaviour and repeatability of MEMS embedded into concrete, require further investigation [NSR08].

3.2.2 Motivation and Objectives

INSYSM project creates innovative strengthening and sensing technologies based on the textile industry experiences. Strengthening equipped with monitoring systems enables very powerful advantages. During all of the work phases collected measurements can picture performance of a whole structure, which can be used for continuous observation of the building and shall allow to master the strengthening solutions due to building real life work, also during accidental situations like floods, earthquakes. The project predicts two main objectives: i) set of the procedures for retrofitting, strengthening, real time monitoring and maintenance of structures

impacted by complex situation of loads (i.e., seismic, paraseismic and dynamic floods, transport, etc); ii) development of technology of smart textile with embedded sensors for the needs of structural engineering on field of strengthening and monitoring existing structures.

The primary objective of our interdisciplinary research is to develop a prototype for WSNs allowing for remotely monitoring certain concrete structures. Our research work is focused on studying the behaviour of a concrete cube immediately after casting and at earlier ages, whilst monitoring all the temperature and moisture changes in real time. This is accomplished by using an IEEE 802.15.4 network enabling a significant reduction of the installation time and costs. The experiments to be carried out also aims at expanding the output from this research to the monitoring of other structures regardless the type of material, and to develop a prototype that facilitates to measure several parameters inside a real concrete structure, e.g., humidity and temperature. Besides the temperature and moisture evaluation in the concrete structures the rate of strength development in the early life of the concrete which is strongly related to its rate of hydration is also studied. As a consequence, it is worthwhile to study the impact of the temperature increase caused by the occurrence of the hydration reaction. In the context of WSNs applied to civil engineering structures it is important to create a monitoring device platform that is able to accommodate a wide range of sensors, depending on the needs, expandability and cost, while sharing the information across the network. From the application perspective, WSNs are useful in situations that require quick or infrastructure-less deployment and continuously monitoring [Jur07, FDC⁺09, IM09]. Structural health monitoring has been identified as a prominent application field for WSNs, since traditional wired-based solutions present some inherent limitations such as installation/maintenance cost, scalability and visual impact. In order to collect the data from the temperature sensors, a WSN was created facilitating the remote monitoring. For this purpose, remote agents can be collectors of information either by storing the data into a microSD card, to be accessed later on, or by wirelessly transmitting this information, in real time, to a Mote Interface Board (gateway) that is connected to a PC, allowing for a rapid intervention of civil engineers, if needed.

3.2.3 SHT15 Humidity and Temperature Sensor

In the second set of tests, the SHT15 [SHT10a] digital sensor was used, facilitating to measure both temperature and humidity with high accuracy in a single chip sensor. Figure 3.20 presents a schematic representation of process to measure the temperature and humidity within the concrete cube.

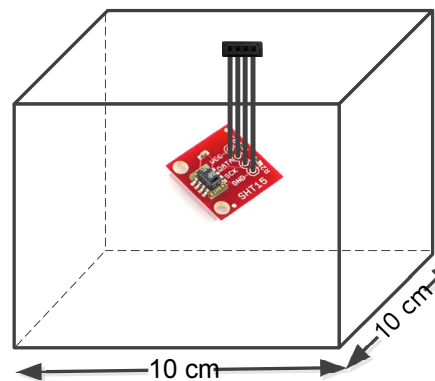


Figure 3.20: Schematic representation of temperature and humidity sensor inside a concrete cube (10 cm length size).

The conversion from the raw value returned by the SHT15 sensor, R_{xval} , to the temperature and humidity values was performed by using the following equations:

$$Temperature[^{\circ}C] = (R_{xval} \times 0.01) - 40 \quad (3.4)$$

$$Humidity[\%RH] = -4.0 + 0.0405 \times R_{xval} - 0.0000028 \times R_{xval} \times R_{xval} \quad (3.5)$$

Before inserting the sensor inside the concrete block, the following preparations have been made (as shown in Figure 3.21):

- the sensor was placed inside a small size cube (4 cm side length) made of cement mortar for its protection. The mortar was produced using low water content with a cement mortar ratio of 1:3 (the mortar works as shell that can protect sensor wire connections when placed inside concrete during casting; high porosity of this mortar shell easily allows moisture measures of involving concrete);
- coarse sand size was used avoiding fine particles, so that the sensors would not become obstructed.

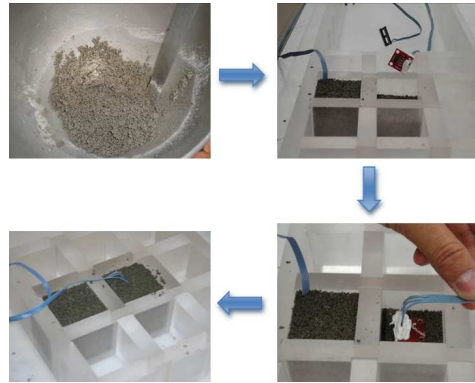


Figure 3.21: Preparation and placement of the temperature and humidity sensors inside a mortar cube (for its protection).

3.2.4 SHT21S Humidity and Temperature Sensor

Standalone version

Besides the SHT15 [SHT10a] (humidity/temperature) sensor, we tested the new Sensirion SHT21S [SHT10b] (humidity/temperature) sensor. Before testing this sensor was also placed inside a cement mortar shell has been used for its protection. This sensor is an updated version of the previous one but with a smaller package. To test this sensor an acquisition system was designed to facilitate the acquisition of the analogue signal while converting it for its digital representation. As previously mentioned we intend to measure both temperature and humidity inside the concrete block, from the early ages, during setting and hardening period.

The temperature and humidity values are obtained by using Equations 3.6 and 3.7, respectively:

$$Temperature[^{\circ}C] = -46.85 + 175.72 \times \frac{V_{SO}}{V_{DD}} \quad (3.6)$$

$$Humidity[\%RH] = -6 + 125 \times \frac{V_{SO}}{V_{DD}} \quad (3.7)$$

where, V_{DD} is the supply voltage at which the SHT21S sensor works, as presented in the datasheet of the sensor in the interface specifications. In this case, $V_{DD}=3$ V. Besides, since the SHT21S output is a Sigma Delta Modulated (SDM) signal, normally this signal is converted to an analogue voltage signal by the means of a low-pass filter. The output of low pass filter provides a voltage value (V_{SO}) which is a portion of V_{DD} , depending on the measured humidity or temperature.

The developed acquisition system (for the standalone SHT21S) incorporates a microSD module, responsible for storing the values acquired from the SHT21S sensor, as shown in Figure 3.22.

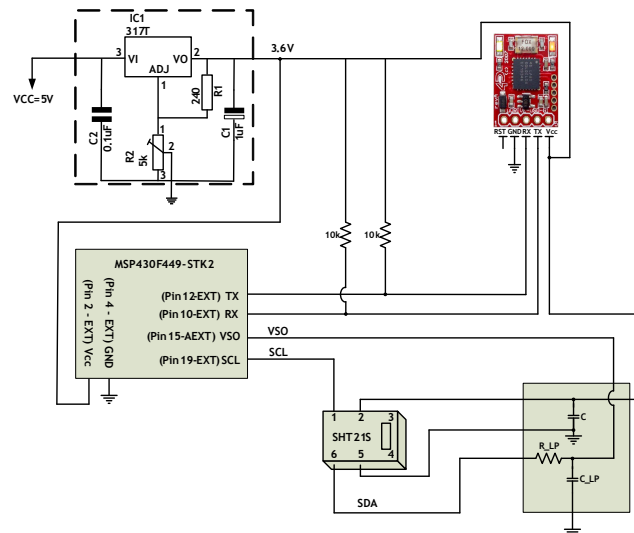


Figure 3.22: SHT21S acquisition system for the standalone version.

The MSP430F449-STK2 module was used to convert the signal output from the RC-filter to the digital format. The algorithm running inside the microcontroller performs five readings (with a 100 ms interval between two consecutive readings for the temperature), storing the fifth reading in a buffer. Then, it switches to the humidity sensor, performing another five readings and conversions with the same duration between consecutive readings, storing the fifth reading in another buffer. Finally, after that it sends the commands to store the temperature and humidity values in separated text files, into the microSD card.

Wireless version

The SHT21S wireless prototype aims at creating a Building Wireless Sensor Network (BWSN) capable of measuring temperature and humidity inside a concrete structure. It has two Integrated Circuits (ICs) interfaces via Serial Port Interface (SPI), and an antenna allowing for connectivity with no additional hardware components. Besides, it provides real-time data information and remote interaction with multiple devices (e.g., laptop, PDA, cell phone with ZigBee[®] capabilities). The MSP430F2274 ultra-low-power microcontroller controls the CC2500

radio transceiver (that operate at the 2.4 GHz band) and establishes a basic wireless networks with minimal power requirements, enabling to extend the system lifetime. Figure 3.23 presents the acquisition system used to read the signal from the SHT215 sensor.

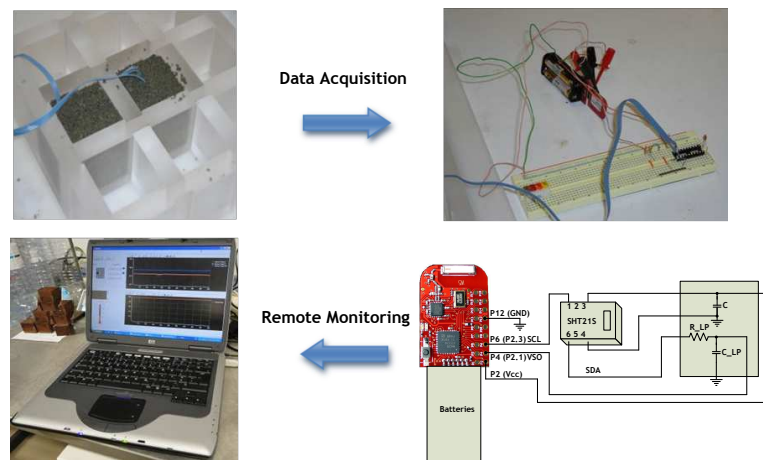


Figure 3.23: SHT215 wireless acquisition system.

The computed temperature and humidity values are sent wirelessly to the Access Point (AP). The End Device (ED) reports periodically values each minutes to the AP. The user depending on the application scenario can change this reporting periodicity value.

3.2.5 Joint Verification of Shielded SHT15 and SHT21S Sensors

The main purpose of shielding the SHT15 and SHT21S sensors is to protect the sensor from the concrete high relatively humidity alkaline environment that could affect the sensor inside the concrete. Besides, the unique capacitive sensor element used to measure humidity as well as the band-gap sensor utilized to measure the temperature do not resist to the high relative humidity alkaline environment present in cement. To overcome this limitation, in the second series of tests we have decided to use a filter cap allowing for protecting the SHT15 and SHT21S humidity and temperature sensors against dust, water immersion, condensation, as well as contamination by particles. The cavity inside the filter cap is made such that the volume between the membrane and the sensor is kept minimal, which reduces the impact on the response time for the humidity measurements. The filter cap is made of a single piece of polypropylene (PP) and a filter membrane welded to the single piece, Figure 3.24.

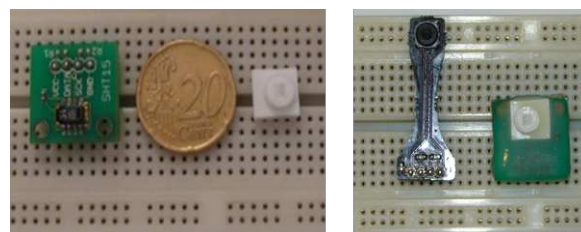


Figure 3.24: Filter cap protection for the SHT15 and SHT21S sensors.

Before inserting the filter cap for sensor protection, the following preparations have been made (as shown in Figure 3.25):

1. the filter cap was mounted on the printed circuit board (PCB) after soldering the SHT15 and SHT21S sensors by sticking the two openings in the PCB;

2. the filter cap was fixed by an adhesive (melting the pins from the back side by heating them up with a hot iron, was also possible);
3. an hermetic seal was applied, which is an adhesive added between the filter cap, sensor housing and PCB, providing higher security against water leakage, condensation inside the housing and corrosion of the soldering paths of the sensors.

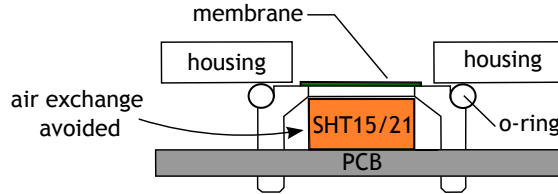


Figure 3.25: Mounting schematics for the filter cap protection for the SHT15 and SHT21S sensors.

After shielding the SHT15 and SHT21S sensors, we have decided to create different humidity and temperature environments and compare the obtained results with a standard climate sensor probe (Rotronic hygroclip probe, for all climatic measurements, operating range $-40\ldots100\text{ }^{\circ}\text{C}$, $0\ldots100\text{ \% RH}$) in order to show the accuracy of the measurements, as presented in Figures 3.26 to 3.29. The response of the sensors was tested in four different conditions. The first test consists of creating a controlled relative humidity of 75 % inside a desiccator. Therefore, the bottom of the desiccator was partially filled with sodium chloride saturated salt solution (salt mixed with water), as shown in Figure 3.26. The test was performed during 23 hours, in which the standard climate sensor probe from Rotronic was used to confirm the measured values with SHT15 and SHT21S sensors.

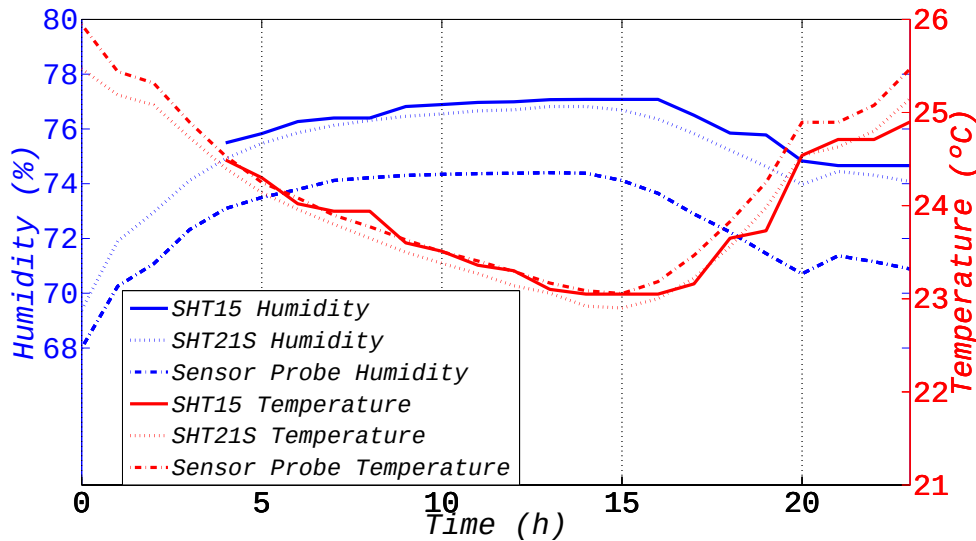


Figure 3.26: Humidity and temperature results obtained using the SHT15 and SHT21S sensors for a controlled humidity of 75 %.

During the first 4 hours the SHT15 was not connected to the Arduino platform, so we did not measure any temperature and humidity value. After 4 hours we power up the SHT15 sensor and it started to measure both humidity and temperature values. Between the 4th and 23rd hours, by comparing the results obtained from the SHT15 and SHT21S sensors with the ones obtained from the sensor probe, we conclude that the results are similar. Moreover, after 7 hours, both humidity and temperature values start to have a constant behaviour, where the

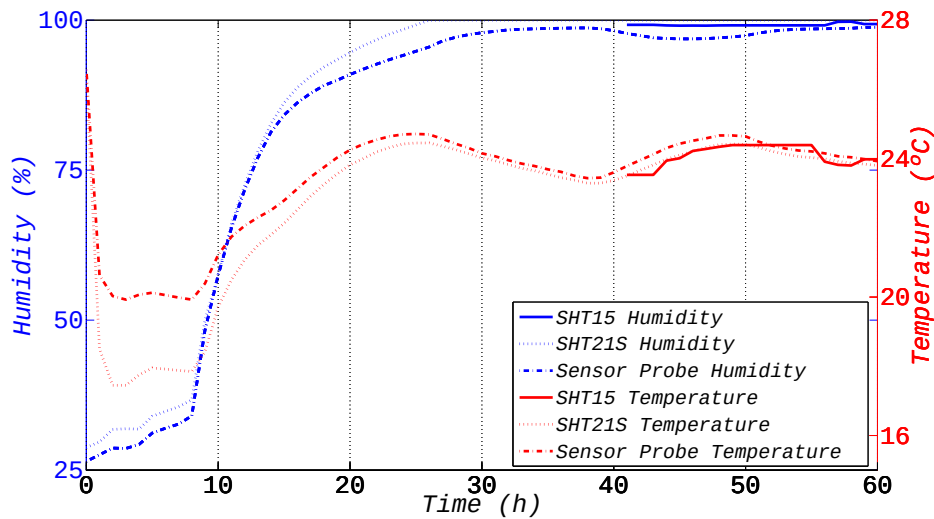


Figure 3.27: Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which silica gel particles are replaced by ice cubes.

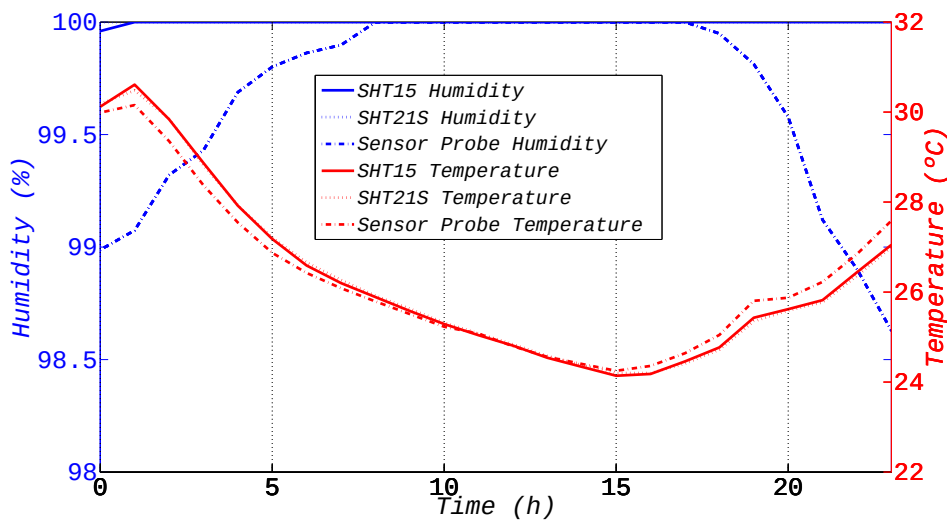


Figure 3.28: Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which the desiccator is filled with water.

humidity is about 75 % and the temperature is about 23 °C. After 16 hours we have decided to open the desiccator to observe if there is any variation in the temperature and humidity values. As presented in Figure 3.26 there is a decrease in the humidity values and an increase in the temperature values. In the second set of tests, Figure 3.27, the bottom of the desiccator which was filled with a salt solution was replaced by ice cubes. Therefore, during the first 5 hours there is a decrease of the temperature and an increase of the humidity values. After 30 hours the air inside the desiccator reaches the equilibrium, where the humidity is about 100 %, and the temperature is ambient dependent. The SHT15 sensor was connected only after 42 hours. Between the 42th and 63th hours and by comparing the results obtained from the SHT15 and SHT21S sensors with the ones from the sensor probe, we conclude that the results are similar. In Figure 3.28, the ice cubes inside the desiccator melted, and the bottom of the desiccator is filled with water. Therefore, as expected the humidity inside the desiccator is around 100 % and the temperature is ambient dependent. In addition, there was an increase of the temperature during the day and a decrease during the night. Finally, the last test consists of replacing the bottom of desiccator previously filled with water, by silica gel particles. As presented in

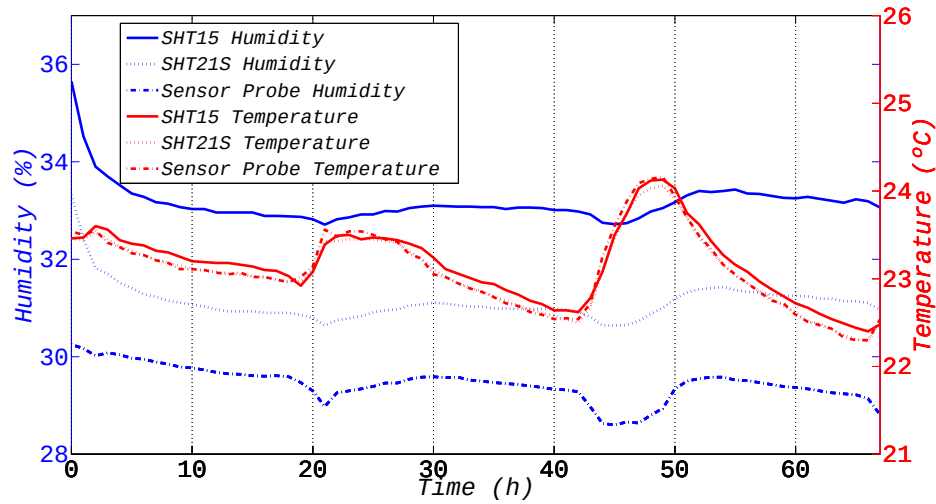


Figure 3.29: Humidity and temperature results obtained using the SHT15 and SHT21S sensors in which the water is replaced by silica gel particles.

Figure 3.29 there is a fast variation in terms of relative humidity inside the desiccator. The humidity values show an average standard deviation of 5 % by comparing the SHT15 and SHT21S sensors. This can be explained by the fact that the positions inside the desiccator are not the same, leading to small variation in the measurements of the humidity values. Besides, we have also noticed that there was an average standard deviation of 2 to 4 % between the relative humidity measured by the standard climate sensor probe from Rotronic and the SHT15 and SHT21S sensors, respectively. This is due to the fact that the sensor probe [Hyg12] is not as accurate as the digital humidity and temperature sensors when fast variations occur.

3.2.6 Results and Discussions

In this section is presented the experimental results obtained for the SHT15 and SHT21S sensors in different scenarios. The experimental results obtained with the negative temperature thermistor are presented in Appendix D.

SHT15 humidity and temperature sensor

The second set of tests considers the use of the SHT15 sensor, allowing for measuring both the humidity and temperature. Two solutions were tested, one with the PIC18F4680 microcontroller and another one using the Arduino platform. Before using the SHT15 sensor in a real scenario, some tests have been performed to verify the accuracy of the temperature and humidity readings. By using a temperature of 16.3 °C inside a fridge chamber, and by comparing the results obtained from the sensor with the ones obtained from the sensor probe, we conclude that the results are very similar, as shown in Figure 3.30.

To measure humidity we place the SHT15 sensor inside a small mortar cube for sensor protection, as explained in Section 3.2.3. When, the cubes were placed in a tray (with 2-3 mm water level), we observed the rise of water inside the cube by capillary, as shown in Figure 3.31. After around one minute, the humidity reaches a value of 98 % RH. The objective of this test was to verify the sensor integrity, as well as the porosity effect of its mortar shell. The results obtained from both PIC18F4680 and Arduino platform were identical. The tests were carried out during several hours, to observe if any variation of humidity and temperature could be detected.

In another experiment a SHT15 sensor with a mortar shell was fully immersed in water. One

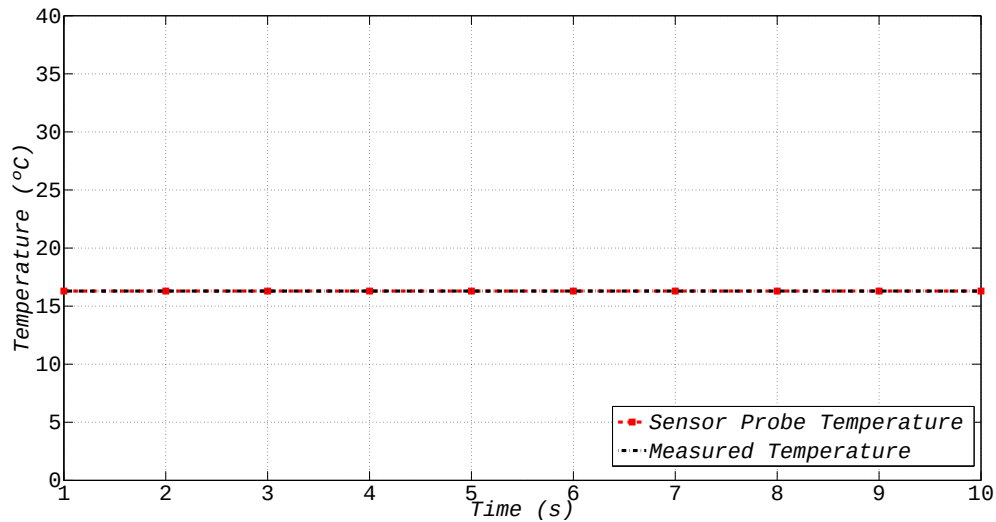


Figure 3.30: Sensor probe temperature versus measured temperature inside the fridge chamber by using an SHT15 temperature sensor.



Figure 3.31: Setup to measure temperature and humidity using an SHT15 sensor inside a mortar cube for sensor protection.

observes that the temperature was decreasing while the humidity was increasing. After 20 minutes of accurate measurements we have decided to prolong the test during one week. However, after one day, the SHT15 temperature sensor went off. Then, after 4 days the same happened to the humidity sensor. It is believed that the primary reason for this occurrence is that some chemical reactions inside the mortar shell have affected the capacitance of the sensor. Sensor components might not resist to alkaline ions present in cement, namely calcium hydroxide, which can be released in water from its mortar shell during immersion. To solve this problem, instead of making a cement-based mortar shell it may be preferable to shield the sensor using other material, textile or polymer based.

SHT21S humidity and temperature sensor (standalone version)

The SHT21S sensor protected by a mortar cube was placed inside a concrete cube during casting, as shown in Figure 3.32. The values measured by the sensor were recorded into the microSD card. The data collected from the sensor is shown in Figure 3.33. The measurements were performed in outdoor environmental conditions during summer. During the first 12 hours there has been a constant and progressive variation; while between the 12th and 16th hours a decrease in the temperature and humidity values has been observed. After 16 hours, the sensor stopped reading the temperature values. Only the humidity values have been measured beyond this

time instant. As occurred with SHT15, the SHT21S sensor components have not resisted long time inside the concrete alkaline environment. To overcome this limitation, shielding of sensor is also advised in this case, e.g., with textile, polymer (Polybutylene Terephthalate) [Cap10] or even metal shielding.



Figure 3.32: Preparations to measure early age concrete temperature and humidity using a SHT21S sensor inside a mortar cube.

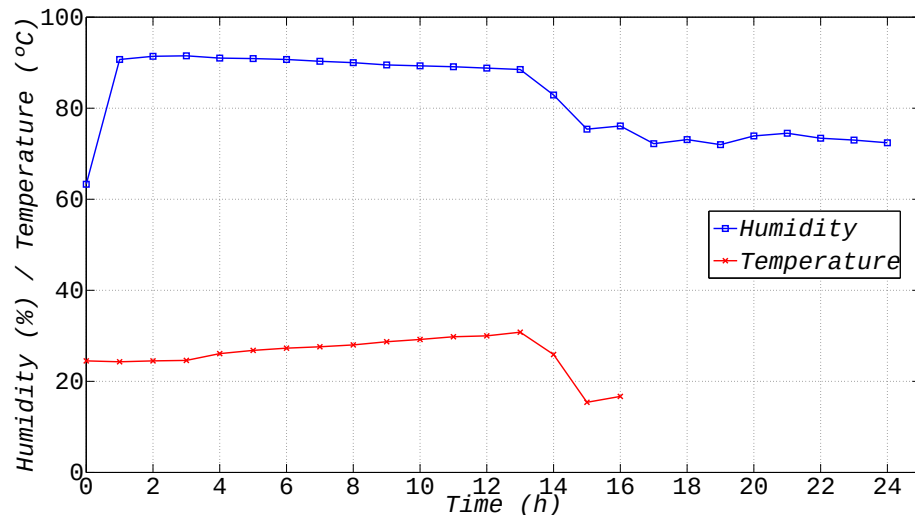


Figure 3.33: Results for the humidity and temperature for the SHT21S sensor obtained in a cube placed in outdoor environmental conditions during summer.

SHT21S humidity and temperature sensor (wireless version)

In scenarios of remote monitoring, there is a need of extracting and recording the data gathered by the sensor nodes. To avoid the need of regularly visiting, remote access to the collected data is essential. Moreover, solutions involving WSNs have a tremendous potential in real time structural health monitoring, since they potentially reduce costs.

The SHT21S wireless version allows for collecting the information from any given structure. Figure 3.34 presents the SHT21S eZ430-RF2500 C++ software program responsible for the acquisition of the values from the SHT21S sensor. The acquired values are shown in two different ways either plotted in a chart as a function of time, or by the instantaneous observation of the values in a segment display (while the AP receives the data packets). To analyse the acquired values we can export the data to a Matlab® file.

As shown in Figure 3.34 the results obtained for temperature and humidity are quite accurate. Therefore, the use of a porous cement mortar as protective shell does not affect the sensor readings. This method of protection of the sensor is similar to those developed by

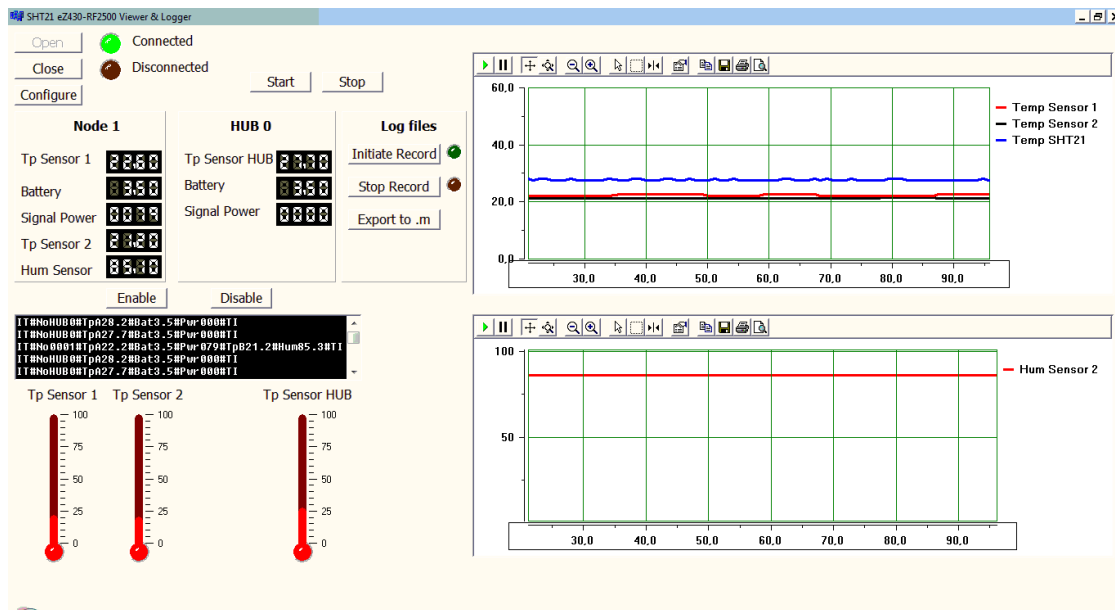


Figure 3.34: Software program for the acquisition of the SHT21S eZ430-RF2500 sensor data.

Chang and Hung [CH12] and recently published, although unknown to authors during the experimental phase. However, the presented solution does not consider an encapsulation box for the electronic acquisition system components (since it is outside the “brick”), as presented in Figure 3.23. This way we are able to obtain more accurately values for the temperature and humidity, since the sensor is placed as close to the environment as possible. By using an encapsulation box the detected temperature and humidity may not be the actual structure temperature and humidity, as stated in [CH12]. Besides, in the work developed by Chang and Hung [CH12] the Radio Frequency Integrated Circuit (RFIC) transmitter is inside the brick, being the maximum effective reception range below 20 m. The research conducted by B. Quinn and G. Kelly [QK10], also considers a package to protect the sensor from the aggressive environment. Preliminary results show that the transmission distance is strongly affected by the steel backed formwork, showing that the maximum distance achieved without the formwork is 7.5 m. In our case, by considering the open field scenario (since the acquisition systems is outside the “brick”) the eZ430-RF2500 can achieve a minimum effective reception range of 35 m.

In this experiment, the SHT21S sensor temperature readings have been successfully performed during the first 16 hours, while the humidity values were successfully obtained during the first 21 hours. After this period, the sensor went off, possibly also caused by the alkaline concrete environment that stopped the sensor operation.

3.2.7 Joint Verification of Shielded SHT15 and SHT21S Sensors

In this set of experiments, the SHT15 and SHT21S sensors previously shielded were inserted into two small size mortar cubes (4 cm of side length) before being inserted into the concrete block. To test the accuracy of the measurements, the mortar cubes were first placed in a tray with water. After some time, we observed the rise of water inside the cube by capillarity. Then, the cubes were removed for drying, Figure 3.35. The cube containing the SHT15 sensor initiated the drying process after 10 hours, while the cube containing the SHT21S sensor started the drying process after 60 hours. After 97 hours, we have repeated the test of placing the cubes in a tray with water, in order to observe the increase of the humidity values. The standard deviation

between the humidity measured by the SHT15 sensor and the SHT21S sensor is explained by the fact that the small cubes are not exactly the same, so some variations in terms of humidity may exist during the drying process. Besides, if the SHT21S is exposed to conditions outside the normal operation range (humidity > 80 %), an offset could exist. Therefore, in high relative humidity environment it is advised to use the SHT15 sensor. The measured temperature is similar to the ambient temperature, in which the small variations are also due to the drying process.

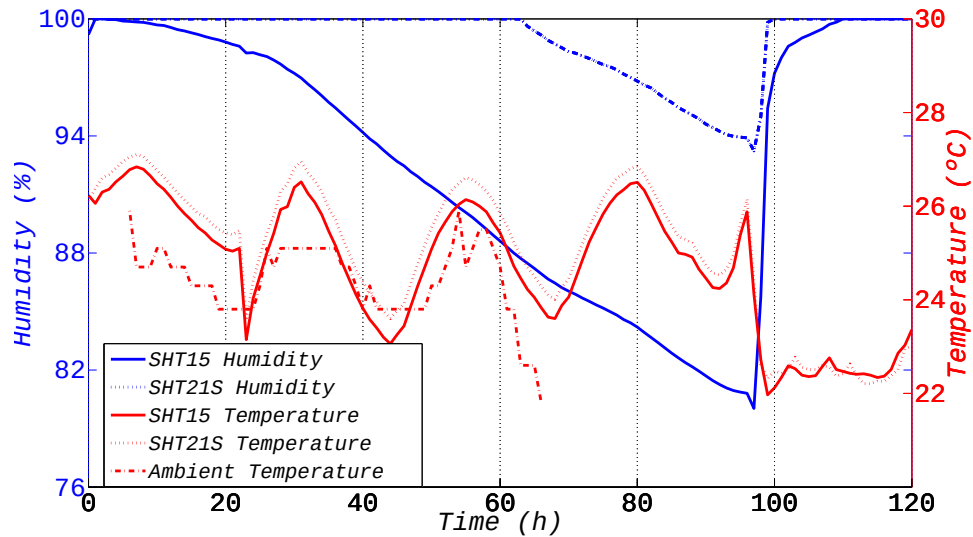


Figure 3.35: Humidity and temperature results obtained using the SHT15 and SHT21S sensors during 5 days.

Then, the SHT15 and SHT21S sensors previously shielded and protected by a mortar cube were placed inside a concrete cube during the casting, as shown in Figure 3.36.

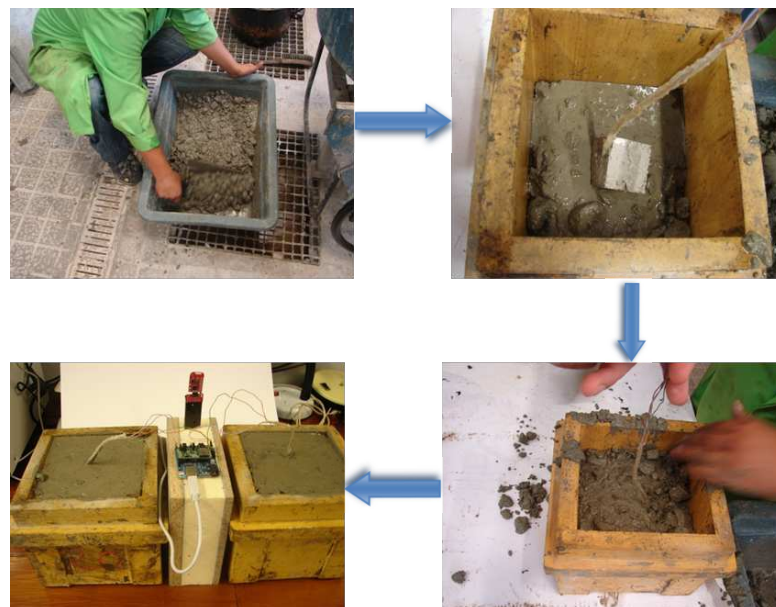


Figure 3.36: Preparations to measure early age concrete temperature and humidity using the SHT15 and SHT21S sensors inside a mortar shell.

The values measured by the sensors were recorded into the microSD card. The data collected from the sensors is shown in Figure 3.37. The tests were performed during 4 days. During the

first 12 hours there is an increase of the humidity for the cube containing the SHT15 sensor, while the humidity inside the cube containing the SHT21S sensor achieves the maximum value (i.e. 100 %). Moreover, during the curing process the temperature inside the cubes was about 37 °C after the first 11 hours. These results are similar to the ones presented in Figure 3.33. Therefore, we may conclude that by using a filter cap (shielding the sensors) as shown in Figure 3.24, we protect the humidity and temperature sensors, allowing for the creation of a long-term solution, which is one of the objectives of these experiments. Finally, it was verified that both sensors were performing measurements inside the concrete after 2 months of experiments.

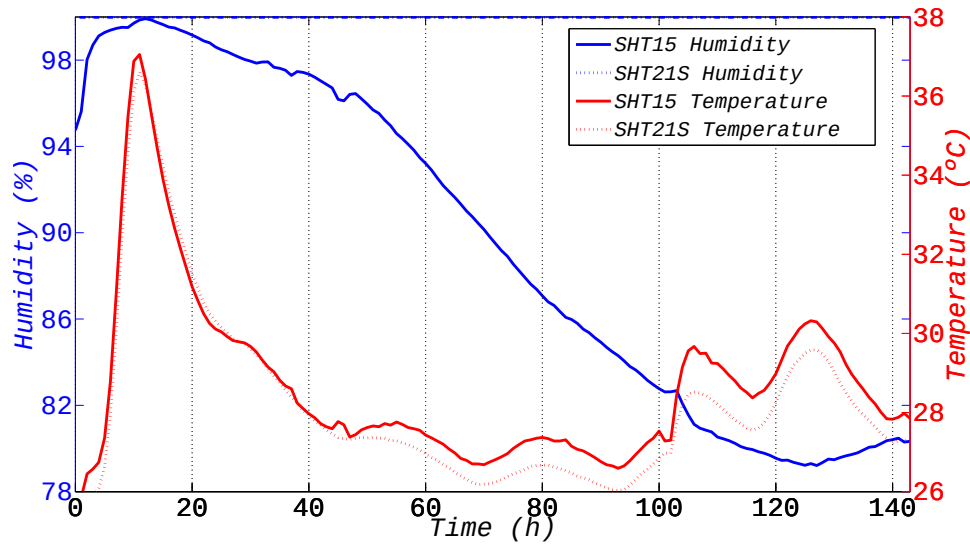


Figure 3.37: Humidity and temperature results obtained using the SHT15 and SHT21S inside a mortar shell for 100 hours.

3.2.8 Limitations and Challenges

In this work, we proposed several tiny systems, capable of (but not limited to) measuring both temperature and humidity, within concrete structures. In the context of sensing devices (i.e., the SHT15 and SHT21S sensors) only the sensor is inside the structure (the instrumentation, test control, and data acquisition is outside the structure allowing for using the same sensor and different acquisition systems, if needed). However, the proposed systems are battery operated. Hence, the service lifetime of the electronic components could be a major concern if there is no possibility to replace batteries and energy harvesting is not exploited in the mote. The need for a system with long-term lifetime is a major concern. To overcome the service lifetime limitation of the electronic components, energy harvesting systems must be addressed facilitating to extend the service lifetime (e.g., by using solar panels or thermal energy scavengers).

In remote monitoring scenarios, the data needs to be transmitted wirelessly. Hence, there is a need to study the influence of the concrete material in the transmission of data (e.g., interference of electromagnetic field of steel bars), in order to provide a general-purposed solution that could be applied not only to new structures but also in the existing ones. From the experimental point of view, we only have measured the humidity and temperature in a single point inside the concrete cube, so a creation of a system allowing for a distributed multipoint humidity and temperature measurement set up is envisaged as future research.

3.2.9 Summary and Conclusions

This Section addresses the development of an automatic measurement system allowing for monitoring the temperature and humidity within civil engineering structures. This system can be very useful when carrying out large works in concrete, such as dams or bridges where the volume of concrete involved is massive. Since the curing process is the process that defines the concrete quality, if the values of humidity and temperature are known, the premature drying of the concrete surface can be avoided by hydrating it. This decreases cracking and increases concrete quality. Moreover, this system can be implemented in existing structures where the concrete is going to be applied in an aggressive environment, therefore preventing corrosion of the reinforcement steel. Several types of hardware implementation have been conceived in order to read the temperature and humidity inside a concrete cube. A wireless sensor network has been created based on the IEEE 802.15.4, allowing for the creation of a continuous monitoring system capable of sending data wirelessly. In this network, the motes used two types of sensors, the SHT15 and SHT21S ones, to read both humidity and temperature, in real-time and continuous monitoring basis. The obtained results show the two types of sensors and the measurement procedure have highly potential for inexpensive concrete structure monitoring. However, during the first set of experiments the SHT15 temperature sensor stopped working after one day. Besides, after four days, the same happened to the humidity sensor. The temperature readings from the SHT21S sensor have been successfully performed during the first 16 hours of the experiment while the humidity values were successfully obtained for the first 21 hours. After this period the sensor went off. The initial sets of results were very promising, although SHT15 and SHT21S sensors went off after some time inside concrete. This is explained by the fact that the components of the sensors do not resist to concrete high relative humidity alkaline environment. The experiments carried on also shown that a porous cement mortar could be used as shell to protect sensor wire connections. High porosity of this mortar shell easily allows moisture and temperature measures of involving concrete. Still this solution does not protect sensors of the alkaline environment. In the second set of experiments, the SHT15 and SHT21S sensors were shielded by a filter cap, so that they are not affected by the alkaline environment, allowing for real-time and continuous monitoring basis. The SHT15 and SHT21S sensors are working since the beginning of this second phase of the experimental research work, for more than two months. One verifies that there is a perfect match between the measured values for the humidity and temperature and the ones obtained by the sensor probe, which confirms the potential of the proposed wireless sensor monitoring approach. Finally, it is worth mentioning that the solutions involving WSNs have a tremendous potential in real time structural health monitoring, since it reduces the cost and prevents from the risks associated to monitoring systems (e.g., inaccuracy in the measured values or negative impact of dangerous environments) in the measurement procedure.

3.3 Precision Agriculture - InterNodal Network Project

3.3.1 Introduction

WSNs are networks composed by several sensory devices (i.e., sensor nodes) on the basis of a non-hierarchic organization (ad-hoc network) that can detect, convert and transmit physical characteristics from the surrounding environment where they are placed. In contrast with ad-hoc networks, WSNs normally have a node(i.e., Master node) or a special terminal to which

all the communications converge, and where the information is stored. From the point of view of distributed systems [HSI⁺01], one sensor network can be defined as a particular class of distributed systems, where low level communications do not depend from the topological location of the network. However, from the point of view of organization, WSNs and Mobile Ad-hoc Networks (MANETs) are identical, since they have computational elements/nodes that communicate directly among them, through wireless chains or paths. However, the MANET organization has as the basic function of supporting the communication between computational elements, which individually can execute different tasks while WSNs purpose is normally more specific. The WSNs [KW05] have specific characteristics different from common networks. One of the characteristics is the typical centralization of data, i.e., in WSNs, sensor nodes must take care of the specific application requirements. Nodes are focused in only one measure or in a small set of measures, needing data processing inside the network. The tolerance to failures, due to the fact that the sensors nodes are low cost ones, is another characteristic of the WSNs. Errors can occur due the energy failure, lack of wireless connection missing, lack of stability in software, or other unknown problem.

Another important characteristic is scalability. As the sensor nodes have low cost and reduced size, it is possible to build up dense networks with high number of nodes.

The low consumption of energy is another basic characteristic of these systems and energy supply to sensor nodes is difficult in nature. Therefore, the nodes must cooperate between them in order to deliver the data in an energy efficient way, e. g., by using multi-hop data communication. Besides, an efficient MAC (Medium Access Control) protocol has to be implemented in order to have efficient node energy management for transmission, reception and sleep modes. Sensor nodes must be in sleep-mode whenever they are not receiving, or processing, or transmitting data packets.

The main goals of this WSN is to build a versatile, portable, auto-configurable and bi-directional wireless network:

- **Versatile:** The network coordinates all the nodes communication from a base-station - Master node - which is the interface with a PC through an Universal Serial Bus (USB) connection, or even through Ethernet, Internet or Wi-Fi communication protocols, depending on the operator choice;
- **Portable:** As sensor nodes are small and light autonomous electronic units, they can adapt to different topographical profiles;
- **Autoconfigurable:** The sensor nodes have the ability to find appropriate paths to establish the best communication between them and with Master node, checking the received power level every time a configuration is built up;
- **Bidirectional:** The sensor nodes send the transduced physical values to the Master node in near real time. The Master node, in turn, sends commands to the sensor nodes;
- **Scalability:** The number of wireless sensors in the network is only limited by a particular hardware configuration.

3.3.2 Sensor Nodes

Sensor nodes, so-called Data Acquisition Processor Radio (DAPR) nodes, are the portable wireless sensor devices of the InterNodal network. They collect the physical data values within the

environment where they are placed and send, to sink (Master) node. They are also able to send data information proceeding from another DAPR node to the Master node, or even to another DAPR node. They also receive information sent by the Master node.

The InterNodal Network has a Master node and one or several DAPR nodes, Figure 3.38. DAPR nodes collect the physical data environment values and retrieve them to the Master node. Communication can be single-hop or multi-hop. In the latter case other DAPR nodes are used as relays. Therefore, DAPR nodes also receive and process information sent by the Master node or other DAPR nodes. The main characteristics of DAPR nodes are the following: i) low steady state energy consumption, ii) 10 pre-setable transmission frequencies, iii) maximum range of approximately of 250 meters in Line-of-Sight (LoS), iv) high data processing capacity with reduced speeds of clock, vi) possibility of expansion, vii) capacity to change the channel of transmission, viii) and to control the transmission power level. Each sensor node contains a microcontroller, a radio module (low power and short range), and a pin connector for the JTAG programming. The selected radio modules for this application are short range devices from Low Power Radio Solutions (LPRS), which operates at the 433 MHz Industrial, Scientific, and Medical (ISM) band. The selected microcontroller to be inserted in DAPR nodes is a Texas Instruments MSP430P-1232, which has low power supply requirements, considering its actual clock frequency.

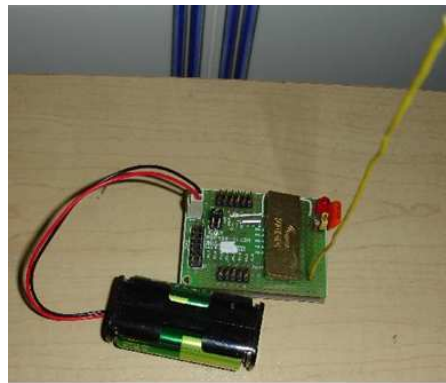


Figure 3.38: DAPR node.

Some of the components that are in the schematics belong to the Proto Board MSP430P-1232M [MSP12b]. The final view of a DAPR node used in the InterNodal network is presented in Figure 3.38. The electrical interconnection diagram from DAPR node is depicted in Figure 3.39.

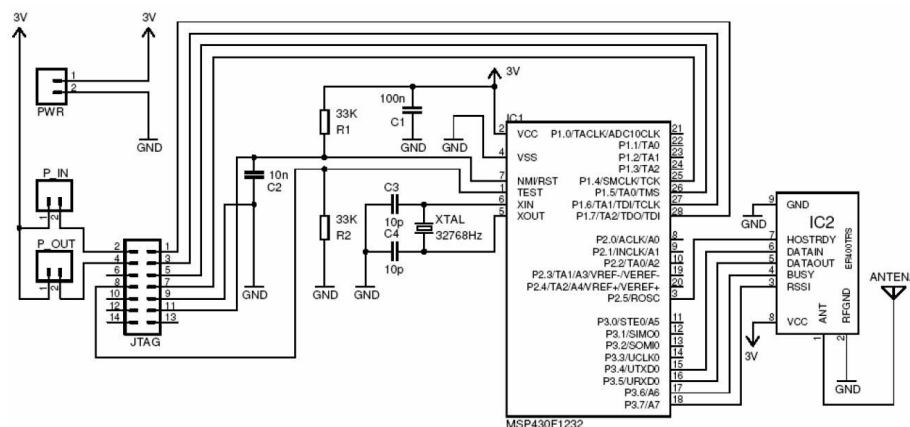


Figure 3.39: Circuit Diagram of DAPR node.

DAPR nodes have three typical supply current consumptions, see Table 3.1. The microcontroller is in sleep mode almost all the time. In short periods of time, when it is processing the arrival of a data package and/or when it has to prepare a data package to be sent, it has a significant power supply current consumption. Table 3.1 presents the microcontroller [MSP12a] and transceiver device consumptions at 3.3 V [ERA12].

Table 3.1: DAPR node consumptions.

Operating mode	Consumption
Hearing	21 mA
Emission (TX/RX)	25 mA
Sleep	121.6 μ A

3.3.3 Master Node

Sensor nodes are spreaded around all the InterNodal area. The Master node is used as a base station that coordinates the entire InterNodal network, including DAPR nodes and enables the interface with a computer through, e.g., a USB connection. The system administrator can operate and control the network via Ethernet, Internet or through Wi-Fi networks.

The Master node, Figure 3.40, is built up around a Telemetry USB-RF kit with a DLP-USB232M serial interface to a PC where the original program is running. It was developed in C++ for controlling and monitoring the InterNodal network.

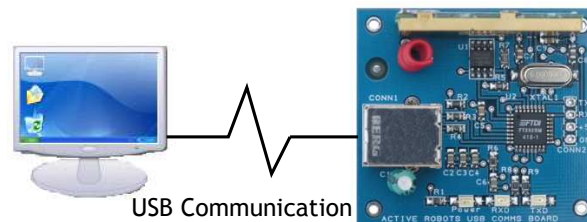


Figure 3.40: Master node connection to PC.

This interface allow for observing the physical data values received from DAPR nodes sensors in real-time (or near real time), as well as to save the historical values of the collected data. Besides monitoring battery voltage, the InterNodal network (applied to the agriculture area) also collects temperature, CO₂ level, moisture level, wind speed, or other functions (susceptible to be implemented), according to the user application. A particular characteristic of this program is the possibility of sending, through Short Message Service (SMS), the information of any DAPR node or even urgent alarms to the agricultural facility supervisor. The InterNodal network basic principle stands on the previous establishment of paths between nodes. During the InterNodal network automatic configuration procedure, each node is identified by a particular address, consisting of two bytes.

3.3.4 Setting an Automatic Configuration of InterNodal Network

The InterNodal network basic functioning principle stands on previously established paths between nodes through a network configuration procedure. Each InterNodal Network node presents a particular address, consisting 2 bytes. The first byte is called “Dominant Address”, and is the same for all the devices in the same network. The second byte must be unique for each node,

and must identify individually each node in the InterNodal network. The range of values for this second byte of address varies values between 1 and 63, being the 64th value reserved for the Master node.

Configuration algorithm

We have defined two concepts:

To give access - The node that gives access to the network sends a data packet to another node. It informs the other nodes signalling that it is already connected to the Master node, and that it accepts connections from other nodes, creating a path to the Master node;

To require access - The node that wants access to the network must wait that a node that gives access to the network sends a packet. When it happens, it should answer, sending a data packet to its interlocutor that it is connected to the network. *To require access* - The node that wants access to the network must wait that a node that gives access to the network sends a packet. When it happens, it should answer, sending a data packet to its interlocutor that it is connected to the network.

The network configuration process is the following one:

1. The Master node sends a command *to give access to the network*;
2. The DAPR node that *wants to have access to the network* answers to it, waiting for its turn, meaning that, after a given time as presented in Equation 3.8, in milliseconds, the DAPR node sends the answer to the other node;

$$2^{nd}byte\_from\_address \times 60 \quad (3.8)$$

3. The Master node waits for the reply of all nodes during a time, in milliseconds, given by Equation 3.9, while keeping the configuration of each node;

$$number\_of\_nodes\_in\_network \times 60 + 300 \quad (3.9)$$

4. After concluding the time period corresponding to a sensor node answer, the Master node asks indicate to all interlocutor nodes, one by one, to perform themselves make steps 1, 2 and 3;
5. After executing steps 1, 2 and 3, sensor nodes send a packet to the Master node, and it will record the paths of the established performed configurations;
6. Steps 4 and 5 are performed until all the nodes of the network gain access to the network;
7. After all this configuration phase, the Master node will go its normal functioning, i. e., it starts to collect and to deliver data to each node;

Maximum configuration time

The maximum configuration time for all wireless sensors can be calculated by Equation 3.10

$$(num\_node\_in\_network \times 60 + 300) \times (num\_node\_in\_network + 1) \quad (3.10)$$

By using Equation 3.10, one obtains the results from Table 3.2, where the time spent for the configuration of the network is presented, as a function of the number of used DAPR nodes.

Table 3.2: Table with configuration times computations.

Number of DAPR nodes	Time		
	t [ms]	t [s]	t [m]
4	2700	2.7	0
8	7020	7	0
16	21420	21.4	0.36
32	73260	73.3	1.22
64	269100	269.1	4.49

Communication protocol

All the communication between nodes is made based on a specific data packet that consists of a byte sequence, and allows for a correct exchange of data between Sender and Receiver. Any device that knows the format of this data packet, Figure 3.41, can communicate within the InterNodal network [BCVL07].

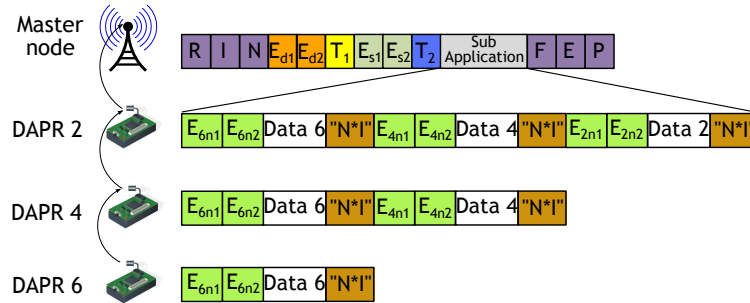


Figure 3.41: Multi-hop data packet.

3.3.5 Practical Results

Indoor results

To test the communication capabilities of the InterNodal network, the experimental nodes (three DAPR nodes and Master node) were spread along the University laboratories, Figure 3.42.

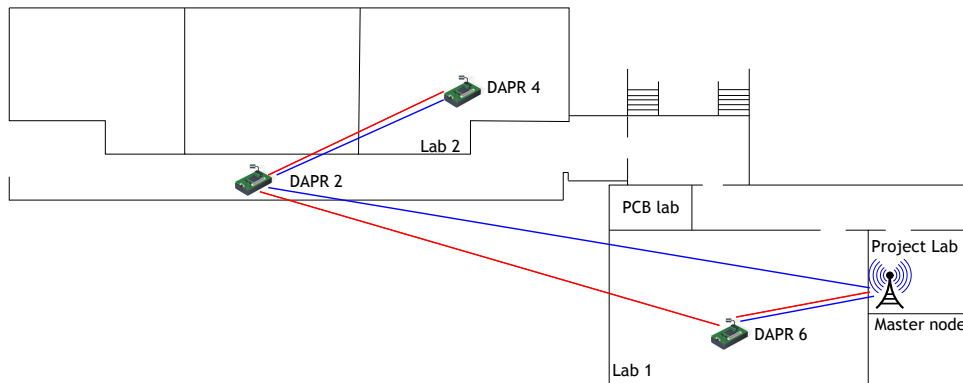


Figure 3.42: Plan of InterNodal network layout.

Table 3.3 presents the power received by each DAPR node (2, 4, and 6), and identifies the nodes that provide access to the respective DAPR node, from the Master node, in five different networks configurations. If the node that provides access to DAPR node is different from the Master node then there is multi-hop. As an example, it can be seen that for configuration

number 1, the multi-hop communication from DAPR node 4 reaches Master node through an initial hop from DAPR node 4 to node 2, and a final hop from node 4 to the Master node. Besides, node 6 is directly connected to Master node. Received power measurements were performed in each DAPR node for each deployment configuration.

Table 3.3: Data from InterNodal network indoor.

Configuration number	DAPR2		DAPR4		DAPR6	
	RSSI [dBm]	Accessing node	RSSI [dBm]	Accessing node	RSSI [dBm]	Accessing node
1	104	Master node	89	DAPR 2	104	Master node
2	103	DAPR 6	88	DAPR 2	104	Master node
3	105	Master node	90	DAPR 2	102	DAPR 2
4	102	Master node	89	DAPR 6	105	Master node
5	102	DAPR 6	89	DAPR 6	103	Master node

Outdoor results

To further demonstrate the potentialities of WSNs we present results from our InterNodal network practical tests in an agricultural facility. The DAPR nodes were placed on the field at a variable distance from each other, but the master node was always at a fixed position. By using the developed computer programs, several tests were made to measure the received power in each DAPR node. The DAPR nodes were deployed on a field with a 2 % of slope, as presented in Figure 3.43.

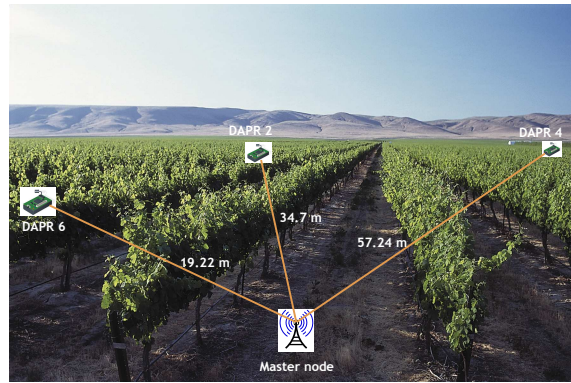


Figure 3.43: InterNodal network deployment.

The distance from the Master node to node 4 is about 58 meters, while the distance to node 6 it is about 19 meters, and to node 2 it is about 35 meters.

Table 3.4: Data from InterNodal network outdoor.

Configuration number	DAPR2		DAPR4		DAPR6	
	RSSI [dBm]	Accessing node	RSSI [dBm]	Accessing node	RSSI [dBm]	Accessing node
1	93	Master node	104	DAPR 2	103	Master node
2	100	DAPR 6	104	DAPR 2	101	Master node
3	110	Master node	111	DAPR 2	101	DAPR 2
4	105	DAPR 6	104	DAPR 6	100	Master node

All the nodes were placed at a height of 1.30 meters from the ground. Table 3.4 presents the power received by each DAPR node (2, 4, and 6), and identifies the nodes that provide access to the respective DAPR node from the Master node in four different networks configurations. If it is different from the Master node, then there is multi-hop. As an example, it can be seen that for configuration number 2, the multi-hop communication from DAPR node 4 reaches Master node through an initial hop from DAPR node 4 to node 2, followed by a connection from node 2 to node 6, and a final hop from node 6 to the Master node.

Measurements of the received power were performed in each DAPR node for each deployment configuration. From a given configuration to the next one, a reset operation was performed, cleaning all the connections between nodes (DAPR nodes and Master node). By analyzing the results, the received power from DAPR node 6 is larger than the one from the remaining DAPR nodes, which is according to our expectations as the distance between each DAPR node and the Master node increases while the received power decreases.

3.3.6 Summary and Conclusions

This Section addresses the conception of an entire WSN, for precision agriculture monitoring purposes. This WSN is capable of establishing all the network connections, in a automatic way, and it measures physical values from the surrounding environment in a vineyard, triggering devices that are attached to sensor nodes. Examples are temperature, CO₂ level, moisture level and wind speed. The WSN itself (sensor nodes, master node, monitor software, and sensor node firmware) was developed, and all protocols used in data exchange communications were started from the scratch.

All the tests of the automatic configurations of the experimental InterNodal network in outdoor and indoor scenarios presented 90 % of success meaning that, in ten attempts to configure the network only one attempt of automatic configuration was not successful, i.e., the interconnection of all the wireless sensors nodes of the network was not achieved. This event can be justified by the attenuation of the transmitted signal, e.g., owing to obstacles.

It is important to consider the possibility of expanding the InterNodal network, and enabling a simple implementation in other operation scenarios of operation. The versatility of this network allows, through additional electronic components, to measure any physical values extracted from transducers and redirect them to the Master node by independently changing the internal size of buffers in each DAPR node. Besides, each sensor node can receive a specific calibration routine for its own electronic sensor, adjusting transducer characteristics to physical environment changes. This network provides information in real time, and controls DAPR nodes. It allows for establishing control points for the sensors (set points) and has the capability to trigger alarms when an emergency situation appears, e.g., voltage drops in batteries, imperfections of analogue-digital conversion, etc. As future works the InterNodal network can be improved aspects like mobility, use of a Microprocessor with more memory Random Memory Access (RAM), use of clean energies and support of new MAC protocols.

3.4 Final Remarks

This chapter addressed three possible WSN applications established in different scenarios. The Smart Clothing application comprises a WBAN suitable to monitor the foetal movements in the last four weeks of low risk pregnancies. The concrete structure monitoring application is addressed in the context of a WSN scenario with local monitoring of possible crackings in the concrete structure. The agriculture scenario represents an outdoor open-field environment, very common in the original WSN concept. The WSN nodes allows for monitoring physical values from the surrounding environment in a vineyard, triggering devices that are attached to sensor nodes.

Chapter 4

Medium Access Control and Physical Layers in WSNs

This chapter is organized into nine parts. The Section 4.1 presents the protocol stack for WSNs as well as the different layers that compose it. Section 4.2 briefly discusses the protocol stack commonly assumed for WSNs while presenting a comparison with other protocol stack models. Section 4.3 describes some basic wireless radio families systems, as well as the evolution of the IEEE 802 standards until the appearing of the IEEE 802.15.4 standard. Section 4.4 briefly discusses the relationship between the IEEE 802.15.4 and ZigBee standards. Section 4.5 presents an overview of the IEEE 802.15.4 standard compliant PHY layer, followed by the Section 4.6, which is dedicated to the MAC layer and its different tasks. Section 4.7 presents the state-of-the-art on MAC protocols for WSNs and proposes a taxonomy for MAC protocols (extra details are given in Section G.3 from Appendix G). MAC protocols are classified into different categories, which depend on the technique employed to access the channel, whilst considering that one MAC protocol may utilize multiple techniques. In Section 4.8, a summary of the MAC characteristics is presented in order to classify and taxonomize the state of the art on MAC protocols for WSNs. Finally, in Section 4.9 conclusions are drawn. Complete details on the IEEE 802.15.4 standard PHY layer are addressed in Appendix F. The MAC protocols comparison tables for the proposed taxonomy are presented in Appendix G.

4.1 Protocol Stack for WSNs

A protocol stack is defined as the aggregation of the network protocols that are divided into several distinct layers, depending on their functions. For each layer, a set of interfaces are defined, leading to a more flexible adaptation when there are changes in the software and hardware. Each layer has certain services to offer to the higher layers, while protecting the details and the primitives of how the services of the layer are implemented. Therefore, each layer hides a considerable complexity and could be faced as a “middleware”, which offers services to the layer above it. When the layer interacts with the layer below it, then a functionality could be implemented. The model widely used for the protocol stack is the Open Systems Interconnection (OSI) model [PTR06], which embraces seven layers: i) Application, ii) Presentation, iii) Session, iv) Transport, v) Network, vi) Data Link and vii) Physical Layers. As the WSNs applications requirements are quite different from the normal desktop applications usually, the WSNs only make use of five layers: Application, Transport, Network, Link and Physical Layers. In this simplified representation, the Middleware Layer implements API for WSN applications, and is presented with a different colour because it can be seen as part of the application layer. Figure 4.1 presents a comparison between the OSI model [PTR06], WLAN computer protocol stack [KHH05a] and OSI model for WSNs.

The five layers of the OSI model for WSNs are as follows:

- **Application Layer:** The top layer of the OSI model for WSN is the application layer. It offers network services and the functionalities for the node by using the network appli-

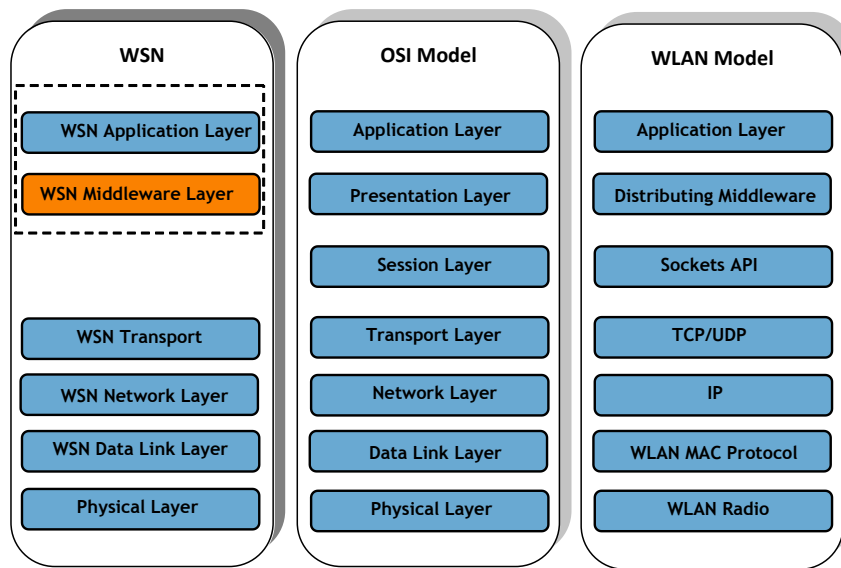


Figure 4.1: Comparison between the WSN OSI, OSI and WLAN computer models.

cations. This layer contains several processes that could be executed in parallel, e.g., sensing applications for different sensors, actuator and node diagnostics. The application layer configuration could be changed, depending on the application requirements, e.g., in an office building environment control application, a node can be configured to have any of the four functionalities: control node, sensor node, actuator node and interface node. Besides, this layer defines the format of exchanged messages and the order of message exchanges between different processes. This means that the application layer makes the hardware and software of the lower layers transparent to the end-user;

- Transport Layer:** The transport layer lays below the application layer. It performs the flow control through the network. The flow control should be made when the receiver of a data stream is temporarily unable to process incoming packets, due to the possible lack of memory or processor power. But flow control has not been a research issue in WSN. Besides the transport layer is responsible for upper layer error control in order to detect and repair losses of packets that were not detected by Data Link Layer (DLL), by using appropriate mechanisms. Since, in WSNs, the nodes operate at low transmission power levels, in order to save energy, link reliability is much worse than in conventional wired and wireless networks. Therefore, the flow and error control should be done separately for each hop than end-to-end, as in conventional networks [KW05]. Another task assured by the transport layer is the congestion control. Congestion occurs when more packets are created than the ones the network can carry out, and the network starts to drop packets. When a network starts to drop packets it will reflect in a waste of energy and it will decrease the reliability or information accuracy. The transport layer tries to avoid this situation or to solve it in a fair manner. One important way to avoid congestion is to control the rate at which packets are generated by the sensor nodes. Besides, the transport layer performs the fragmentation task in order to divide the upper layer application data into small segments appropriate for DLL and on the other hand, the transport layer reorders and join the received data segments into data packets suitable for application layer. Other feature is the network abstraction of the transport layer where it offers a programming interface to applications, covering the latter from the

many complexities of data transport;

- **Network Layer:** The network layer is located below the transport layer and is responsible for the network self-configuration and data routing. In order to configure the network topology the network layer selects an appropriate operation mode for a node and determines the most suitable neighbours with which to associate and establish communication links. The exchange of routing information process takes place either periodically, set by the network administrator or designer, or it is triggered based on events, i.e., when the routing information changes in order to ensure the network connectivity while optimizing network lifetime by balancing energy consumption among other nodes in the network. The routing protocol is responsible by the decision of the suitable next-hop node in which to forward each data frame in order to the frame eventually reaches its desired destination. In the overall of the WSN protocol stack a routing protocol executed in the network layer performs end-to-end data routing. Routing packets from the source node to the destination, through the wireless multi-hop network is the main function of this layer but it is challenging in WSNs considering the computational and energy constraints of the nodes and the network-wide function that it needs to accomplish. The routing algorithm is in charge of finding the best possible path from source to destination. It utilizes the routing information collected by the node through the routing protocol to find such route. The best possible path is chosen according to some predefined optimization criteria related to the network or application needs. For example, the simplest routing algorithm is find the shortest path, as it is the path that utilizes the least amount of network resources and the path that should provide the best delay. Once the routing protocol and algorithms are run, each node should have a routing table that tells the node which is the most appropriate neighbour to forward the packet to in order to reach the destination through the best possible path. Other consideration to remind is the energy costs of lower protocol layers caused by associations and neighbour discoveries that should also be considered [ZZJ09, KSK⁺08];
- **Data Link Layer (DLL):** Below the network layer is located the DLL that makes the interface between the physical and the network layers. It is constituted by a MAC sublayer and a Logical Link Control (LLC) module, where the MAC sublayer provides a fair mechanism to share access to the medium among other nodes and determines how and when to utilize PHY functions. MAC sublayer plays a key role in the maximization of a node's energy efficiency. The LLC operates above MAC and is responsible for encapsulating message segments into frames and adding appropriate header information, with destination and source addresses and control and sequencing information and CRC calculation. With the information contained in the frame it allows the desired destination node to receive a frame, ensure frame integrity and maintain proper sequencing of frames [KSK⁺08]. Therefore, the Data Link Layer plays an important role discovering new nodes. This may be the case in two situations: i) applications with mobile nodes, and ii) in re-deployments, because new nodes are re-deployed to bring the network back to its original operational level. In any case, the topology control thin layer needs to know about the existence of new neighbours before a new topology construction phase is triggered [ZZJ09];
- **Physical Layer:** The lowest layer in the WSN protocol stack is the PHY layer where implements a network communications hardware, which transmits and receives messages, one bit or symbol at a time. In a real sensor node the PHY receives analogue symbols

from the medium and converts them to digital bits for further processing in the higher layers of the protocol stack. In most transceivers the PHY functions available are the selection of a frequency channel and a transmit power, the modulation transmitted and demodulation of received data, symbol synchronization and clock generation for received data. The PHY transceiver may also include extra functions, which could lead to a reducing of processing requirements of the MicroController Unit (MCU). One example is the IEEE 802.15.4 compliant PHY that includes: data frame synchronization for perceiving the start of an incoming frame; Clear Channel Assessment (CCA) for detecting ongoing traffic in a frequency channel; Received Signal Strength Indicator (RSSI) and Link Quality Indication (LQI) for measuring signal strength and estimating link quality to neighbouring nodes; Cyclic Redundancy Check (CRC) calculation for checking bit errors on received frames; data encryption/decryption for improving network security; and automatic acknowledge transmissions after received frames. All these features mentioned above are implemented most efficiently in physical layer and can contribute to the overall network energy efficiency. But there is a trade-off when including more features at physical level because the increase of complexity can result in an increase of hardware costs. The physical layer includes theoretical aspects like propagation models, energy consumptions models and sensing and error models in WSN [KSK⁺08].

4.2 Other Protocol Stacks for WSNs

Besides the OSI model for WSN previously presented there are other authors that propose other type of protocol stack. However, although network stacks models are proposed by some authors, [Mah06], uniqueness of addresses may not be feasible or even required. But this protocol stack, is similar to the one used in MANETs, and is also the same stack used in TCP/IP networks, except for the addition of power, mobility and task management planes that operate across all the layers, as shown in Figure 4.2 While this layered approach has been accepted and mostly untouched in MANET networks for quite a long time, most researchers find serious difficulties to apply it in WSNs. The main arguments for this opposition are that WSN is very application-specific and resource-constrained; also a layered architecture may not be the best way to approach the wide range of applications and optimize the limited resources. Due to this, a cross-layer view of WSN is becoming more and more accepted in the research community.

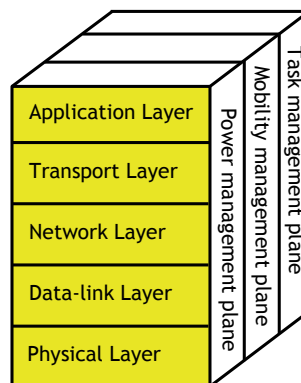


Figure 4.2: Proposed WSN protocol stack.

The proposed WSN protocol stack presents a crossing of all the layers in [ASSC02] the power, mobility and task management planes. The power plane emphasizes the power-awareness that

should be included in each layer and across all layers in WSNs. For example, a sensor may keep its radio on after sensing some activity in the channel, or it may turn it off if it is not generating any data or if it does not belong to any active route. A sensor that is running low in energy may turn off its radio and save its energy for sensing activities only. The mobility plane is responsible for maintaining the full operation of the sensor network even in the presence of sensor mobility. Nowadays, although most sensing applications we can think of are fixed, it cannot be discarded that sooner or later mobile sensing applications will emerge. This could be the case of sensors mounted on mobile platforms such as robots, persons, animals or cars. Routes used to carry information across the network have a limited lifetime and need to be periodically re-established because of node mobility. Even without mobility, routes may change due to the fact that nodes run out of power or follow an awake/sleep duty cycle; hence, a route that is valid at some instant in time may no longer be valid a little bit later [Nic05]. In both cases, the routing layer is mainly responsible for route maintenance.

The task management plane should be capable of coordinating all nodes toward a common objective in a power-aware mode. For example, some sensors in a given region, may be temporarily turned off if there is enough sensing redundancy from other sensors in that region.

The follow description simplifies the understanding of the main role of each of the three management planes:

- **Power management plane:** Manages how a sensor node how uses its energy; Each sensor node manages its own energy;
- **Mobility management plane:** Detects and registers the movement of sensor nodes, know its neighbours and balance their power and task usage; Knows others around;
- **Task management plane:** Balances and schedules the sensing tasks given to a specific region.

Other WSN protocol stack proposed by some authors is intituled as the data-centric architecture, Figure 4.3, where the WSN is mainly focused to the data. The main difference between the OSI protocol stack for WSN [GEWD05] is the fact that the blocks needed to build the sensor network usually span themselves over multiple layers while depending on each-other, as WSNs have to provide functionalities that are not present in traditional networks.

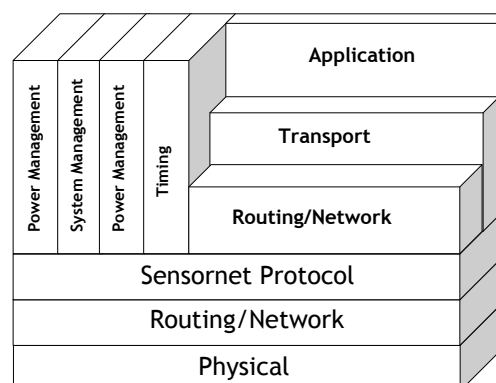


Figure 4.3: Sensor network data-centric stack models (SensorNet example).

Figure 4.4 presents a mapping of the main blocks onto the traditional OSI protocol layers. The service-centric model mentioned by the authors [GEWD05] consists of different layers, namely mission, network, region, sensor and capability layers, Figure 4.5.

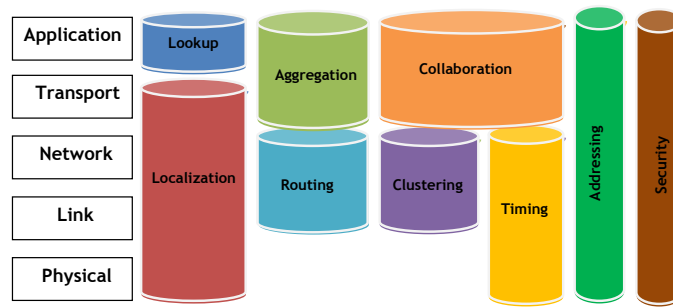


Figure 4.4: Functionality blocks over a WSN stack model.

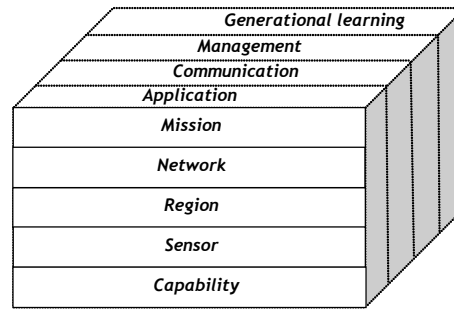


Figure 4.5: Layered model.

Each layer has associated semantics that use lower level components as syntactic units (except for the capability layer). Within each layer there are four planes or functionality sets normally the communication, the management, the application, and the generational learning ones. The combination of layers and planes enables a service-based visualization paradigm that can provide better understanding of the WSN. These planes do not constitute vertical segments in the model; instead they establish a group with similar functions. This grouping can be used as a reference point for mappings between layers.

The key benefit of using a service centric-model is a clear separation between the high-level purpose of the WSN (mission/services) and the low-level hardware specific capabilities of an individual sensor node (capability services). A mapping between mission and capability layers, created as a composition of mappings between intermediate layers, provides formalism for a service-centric description and evaluation of the WSN.

Hence, the layered model corresponds to a given level of detail that is used for visualization as follows:

- **Mission:** Presents a general status of the mission using the outline of the geographical location (terrain) where the WSN is located. The displayed information shows the status of a currently processed mission service(s);
- **Network:** Displayed as a collection of regions. Network traffic among regions indicates the overall level of activities in the WSN;
- **Region:** Individual nodes and traffic among nodes in a region are visible;
- **Sensor:** Individual sensor state and characteristics are shown;
- **Capability:** Individual sensor capabilities are shown.

4.3 Evolution of the IEEE 802 Standards

Nowadays, there are various types of wireless networks such as WLANs, Wireless Personal Area Networks (WPANs), Wireless Metropolitan Area Networks (WMANs), Wireless Wide Area Networks (WWANs), MANETs, WSNs and mesh network, Figure 4.6.

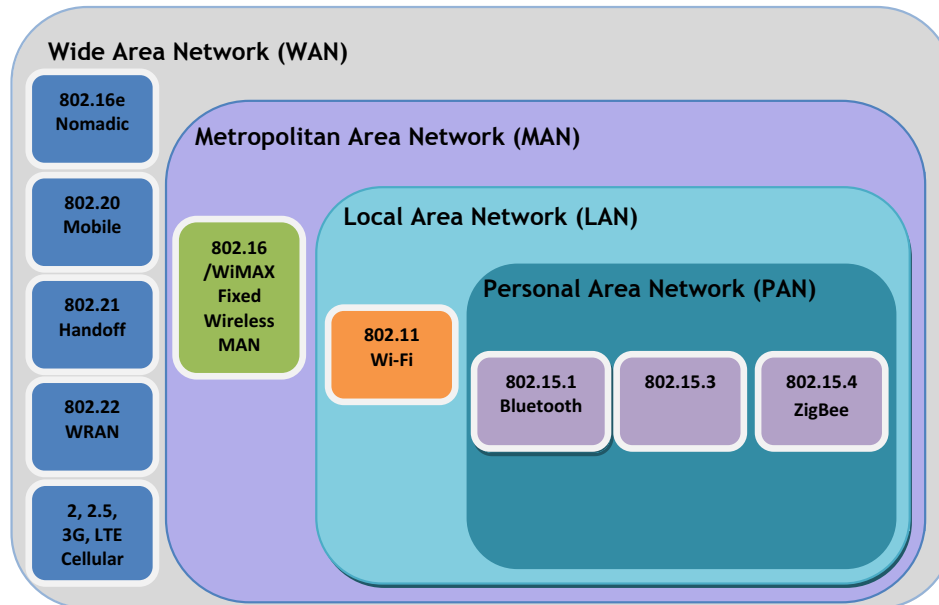


Figure 4.6: Wireless standards.

The evolution starts by IEEE 802.11 WLAN, which was created as the wireless extension of the IEEE 802 wired local area network. The IEEE 802.11b technology supported data rate varies from 2 to 11 Mbps and it has a range until 100 meters [IEE03c]. Then the development follows two directions from IEEE 802.11. One of the directions leads to a larger networking range, higher data throughput and it has QoS characteristics. The main applications purposes are the Internet, e-mail, data file transfer and even Internet Protocol Television (IPTV) in WMAN. In this category the WiMAX IEEE 802.16 standard is also included [IEE04].

The other direction of development led to a smaller networking range (and simple networks). The main targets applications are the WPANs, which are used to transmit information over relatively short distances among the participant devices. The family standards of IEEE 802.15.4 are defined in this category, differentiating from the others by the data rate supported, the battery drain and QoS. IEEE 802.15.3 is suitable for multimedia applications that require very high QoS [IEE03a], while IEEE 802.15.1 and Bluetooth are used for cable replacements in electronic devices from the consumer for voice applications [IEE02]. The IEEE 802.15.4 standard is used in applications that are not covered by the other 802.15 technologies. WPANs are divided into three classes, as shown in Figure 4.7: High-Rate (HR) WPANs, Medium-Rate (MR) WPANs, and Low-Rate (LR) WPANs [Far08]. An example of an HR-WPAN is IEEE 802.15.3 with a data rate of 11 to 55 Mbps. High data rates are helpful in applications such as real-time wireless video transmission from a camera to a nearby TV. Bluetooth, with a data rate of 1 to 3 Mbps, is an example of an MR-WLAN and can be used in high quality voice transmission in wireless headsets. If the objective is the long term usability, the power consumed by individual nodes in each of these networks needs to be managed efficiently. A subset of WPANs known as WSN and are specifically designed for very low power operation and thus deserve this degree of special attention.

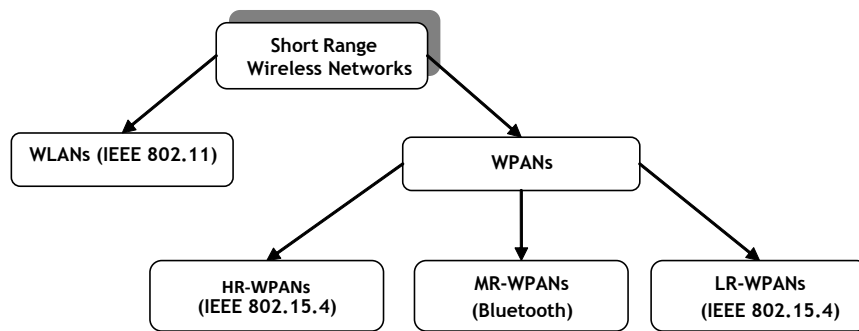


Figure 4.7: Short-range wireless networking classes.

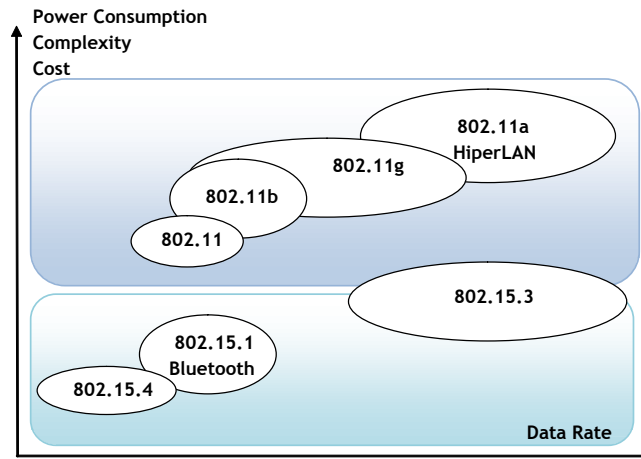


Figure 4.8: Power consumption in IEEE 802 based networks.

Figure 4.8 shows how these different types of networks are compared in terms of data rate and power consumption. The IEEE 802.15.4 standard shown in the figure is the one most widely used by WSN and will be presented in detail.

4.4 IEEE 802.15.4 and ZigBee

The first release of the IEEE 802.15.4 standard was issued in October 2003 by the Institute of Electrical and Electronic Engineers (IEEE) [IEE03b]. The IEEE 802.15.4 specified a standard where that enables a sensor rich environment. Then, the IEEE 802.15.4b Group focused on refining the IEEE 802.15.4, where the main objective was removing and addressing issues raised during early implementation efforts of IEEE 802.15.4 devices, resolving ambiguities, reducing unnecessary complexity, increasing flexibility in security key usage, considerations for newly available frequency allocations, and others. The revisions made by the group ended in 2006 and resulted in the release of an updated version from the original standard. In August 2007, another revision was made to the IEEE 802.15.4 of 2006 where it was added new alternate PHY layers, such as UWB PHY layer at frequencies of 3 GHz to 5 GHz, 6 GHz to 10 GHz and less than 1 GHz and a Chirp Spread Spectrum (CSS) PHY at 2450 MHz. The revision states that UWB PHY supports an over-the-air data rate of 110 kbps, 6.81 Mbps and 27.24 Mbps. The CSS PHY supports an over-the-air data rate of 1000 kbps with option of 250 kbps. The PHY layer depends on the region local regulations, type of application [IEE07].

The IEEE 802.15.4 describes the PHY layer and the MAC layer for WPANs. Usually there is a confusion between IEEE 802.15.4 and ZigBee (ZigBee Alliance 2005), which corresponds to the

specification developed by the ZigBee Alliance [Far08]. The ZigBee[®] protocol (ZigBee Alliance 2005) specifies the protocol layers above IEEE 802.15.4 to provide a full protocol stack for low-cost, low-power, low data rate wireless communications. The ZigBee[®] standard defines the networking, application, and the security layers of the protocol and adopts IEEE 802.15.4 PHY and MAC layers as part of the ZigBee[®] networking protocol and any ZigBee-compliant device conforms to IEEE 802.15.4 as well. Therefore, it is possible to create short-range wireless networks using only the IEEE 802.15.4 without implement the ZigBee[®] layers.

The ZigBee[®] Alliance adopted themselves the IEEE 802.15.4 standard for WPANs [Far08]. The Stack Architecture of the ZigBee[®] is represented in Figure 4.9 using the IEEE 802.15.4 specification and only defines the network, security and application layers.

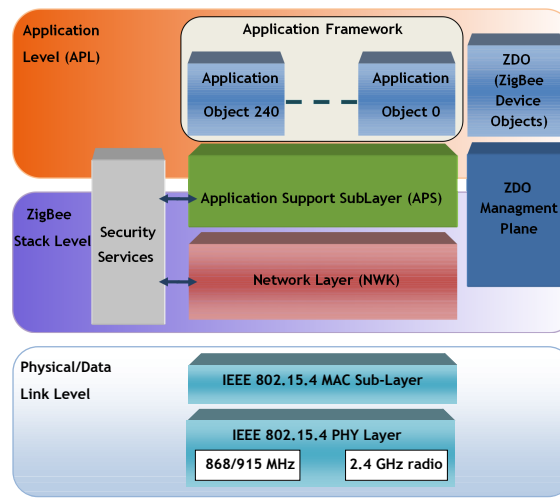


Figure 4.9: ZigBee[®] functional layer architecture and protocol stack.

The Application (APL) layer is the highest protocol layer in the ZigBee wireless network and hosts the application objects. Manufacturers develop the application objects to customize a device for various applications. Application objects control and manage the protocol layers in a ZigBee device. There can be up to 240 application objects in a single device. The ZigBee standard also offers the option to use application profiles in developing an application. An application profile is a set of agreements on application-specific message formats and processing actions. The use of an application profile allows further interoperability between the products developed by different vendors for a specific application.

The ZigBee Device Objects (ZDO) represents the ZigBee node type of device (End Device, Co-ordinator or Router), and has a number of initialization and communication roles, while the ZDO Management Plane is responsible by the spanning of the Application Sub Layer (APS) and Network (NWK) layers, and allows the ZDO to communicate with these layers when performing its internal tasks. It also allows the ZDO to deal with requests from applications for network access and security functions using ZigBee Device Profile (ZDP) messages.

The APS will be responsible to communicate with the application. For example to blink a LED the APS relays this instruction to the application using the endpoint information in the message. Also is responsible by the maintaining of binding tables and the sending of messages between bound nodes.

The NWK layer of a ZigBee coordinator is responsible for establishing a new network and selecting the network topology (tree, star, or mesh). The ZigBee coordinator also assigns the NWK addresses to the devices in its network. The NWK layer interfaces between the MAC and the

APL and is responsible for the management of the network formation and routing. The routing process is used to select the path through which the message will be relayed to its destination device. The ZigBee coordinator and the routers are responsible for discovering and maintaining the routes in the network, the ZigBee end device cannot perform route discovery and the ZigBee coordinator or a router will perform route discovery on behalf of the end.

The ZigBee technology incorporates security functionality, which is managed by the security layer. Different levels of security are available. The security functionality makes use of keys at different levels, as well as challenge-authentication procedures. The keys can be pre-configured within devices to increase security.

The IEEE 802.15.4 standard supports the use of Advanced Encryption Standard (AES) [oST01] to encrypt their outgoing messages.

Since IEEE 802.15.4 was developed independently of the ZigBee standard it is possible to build short-range wireless networking based solely on IEEE 802.15.4 without implementing ZigBee-specific layers. In this case, the users develop their own networking/application layer protocol on top of IEEE 802.15.4 PHY and MAC, Figure 4.10. These custom networking/application layers are normally simpler than the ZigBee protocol layers and are targeted for specific applications [Far08].

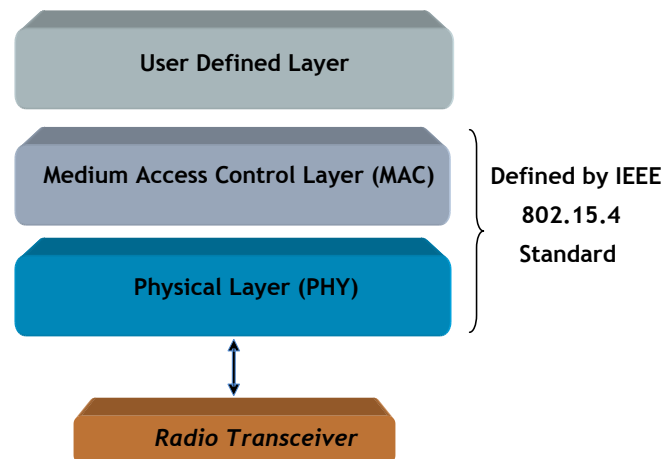


Figure 4.10: Network Protocol based on IEEE 802.15.4 and not conform to the ZigBee Standard.

4.5 IEEE 802.15.4 Physical Layer

The PHY layer main purpose is to establish an interface with the physical medium where the communications are done. The PHY layer is the lowest layer in the protocol stack for WSN and it is responsible by the control (enable and disable) the radio transceiver, energy detection, link quality, CCA, channel selection and the transmission and reception of message packets that are exchanged in physical medium [GCB03].

The IEEE 802.15.4 standard proposes three operational frequency bands: 868 MHz, 915 MHz and 2.4 GHz, as presented in Figure 4.11.

There is room for only a single channel in the 868 MHz band (20 kbit/s). The 915 MHz band has 10 channels (excluding the optional channels) with a bit rate of 40 kbit/s. The total number of channels in the 2.4 GHz band is 16 (250 kbit/s). In IEEE 802.15.4 standard there are three modulation types: BPSK, Amplitude Shift Keying (ASK), and offset quadrature phase shift keying (O-QPSK). In BPSK and O-QPSK, the digital data is in the phase of the signal. While in ASK,

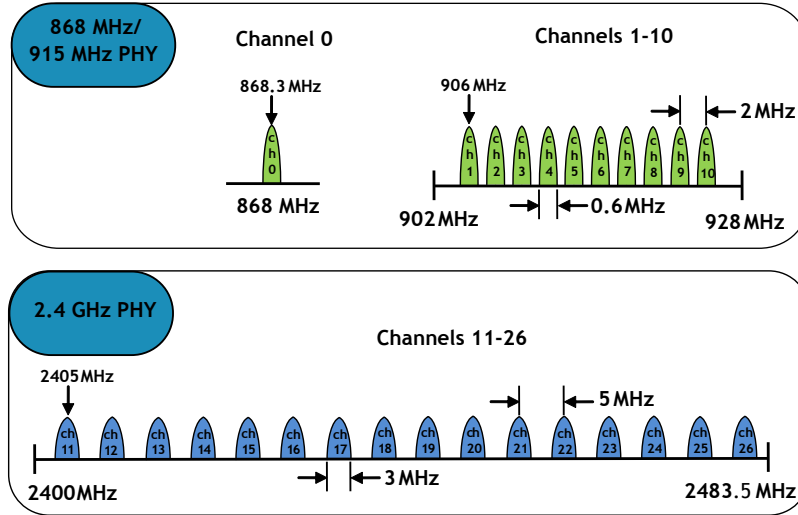


Figure 4.11: Channelization at the 868/915 MHz and 2.4 GHz bands.

the digital data is in the amplitude of the signal. All wireless communication methods in IEEE 802.15.4 utilize either DSSS or Parallel Sequence Spread Spectrum (PSSS) techniques. DSSS and PSSS help to improve performance of receivers in a multipath environment [SW04b]. Details about the IEEE 802.15.4 data rates and frequencies of operation along with the supported modulations are given in Appendix F.

The way how channelization, Figure 4.11, is done takes into account that in the 2.4 GHz band there are 16 channels, with each channel requiring 5 MHz of bandwidth. And for 915 MHz band there are 10 channels, with each channel requiring 2 MHz of bandwidth. The centre frequency for each channel for each band can be calculated as,

$$\begin{aligned}
 F_c &= 868.3 \text{ MHz}, ch = 0 \\
 F_c &= (906 + 2(ch - 1)) \text{ MHz}, ch \in \{1, 2, \dots, 10\} \quad (4.1) \\
 F_c &= (2405 + 5(ch - 11)) \text{ MHz}, ch \in \{11, 12, \dots, 26\}
 \end{aligned}$$

4.5.1 IEEE 802.15.4 Device Types

In IEEE 802.15.4 there are two types of devices that could appear in a wireless network:

- **Full Function Devices (FFDs):** These devices are capable of performing all the tasks described in the IEEE 802.15.4 standard and can play any role in the network;
- **Reduced Function Devices (RFDs):** These devices have limited capabilities in a WSN, since these devices can only communicate with an FFD and they are only meant to do simple tasks such as turning on or off a switch. The memory size is smaller than in an FFD device [Far08];

4.5.2 IEEE 802.15.4 Device Roles

In an IEEE 802.15.4 wireless network, an FFD device can support three different roles, Figure 4.12:

- **Personal Area Network (PAN) coordinator:** is the primary controller of PAN, which initiates the network and often operates as a gateway to other networks. Each PAN must have exactly one PAN coordinator;
- **Coordinator:** Is an FFD device capable of relaying messages using data routing and network self-organization operations to achieve it;
- **Devices:** Devices do not have data routing capability and can communicate only with coordinators [KSK⁺08].

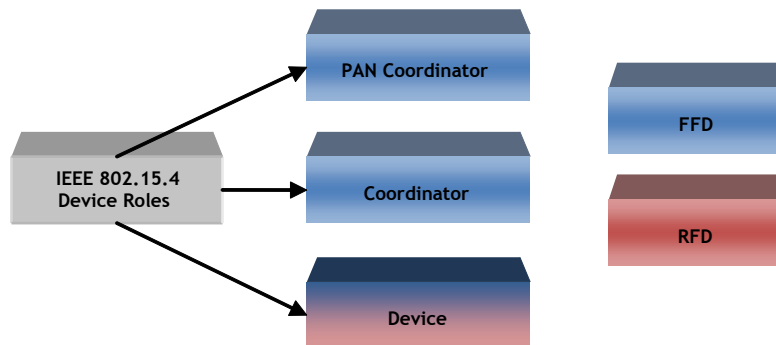


Figure 4.12: Device roles in the IEEE 802.15.4.

4.5.3 IEEE 802.15.4 Network Topologies

To overcome the limited transmission range of the wireless devices from a WSN, multi-hop self-organizing network topologies are necessary. The IEEE 802.15.4 standard supports three types of network topologies:

- **Star topology:** In the star topology, Figure 4.13, all devices establish a communication link with a single central controller, called the PAN coordinator.

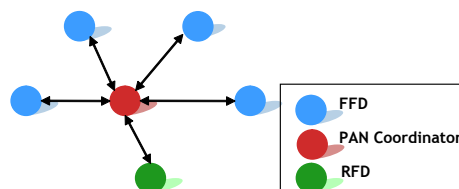


Figure 4.13: IEEE 802.15.4 star topology.

- **Peer-to-peer topology:** In the peer-to-peer topology, Figure 4.14, there is also one PAN coordinator and in contrast to the star topology each device can communicate directly with any other device if the devices are placed close enough together to establish a successful communication link.

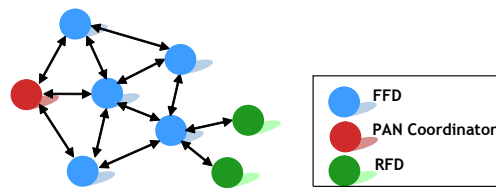


Figure 4.14: IEEE 802.15.4 peer-to-peer topology.

- **Cluster tree topology:** The cluster tree topology, Figure 4.15, is a special case of a peer-to-peer network in which most devices are FFDs and an RFD may connect to a cluster-tree network as a leaf node at the end of a branch.

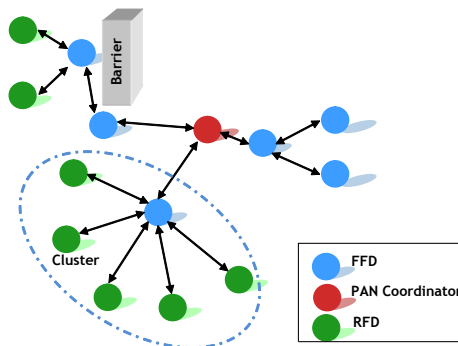


Figure 4.15: IEEE 802.15.4 cluster tree topology.

Further details concerning the IEEE 802.15.4 network topologies are discussed in Appendix F.

4.5.4 IEEE 802.15.4 PHY Specifications

The IEEE 802.15.4 standard not only specifies the PHY protocol functions and interactions with the MAC layer, but also defines the minimum hardware-level requirements. Hence, the physical layer of the IEEE 802.15.4 is responsible by the following tasks:

- **Receiver energy detection (EnD):** When a device plans to transmit a message, it first switches into the receive mode to detect and estimate the signal energy level in the desired channel. This task is known as energy detection. The receiver EnD measurement is used by a network layer as part of the channel selection algorithm;
- **Link Quality Indication (LQI):** The LQI main function is the indication of the quality of the data packets received by the receiver. To obtain the quality of the data packets received the device uses the Received Signal Strength (RSS) as a measure of the signal quality. The NWK layer can use for example the LQI information to decide which path to use to a message;
- **Carrier Sense (CS):** The CS technique is quite similar to the EnD technique and it is used to perform verification if whether a frequency channel is available to use. While in EnD the signal detected in the channel is not decoded, in the CS technique the signals is demodulated;
- **Clear Channel Assessment (CCA):** The CCA mechanism is the first step of the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) channel access mechanism when MAC requests the PHY to perform a CCA to the channel in order to detect that the channel is

not in use by any other device. There are three CCA modes defined in the IEEE 802.15.4 standard: i) CCA mode 1: the EnD result is the only one that is taken into account when performing CCA; ii) CCA mode 2: the CS result is the only one that is taken into account when performing CCA; iii) CCA mode 3: This mode is the result of a logical combination (AND/OR) of mode 1 and mode 2 in which the channel is considered busy if the detected energy level is above the threshold and/or a compliant carrier is sensed;

- **Channel Selection:** The IEEE 802.15.4 standard initial release has a total of 27 channels and the implementation of multiple operating frequencies bands could not be supported. Hence, the physical layer should be able to tune the radio transceiver in a specific channel when requested by a higher layer;
- **Activation and deactivation of the PHY radio transceiver:** The radio transceiver may operate in three different states: transmitting, receiving or sleeping. Upon a request of the MAC sub-layer, the transceiver switches in to one of the three main states: transceiver disabled, transmitter enabled, and receiver enabled. The standard recommends that the turnaround time from transmitting to receiving states and vice versa should be at least 12 symbol periods;

Details on the different tasks of the IEEE 802.15.4 PHY layer are given in Appendix F.

4.5.5 IEEE 802.15.4 PHY Packet Structure

The PHY Protocol Data Unit (PPDU), Figure 4.16, is the packet data structure at the PHY protocol level that modulates the wireless transmitter.

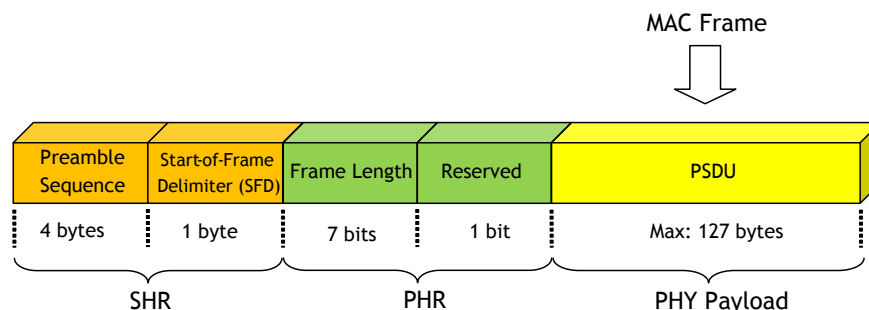


Figure 4.16: PPDU format.

The structure of the PPDU encapsulates all data structures from the higher levels of the protocol stack. In IEEE 802.15.4, the first bit that will be transmitted is the Least Significant Bit (LSB) of the SHR. The Most Significant Bit (MSB) of the last byte of the PHY payload is transmitted last. It consists of three components:

- **Synchronization Header (SHR):** Consists of two fields, a preamble and a Start-of-Frame Delimiter (SFD). The lengths and durations of the preambles in all PHY layer is resumed in Appendix F;
- **PHY Header (PHR):** It is a single 8 bit field with the MSB reserved and the remaining low order bits used to specify the total number of octets in the PHY payload.
- **PHY payload:** The PHY payload is composed of only one field called the Physical Layer Service Data Unit (PSDU). The PHY payload length can be any value from 0 to 127 bytes;

4.6 IEEE 802.15.4 MAC Layer

The MAC layer provides access control to a shared channel and reliable data delivery between the PHY and the next higher layer above the MAC. It is also responsible by: the generation of acknowledgement frames, support of PAN association and disassociation and the security control [Far08]. The IEEE 802.15.4 standard uses a CSMA-CA algorithm, which requires listening to the channel before transmitting in order to avoid collisions with other transmissions that are being performed using the channel and coordinators are required to constantly receive for possible incoming data [KSK⁺08]. The IEEE 802.15.4 MAC only supplies application support for the creation of the two wireless topologies already mentioned before: star topology and peer-to-peer topology. But the management of these topologies is done by the network layer and therefore is beyond the scope of IEEE 802.15.4 standard. The MAC layer only performs functions that are required by network layer. Applications that benefit from a star topology include home automation, Personal Computer (PC) peripherals, toys and games, and personal health care. The peer-to-peer topology is used in industrial and commercial application and then leading to the appearing of a more complex type of self-organizing wireless network (multi-hop/mesh networks). The MAC protocol transfers data as frames with a maximum size of 128 (bytes), which enables a maximum MAC payload of 104 (bytes), turning the IEEE 802.15.4 standard ideal for low data rate systems. The MAC protocol can operate on two operational modes:

- **The beacon-enabled:** The beacons are periodically sent by the PAN coordinator and when a device wishes to transfer the data to a coordinator it first listens to the medium for a network beacon frame. The beacon frame is responsible by the limits establishment for the beginning of a superframe and by the establishment of the time interval to exchange packets between different the nodes. The medium access is therefore performed using a slotted CSMA-CA. Since this mode is used in applications that require a certain amount of bandwidth and low latency, the PAN coordinator enables the allocation of some time slots in the superframe. These portions are called Guaranteed Time Slots (GTSs) and they are used when the node needs to have guaranteed services [Far08];
- **The non-beacon-enabled:** the PAN coordinator does not transmit regular beacons and therefore it transmits a data frame using a *non-slotted* CSMA-CA.

The operational modes in IEEE 802.15.4 can be listed as in Figure 4.17.

4.6.1 IEEE 802.15.4 Beacon-Enabled - Star topology

When considering a beacon-enabled star network topology the network device that wishes to send data to the PAN coordinator needs first to listen for a beacon. If a GTS is not assigned to the device, it transmits its data frame during the contention access period, after using the CSMA-CA technique. But if the GTS is assigned to the device then it waits for the right time within the superframe structure so that it can transmit its data frame. The PAN coordinator after receiving the data frame will send back an acknowledgement to the network device when the data transfer finishes. This message exchanges is shown in Figure 4.18.

In the case when the PAN coordinator has data waiting to be transmitted to a network device, it sets a special flag in its beacon. After that, when the destination network device detects that the PAN coordinator has data pending for him, it sends a data request message back to the PAN coordinator. The PAN coordinator responds with an acknowledgement followed by the data

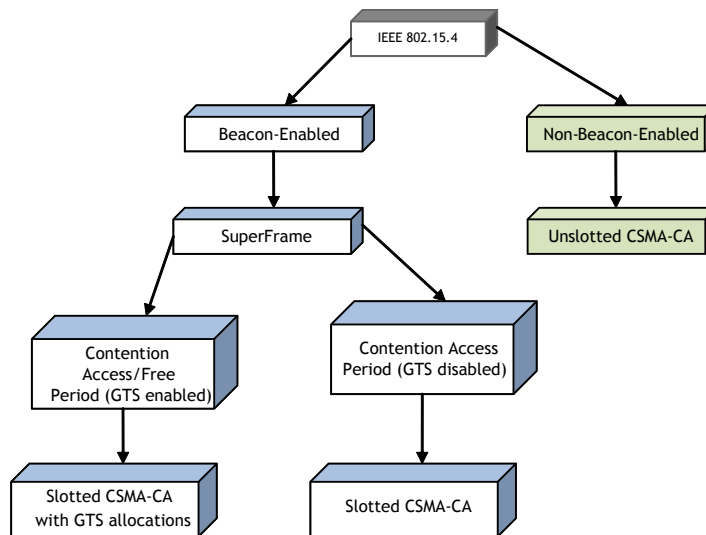


Figure 4.17: IEEE 802.15.4 operational modes.

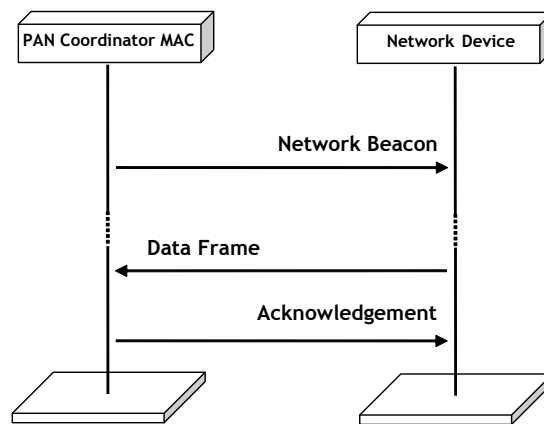


Figure 4.18: Star network data transfer from network device in a beacon-enabled network.

frame. In the end of the transmission the exchanging is finished with an acknowledgement sent from the network device. This process is described in Figure 4.19.

The IEEE 802.15.4 design group decided not to implement a combined acknowledgement/data frame in order to simplify implementation.

4.6.2 IEEE 802.15.4 Non-Beacon-Enabled - Star topology

When considering a non-beacon-enabled star network, the network device that wishes to transfer data it sends a data frame to the PAN coordinator using a CSMA-CA mechanism. Then the PAN coordinator responds to the network device, sending an acknowledgement message, as shown in Figure 4.20.

Following the same idea when the PAN coordinator needs to do a data transfer to a network device, it will keep the data until the network device sends a data request message. The PAN coordinator sends an acknowledgement message containing information indicating to the network device if there are data pending to be sent. Then the data will be sent immediately after the acknowledgement message. The transaction is finished when the network device acknowledges the reception of the data frame, as shown in Figure 4.21.

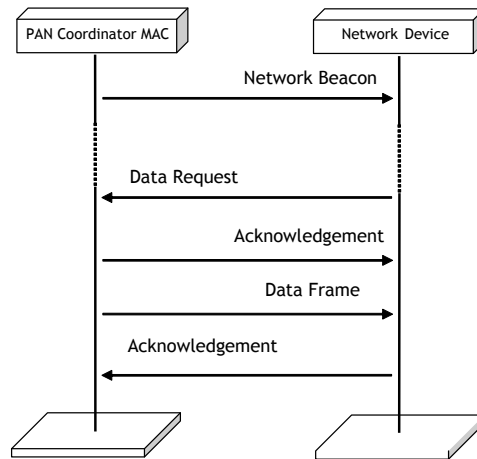


Figure 4.19: Star network data transfer from a PAN coordinator in a beacon-enabled network.

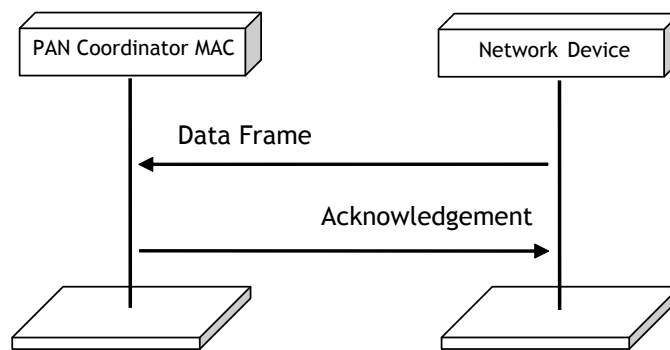


Figure 4.20: Star network data transfer from a network device in a non-beacon-network.

4.6.3 IEEE 802.15.4 Non-Beacon-Enabled - Peer-to-peer topology

For the peer-to-peer topologies the data transfer strategy depends on the network layer that is managing the protocol stack of the WSN. A network device may stay in reception mode while scanning the radio frequency channel for any communications present in channel or it can send “SYNC” messages in order to achieve synchronization with other potential listening devices.

4.6.4 SuperFrame Structure

The IEEE 802.15.4 standard includes an optional superframe structure. The superframe is managed by the PAN coordinator after regular intervals. The superframe is delimited by two beacon frames. Each beacon contains information that will help network devices synchronize to the network and includes the network identifier, the beacon periodicity and the superframe structure. In a superframe three types of periods can appear: the Contention Access Period (CAP), the Contention-Free Period (CFP) and the inactive period. During the CAP, if a device wants to transmit a packet then it will use a CSMA-CA mechanism in order to gain access to a frequency channel.

The probability of a frequency channel be available is equal to all the devices in the same network. When a device starts using an available channel will continue using it until it finishes the transmission of the packet. If the device detects the channel busy then it will back off a random time period and tries again.

The MAC command frames must be transmitted during CAP. During CAP there is no guarantee for any device that it will use the frequency channel exactly when it needs it. But during the

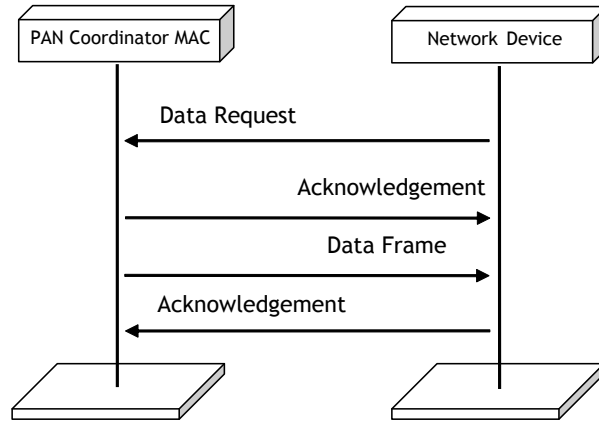


Figure 4.21: Star network data transfer from a PAN coordinator in a non-beacon-enabled network.

CFP it has to guarantee a time slot for a specific device and this device will not need to use a CSMA-CA mechanism for channel access.

The use of guaranteed slots in CFP is a good option when considering low latency applications and when a device cannot wait for a random period of time until channel is available. The use of a CSMA-CA mechanism is not allowed during CFP. The junction of the CAP and CFP is known as the active period and is divided into 16 contiguous equal time slots. The superframe with GTS is presented in Figure 4.22. The IEEE 802.15.4 allows up to seven GTSs in CFP and each GTS can occupy one or more slots. Each GTS is formed by an integer multiple of time slots and each time slot is equal to 1/16 of the time between the start of two successive beacons. A superframe may have an inactive period that allows a device to enter power-saving mode. During power-saving mode, the coordinator can turn off the radio transceiver in order to conserve battery energy [Far08].

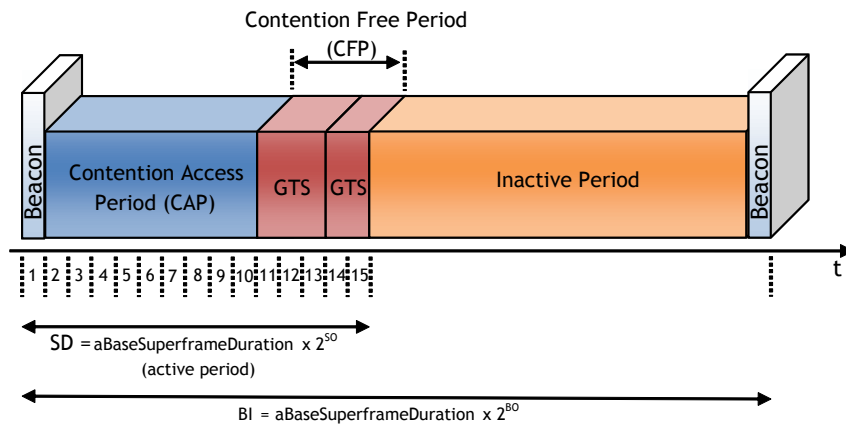


Figure 4.22: Superframe structure with GTS.

The superframe is configured by the Network (NWK) layer using *MLME-START.request* primitive. The Beacon Interval (BI) is defined as the duration between two consecutive beacons and is obtained by using the values of the *macBeaconorder* (BO) attribute and the *aBaseSuperframeDuration* constant. The value (in symbols) is obtained from the equation:

$$BI = aBaseSuperframeDuration \cdot 2^{BO} \quad (4.2)$$

The *macBeaconorder* can assume any value from 0 to 14 in a beacon enabled network. When

the value of *macBeaconorder* is set to 15, the network is assumed to be non-beacon-enabled and the superframe description will not be applied.

The same way as the BI value, the length (in symbols) of the active period of the superframe, Superframe Duration (SD), is obtained from the equation:

$$SD = aBaseSuperframeDuration \cdot 2^{SO} \quad (4.3)$$

Where SO is the value of the *macSuperframeOrder*. The superframe duration cannot exceed the beacon interval, and is given by the following relation.

$$SO \leq BO \quad (4.4)$$

When considering a non-beacon-enabled network (*macBeaconOrder* is equal to 15), the PAN coordinator will only transmit beacons if receives a beacon request command from a device in its network. A device uses the beacon request command in order to locate the PAN coordinator. The PAN coordinator in a non-beacon-enabled network sets the value of *macSuperframeOrder* to 15.

Now when a beacon-enabled network is assumed, any coordinator besides the PAN coordinator can transmit beacons and create its own superframe.

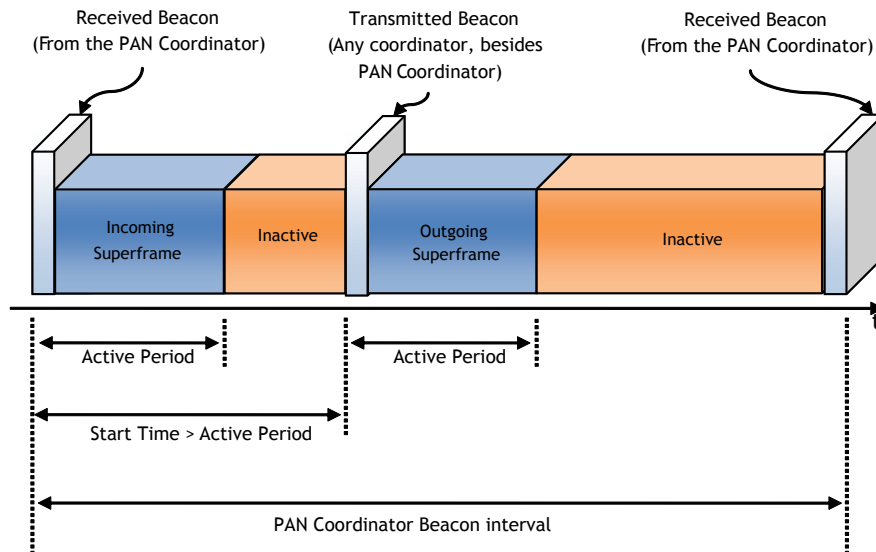


Figure 4.23: The incoming and outgoing Superframes temporal evolution.

Figure 4.23 presents the temporal evolution when both PAN coordinator and another coordinator, located in the same network, are transmitting beacons. The coordinator starts the transmission of its beacon only during the inactive period of the PAN coordinator superframe. For the beacon sent by the PAN coordinator the beacon is named as the received beacon and for the beacon of other coordinator the beacon is named as the *transmitted beacon*. The active period for both superframes must have the same length [Far08].

If a device from the network does not use its GTS for an extended period of time, the GTS will reach a timeout and the coordinator can then assign that GTS to a different device.

The inactive period present in Figure 4.23 is an integer multiple of twice the superframe length, while the value of this integer multiple (n^*) depends on the *macBeaconOrder* and is given by the following equation:

$$n^* = \begin{cases} 2^{8-\text{macBeaconOrder}} & , 0 \leq \text{macBeaconOrder} \leq 8 \\ 1 & , 8 \leq \text{macBeaconOrder} \leq 14 \end{cases} \quad (4.5)$$

The timing parameters in the beacon enabled operating mode are presented in detail in Appendix G. In addition, the InterFrame Spacing (IFS) feature is discussed in detail in Appendix G.

4.6.5 IEEE 802.15.4 MAC frames

The IEEE 802.15.4 standard [IEE07, Far08] defines four MAC frames structures:

- **Beacon frame:** It is used by the coordinator in order to transmit beacons that are used to synchronize the clock of all the devices located in the same network;
- **Data frame:** It is used to transmit data;
- **Acknowledge frame:** It is used to transmit an acknowledgement when a successful reception of a frame happens;
- **MAC command frame:** It is transmitted using a MAC command frame.

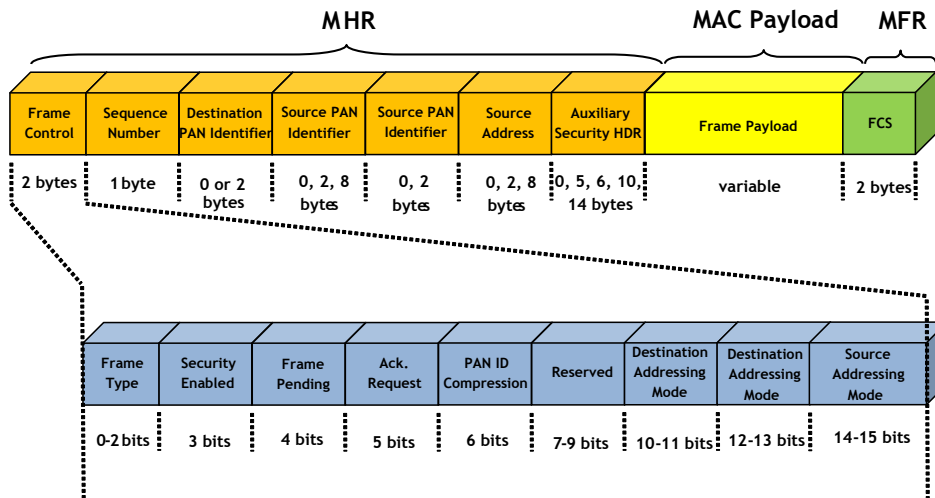


Figure 4.24: General MAC frame format and details of the frame control field.

The four different MAC frames structures considered in the IEEE 802.15.4 standard are described in detail in Appendix G.

4.6.5.1 CSMA/CA Mechanism

The IEEE 802.15.4 standard [IEE07] utilizes to access the channel the CSMA-CA mechanism. Nodes in clusters that operate in beacon-enabled mode must utilize the slotted CSMA-CA mechanism, with few exceptions.

When a device is using the CSMA-CA mechanism, whenever it wants to transmit, it performs a CCA first in order to ensure that the channel is not occupied by any other device. Then after being sure that no other device is using the channel it starts transmitting its own signal.

There are two situations on which a device accesses the channel without using the CSMA-CA algorithm:

- The access to the channel during the CFP;
- Transmit immediately after acknowledging a data request command. This can happen when a device requests data from a coordinator, the coordinator transmits the acknowledgement followed immediately by the data without performing CSMA-CA between these two transmissions, even during the CAP.

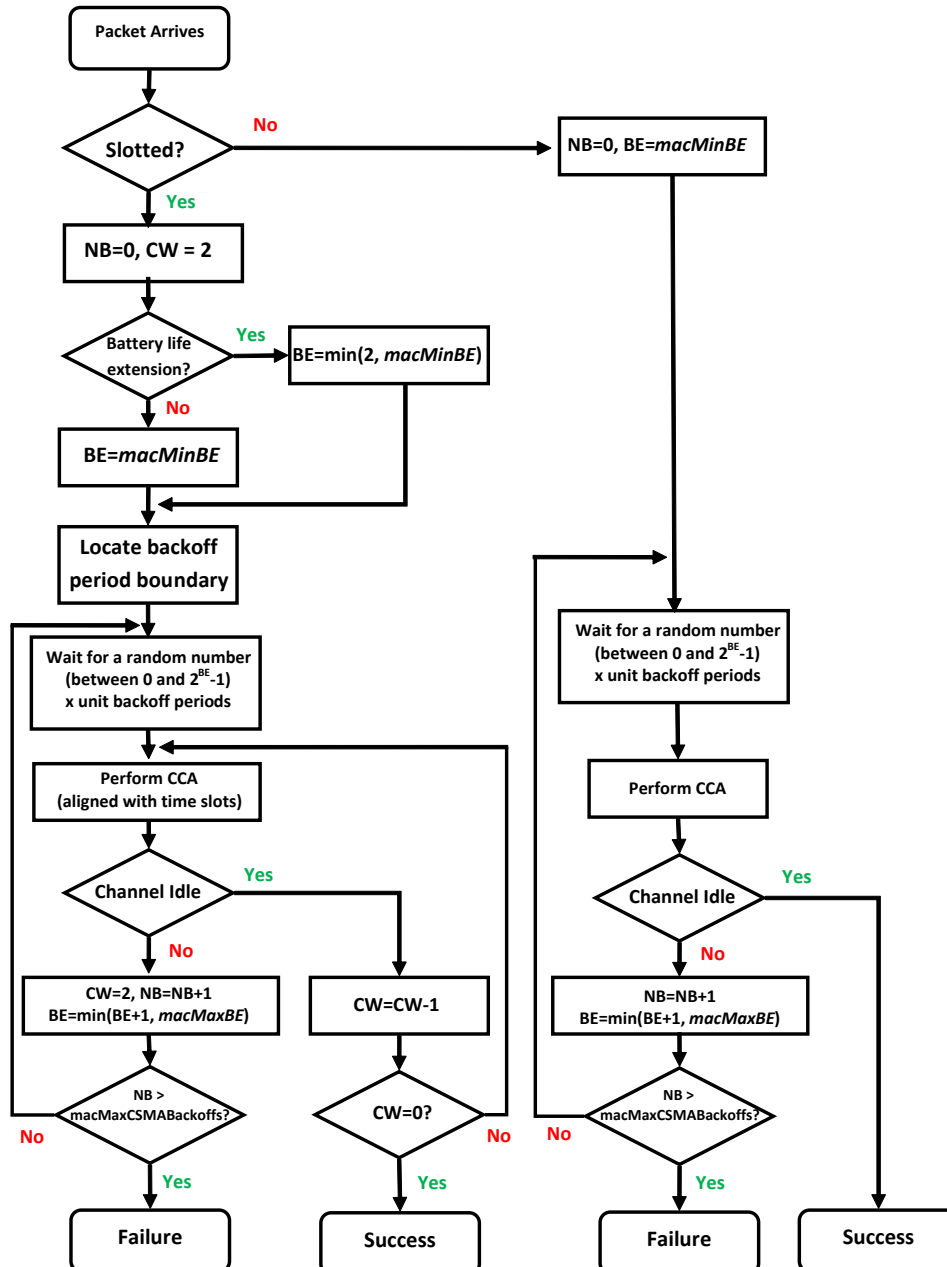


Figure 4.25: Slotted and unslotted CSMA-CA mechanism for MAC Layer.

Two types of CSMA-CA can be used:

- **Slotted CSMA-CA:** The slotted CSMA-CA mechanism is defined as a CSMA-CA mechanism that uses a superframe structure for the frames exchanged between the devices. The

superframe divides the active period into 16 equal and contiguous time slots and the backoff period has to be aligned to specific time slots;

- **Unslotted CSMA-CA:** The unslotted CSMA-CA mechanism is defined as a CSMA-CA mechanism where there is no superframe structure evolved during the exchanges between the devices and therefore there is no need for backoff slot alignment [Far08, GCB03].

The flowchart presented in Figure 4.25 describes the slotted and unslotted CSMA-CA algorithm which is initiated when a packet is ready to be transmitted.

The CSMA-CA mechanism [IEE07, Far08, GCB03] keeps three global variables updated:

- **Backoff Exponent (BE):** It is a variable that determines the allowed range for the random period the CSMA-CA algorithm will wait every time the algorithm faces a busy channel. The initial value of BE is equal to *macMinBE* in an unslotted CSMA-CA channel access. When considering a slotted CSMA-CA, the choice of the Battery Life Extension (BLE) option affects the value of BE. Therefore if the BLE option is enable, the coordinator turns off its receiver after a period equal to *macBattLifeExtPeriods* and transmits a beacon frame right after in order to conserve energy. The range for the backoff period is limited to be the minimum value of 2 or the value of *macMinBE* ($BE = \min(2, macMinBE)$). If the BLE option is disabled, the coordinator is active during the CAP and the value of BE is equal to *macMinBE* and every time the CCA is performed and the channel is busy it is incremented by one unit, while not exceeding the variable *macMaxBE*;
- **Number of Backoffs (NB):** It is a counter that keeps updated the number of times the device backs off and retries to access the channel by means of the CSMA-CA mechanism. This counter at the beginning is equal to zero and each time the device backoff due to the detection of a busy channel, BE is incremented by one unit. When the NB reaches the *macMaxCSMABackoffs* value and still did not got access to the channel then quits the CSMA-CA mechanism and reports failure to access the channel to the NWK layer;
- **Contention Window (CW):** It is used to define the number of backoff periods that the channel must be available before starting to transmit. The CW is only used in the slotted CSMA-CA mechanism. Each backoff period channel sensing, is performed during the 8 first symbols of the BP.

The random backoff time, rdm_{nb} , given by Equation 4.6, results from the random choice of any integer number between 0 to $(2^{BE}-1)$ multiplied by the unit back-off period.

$$Backoff = rdm_{nb} \cdot aUnitBackoffPeriod \quad (4.6)$$

The detailed description of the slotted and unslotted CSMA-CA algorithm is presented in the Appendix G.

4.7 Taxonomy for Medium Access Control

When using battery-powered nodes in WSNs, energy efficiency is of primary importance since it is directly related to the lifetime of the network. Major sources of energy waste are idle listening, packet retransmissions (due to packets collisions), unnecessary high transmission powers,

overhearing and control overhead [BDWL10, YHE04]. From all the electronic components of a sensor node, the radio transceiver is the most power consuming component. At the link layer, where the MAC protocol manages the use of the radio transceiver, higher efficiency can be achieved, depending on what performance metrics the MAC protocol intends to improve. MAC protocols from typical ad-hoc wireless networks differ and share some points from the MAC protocols for WSNs. WSNs share some of the objectives of the ad-hoc wireless networks, e.g., error prone channels and limited bandwidth. In WSNs, the MAC protocols must have a built-in power conservation mechanism, mobility module to handle the issues that may arise from the movement of the nodes, and mechanisms that allow the node to recover from failures (e.g., packets transmissions failures, out-of-range, ...). All these mechanisms are deeply related with energy-efficiency and network lifetime, which are performance metrics of paramount importance in a WSN. Moreover, important metrics include latency, accuracy, scalability and throughput.

In WSNs research, medium access control protocols, has been a hot topic in wireless networks during the last seven years. Many MAC protocols (with different purposes) have been proposed for WSNs in the literature. From the entire range of WSN MAC protocols, one common feature is the energy efficiency, since the hardware is battery-powered in the majority of the applications. Furthermore, WSN MAC protocols present more constraints that should be taken into account, e.g., duty cycle mechanisms, necessity of multi-hop operations to forward packets, collision avoidance mechanisms, overhearing, idle listening, overhead, limited memory and processing capabilities.

When a new MAC protocol is proposed to solve one of the sources of energy wastage mentioned in the beginning, it is very hard to accomplish the proposed objective. If the source of energy wastage is solved, for sure there is other one that is increased. Therefore, instead of solving the chosen source of energy wastage, we should try to mitigate at maximum that source of energy waste, while achieving a high energy performance and efficient trade-offs between the considered performance metrics of the respective MAC protocol.

The authors from [YBO09] performed a study on existing WSN MAC protocols where they first outline and discuss the specific requirements and design trade-offs of a WSN MAC protocol, while describing the properties of WSNs that affect the design of MAC layer protocols. Then, a typical collection of WSN MAC protocols presented in the literature are surveyed, classified and described.

Authors from [BDWL10] presented a state-of-the-art study in which they thoroughly expose the prime focus of WSN MAC protocols, design guidelines that lead to these protocols, as well as disadvantages and liabilities of the solutions. Moreover, in contrast to previous surveys from the literature that classify MAC protocols by the technique being used, this taxonomy is based on the problems being dealt with.

As we have seen before, this research can be categorized into many different ways. For the purpose of this thesis, the classification of the MAC protocols into different categories is performed by the technique to access the channel being used in the protocol, but also taking into account that one MAC protocol may utilize multiple techniques. However, due to the growing number of WSN MAC protocols, many of those apply more than one technique in the MAC layer. Hence, this taxonomy for the classification of MAC protocols extends the classification of WSN MAC protocols for the new ones, which employ multiple techniques to achieve the purposed objective. Moreover, a comparison table is presented for the considered MAC protocols, where the MAC characteristics (e.g., slot assignment, frequencies allocation) are categorized for each one of the MAC protocols.

As presented in Figure 4.26, three main categories of MAC protocols stand out as the most

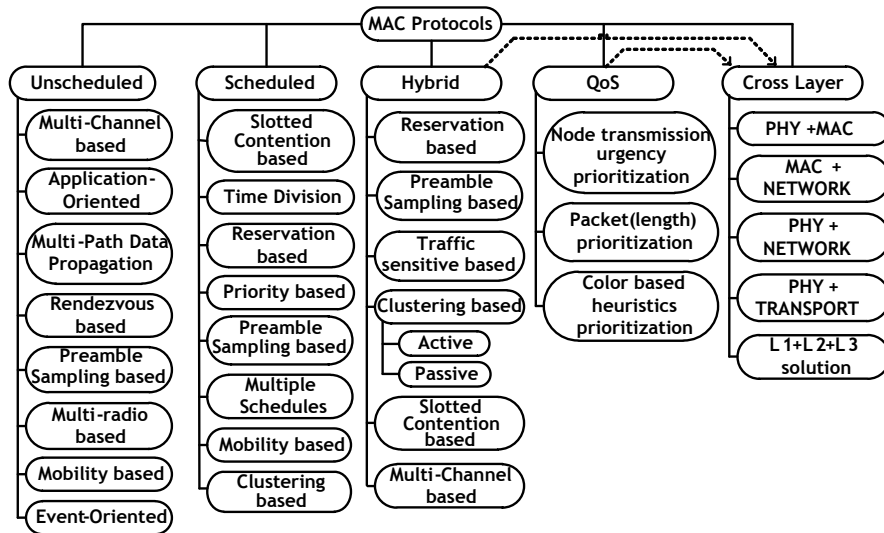


Figure 4.26: Taxonomy for WSN MAC protocols.

prominent ones: Unscheduled, Scheduled and Hybrid MAC protocols. The former category addresses the MAC protocols that allows for sensor nodes to operate independently, while it conserves energy due to the low complexity of the MAC protocol. The second category is related to the MAC protocols that organize the communication between sensor nodes in an ordered way, while reducing collisions and retransmissions by using synchronization mechanisms. The latter ones use different techniques to conserve energy among nodes, namely by adjusting their behaviour between techniques used in scheduled and unscheduled MAC protocols.

Besides these three main categories, there is the QoS and Cross-layer categories. The QoS category includes the WSN MAC protocols that employ quality of service policies in the communication between sensor nodes, while maintaining the energy efficiency. The last category is dedicated to MAC protocols that do not follow the traditional layered protocol architecture. In contrast with traditional MAC protocols, these ones achieve higher performance metrics due to the joint optimization and design of networking layers (i.e., cross-layer design).

Unscheduled Protocols

As presented in Figure 4.27, the Unscheduled protocols can further be divided into roughly eight categories: Multi-Channel, Application-oriented, Multi-path Data propagation, Rendezvous based, Preamble Sampling based, Multi-radio based, Mobility based and Event-oriented. The Multi-channel sub-category accounts for the MAC protocols whose main characteristic is the use of multiple radio channels by the sensor nodes, allowing for the node to simultaneously communicate on separate channels. For the Application-oriented sub-category, the application characteristics may be considered to enable the MAC protocol to conserve energy. The Multi-path Data propagation sub-category is dedicated to the MAC protocols where information is broadcasted to more than one node in each single-hop without, however, flooding the network. The receiving nodes continue to broadcast until the message reaches its final destination.

Rendezvous based MAC protocols utilize a method called rendezvous, which allows for nodes to communicate if both of them are powered simultaneously. The study of Preamble sampling-based MAC protocols accounts for the protocols that do not use common active/sleep schedules. Instead, each node chooses its active schedule independently of the other nearby nodes. The Multi-radio based MAC protocols utilize more than one radio transceiver in the communications between the sensor nodes. One is used to communicate the data between nodes

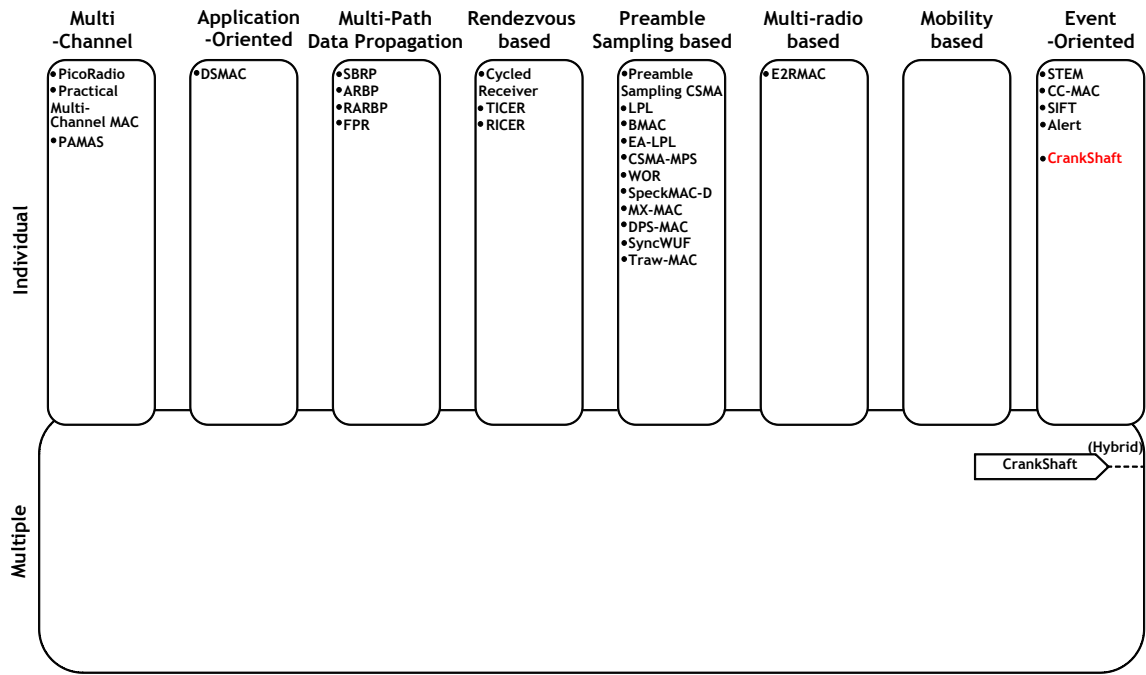


Figure 4.27: Taxonomy for the Unscheduled MAC protocols and different sub-categories.

while other one is used to wake-up the nodes. The Mobility-based sub-category accounts for the MAC protocols that have a mobility feature embedded in the sensor node architecture. The Event-oriented regards the MAC protocols that are triggered by an event that is sensed by the sensor nodes.

Scheduled Protocols

In Figure 4.28 Scheduled protocols are additionally divided into eight categories: Slotted contention based, Time division based, Reservation based, Priority based, Preamble sampling based, Multiple schedules, Mobility based and Clustering based. Some of these sub-categories have already been previously described. Therefore, only the new ones are going to be further described.

The Slotted contention based sub-category is the one that includes the majority of the MAC protocols. Slotted protocols divide time into frames. Each frame is subdivided into a certain number of slots.

The Time division based MAC protocols divide the channel access time into repeated frames. Each frame is subdivided into N_n time slots, which allocates one slot to only one node. The Reservation based MAC protocols employ a reservation request scheme based on Time Division Multiple Access (TDMA) techniques. The Priority based sub-category aggregates the MAC protocols that utilize a TDMA scheme jointly with a priority based scheme, to decide when packets are transmitted. The study of Preamble sampling-based MAC protocols accounts for the protocols that do not use common active/sleep schedules.

The Multiple schedules sub-category includes the MAC protocols that enables the nodes to have multiple schedules. However, it employs different schemes that allows for the nodes to communicate between them. The Mobility-based sub-category accounts for the MAC protocols that have a mobility feature embedded in the sensor node architecture. The Clustering based sub-category accounts for the MAC protocols that employ an adaptive clustering hierarchy scheme

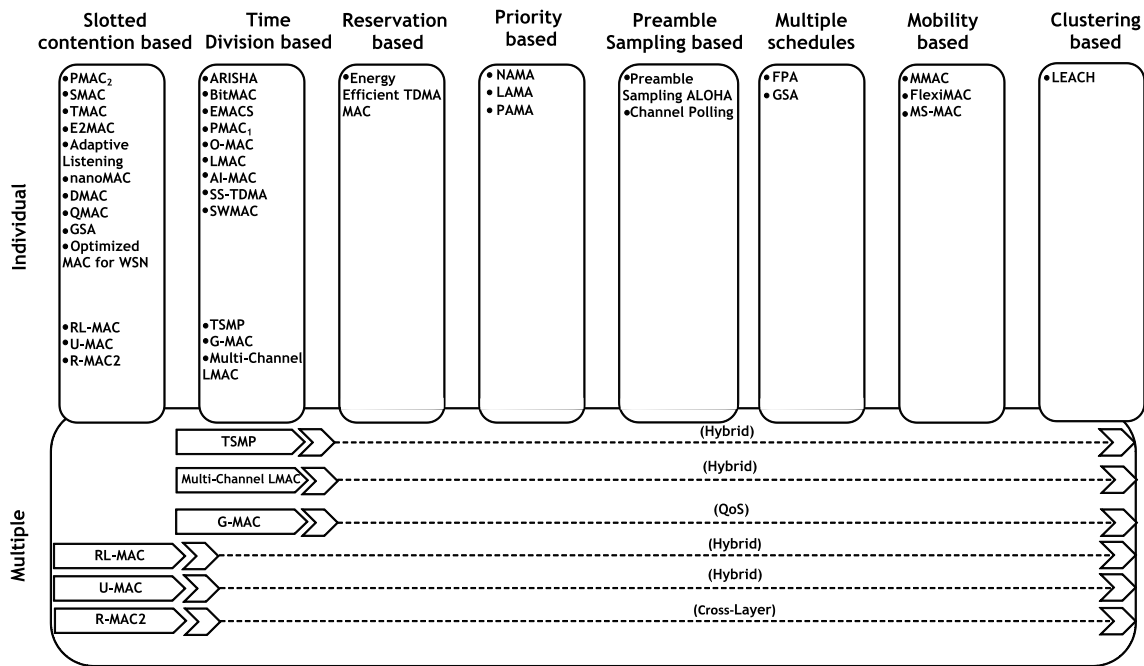


Figure 4.28: Taxonomy for the Scheduled MAC protocols and different sub-categories.

that allows for the nodes to send data to the cluster heads, based on a TDMA approach.

Hybrid Protocols

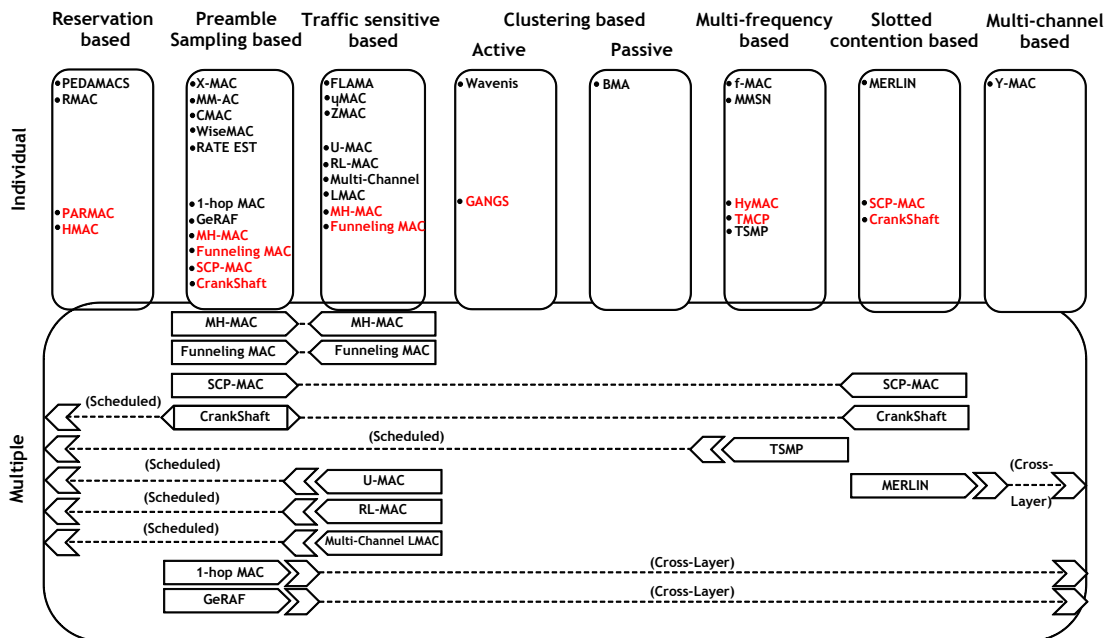


Figure 4.29: Taxonomy for the Hybrid MAC protocols and different sub-categories.

The Hybrid category results from the combination of different characteristics from the Scheduled and Unscheduled categories, as presented in Figure 4.29. It can be further sub-divided into seven categories: Reservation based, Preamble sampling based, Traffic sensitive based, Clustering based (active and passive), Multi-frequency based, Slotted contention based and Multi-channel based. The Reservation based and Preamble sampling based have been described

above. The Traffic sensitive based sub-category corresponds to the MAC protocols that shape their behaviour accordingly with the traffic patterns that the sensor node detects. The Clustering based protocols can be either active, if the protocol utilizes control packets to collect topological information, or passive if no control packets are used to gather this information. The Multi-frequency based MAC protocols correspond to the ones that choose different frequencies which allows for the sensor node to communicate control and data packets in separate frequency bands.

QoS Protocols

The QoS category, presented in Figure 4.30, can be sub-divided into three categories: the Node transmission urgency prioritization, packet (length) prioritization and colour based heuristics prioritization. All the QoS sub-categories account for quality of service policies that may be interpreted as prioritization based schemes.

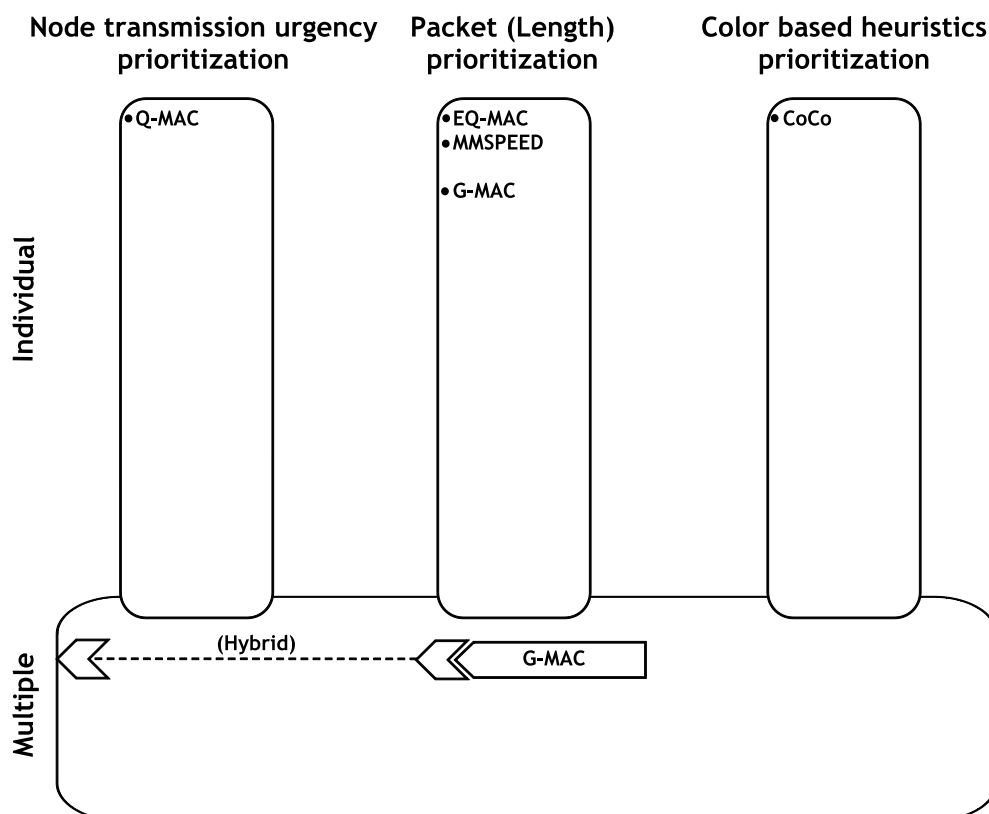


Figure 4.30: Taxonomy for the QoS MAC protocols and different sub-categories.

Cross-layer Protocols

Figure 4.31 presents the cross layer category, which can be divided into five categories: PHY+MAC, MAC+NETWORK, PHY+NETWORK, PHY+TRANSPORT and L1+L2+L3 solutions. Each one of the first four aforementioned sub-categories handles the combination between two layers, while the last one suggests a solution based on the Physical (L1), Link (L2) and Routing (L3) layers. These solutions are becoming the most promising alternative to inefficient traditional layered protocols. In these solutions there is a joint optimization and design of networking layers (i.e., cross-layer schemes).

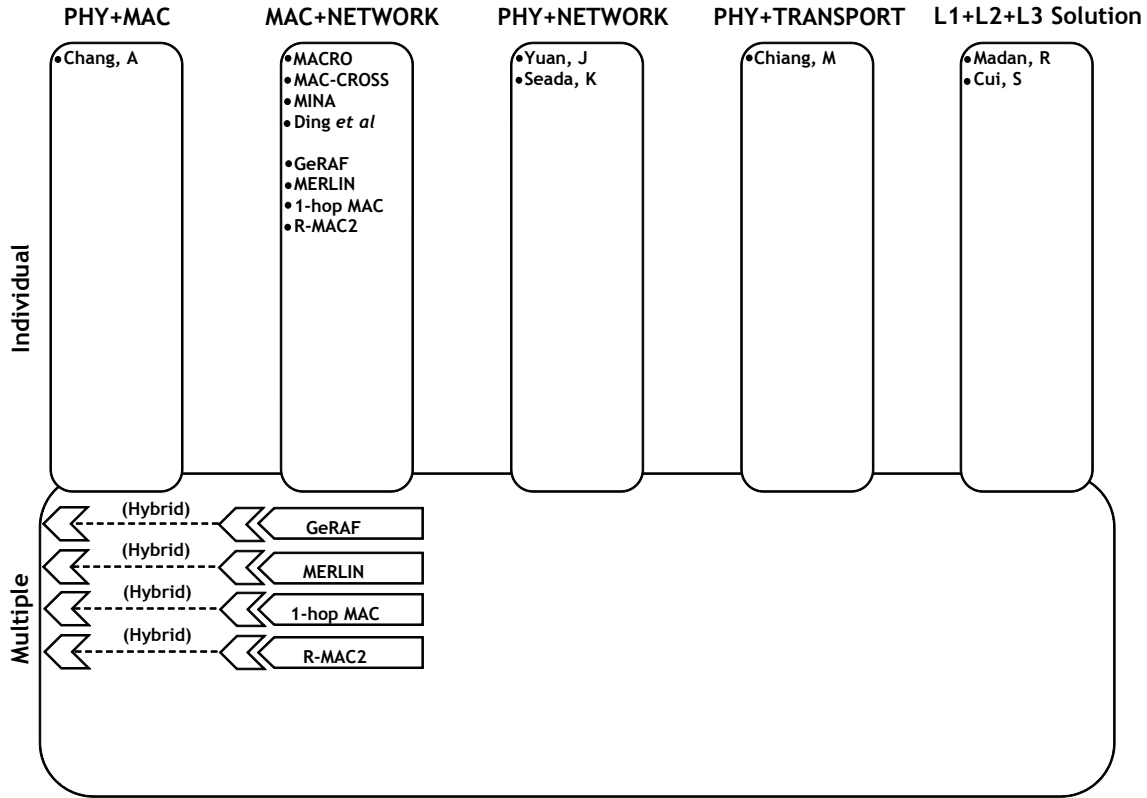


Figure 4.31: Taxonomy for the Cross-layer MAC protocol for different sub-categories.

Extended Taxonomy

Figure 4.32 presents an extended taxonomy of the WSN MAC protocols, from [YBO09], where the protocols are categorized, according to their medium access and control technique and distinguishes the MAC protocols that use more than one medium access technique. The MAC protocols that employ only one medium access technique are represented in the individual zone. The ones that utilize more than one medium access technique are represented in the multiple zone of Figure 4.32, where the overlapping regions of two different sub-categories allows for understanding the techniques that are shared between categories and sub-categories, for a specific MAC protocol. By observing Figure 4.32, it is easy to notice that there are only a few QoS and Cross-layer MAC protocols. In contrast to this small number of MAC protocols, the scheduled and unscheduled categories are the ones that present more MAC protocols. Nevertheless, the Hybrid protocols category also presents a notable number of MAC protocols. Considering the multiple zone of Figure 4.32, the majority of the MAC protocols are shared between the Scheduled, Hybrid and Cross-layer categories. This means that the most recent proposed MAC protocols combine different techniques and methods from different categories in order to accomplish a better energy performance, while maintaining acceptable values for the throughput and latency.

Apart from the taxonomy of WSN MAC protocols presented in Figure 4.32, which provides an idea of the vast number of MAC protocols available nowadays, a few MAC protocols stand out as being the boosters for the field of WSN research. From all the presented MAC protocols there are some ones that have been more referenced and led to the appearing of incremental or derivative MAC protocols all over the last years. These protocols are the following ones: ALOHA [EH02], S-MAC [YHE04], T-MAC [DL03], X-MAC [BYAH06], IEEE 802.15.4 [IEE07], LEACH [HHT02], WiseMAC [EHD04], CSMA/CA [TK85], LPL [PHC04] and SIFT [TJB04].

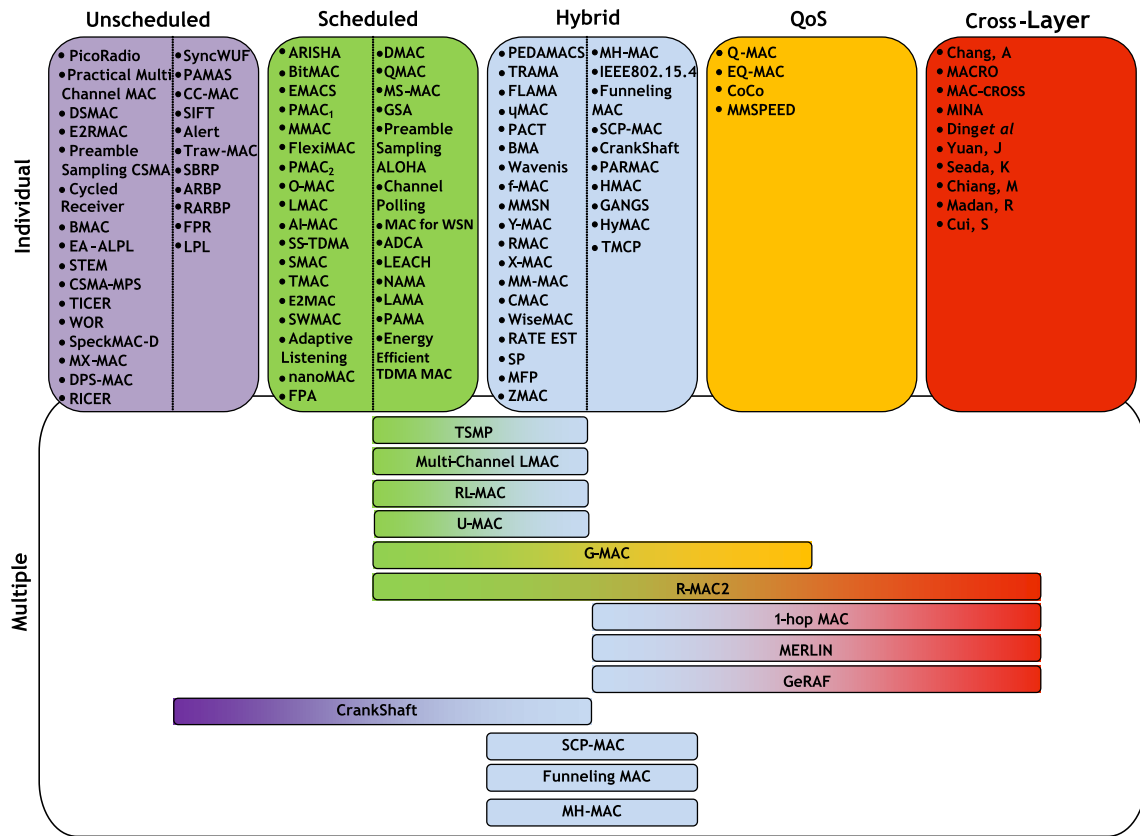


Figure 4.32: MAC protocols distribution among different categories.

In this thesis, some of the aforementioned MAC protocols, are mentioned and referenced as related work. However, there is one MAC protocol that the author of this thesis considers as noteworthy and needs further attention: the SCP-MAC protocol. Since the SCP-MAC protocol employs some of the most effective techniques to access the medium, special attention must be given to it, in order to better exploit upgrades that may be added, to achieve higher energy performance. The following sections present some of the most important MAC protocols. The remaining MAC protocols used to build up the taxonomy for the MAC protocols are presented in Appendix G.

4.7.1 Survey on Unscheduled MAC protocols

Berkeley MAC

Berkeley MAC (BMAC) [PHC04] protocol employs several techniques, namely CCA and packets backoff for channel arbitration, and Low Power Listening (LPL) for low power communication. Nodes follow a sleeping schedule independently, by following a duty cycle of the sensor network. BMAC utilizes long beacons/preambles when a message transmission is needed, as presented in Figure 4.33. The CCA technique is one the innovations which evaluates the received signal and the noise floor in particular way. It starts by searching for outliers in the received signal such that the channel energy is significantly below the noise floor. If the node detects an outlier during the sampling, the channel is declared as “clear”, because a valid signal will never have outliers significantly below the noise floor. After the nodes sample five times the channel without finding an outlier, then the node declares the channel as busy. The sender node transmits a beacon with a length enough to cover the time when the receiver node wakes up and senses activity. If the node detects activity it remains awake in order to receive the

packet that is sent after the beacon or return to sleep if no activity is detected. BMAC allows for controlling several parameters in the protocol. However, the long preambles can lead to higher latencies.

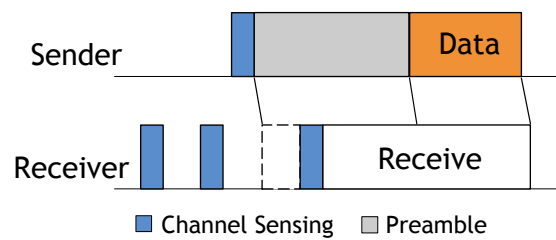


Figure 4.33: BMAC packet exchange.

SIFT

SIFT [TJB04] is designed for low latency. Like previously presented protocols, SIFT uses a contention window with a fixed size. The novelty is that, instead of picking a slot randomly and uniformly, nodes use a skewed distribution which gives preference to the slots at the end of the contention window. It is therefore more likely that only one node will have chosen the lowest order slot; SIFT eventually uses that node to transmit data. When the number of contending nodes is low, if no node starts to transmit in the lowest order slot of the Contention Window (CW), each node increases its transmission probability exponentially for the next slot. However, SIFT does not solve the hidden terminal problem and may use a CSMA/CA mechanism.

4.7.2 Survey on Scheduled MAC protocols

Sensor-MAC

The Sensor-MAC (S-MAC) [YHE04] is based on periodic sleep-listen schedules and local synchronizations between nodes. Schedule exchanges are accomplished by periodical SYNC packet broadcasts to the direct neighbours, as presented in Figure 4.34. Collision avoidance is achieved by carrier sense. RTS/CTS packets exchanges can be used for unicast type data packets. A new concept employed in S-MAC is the message fragmentation where long messages are divided into frames and sent in a burst. Periodic sleep may lead to high latency when considering multi-hop routing algorithms. Adaptive listening technique is proposed to improve the sleep delay and consequently the overall latency.

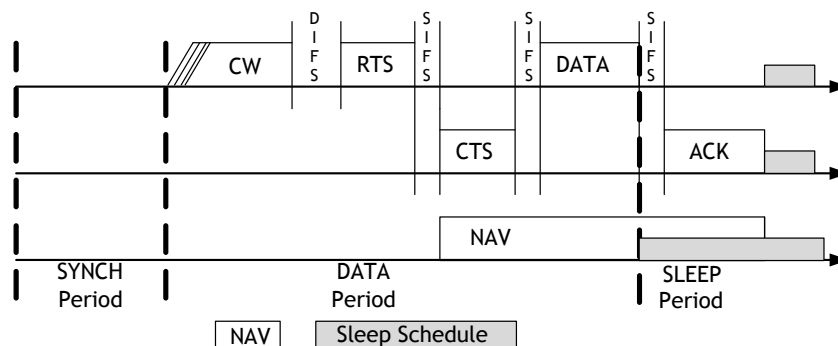


Figure 4.34: S-MAC frame format.

By employing sleeping schedules the idle listening time is reduced and consequently reduces the energy consumption. However, the adaptive listening improves the sleeping delay but causes overhearing or idle listening increase if the packet is not destined to the listening node.

Preamble sampling

Preamble sampling protocols [EH02] do not use common active/sleep schedules. The node spends more time in the sleep mode and it wakes-up only for a short duration, to check if there is an on-going transmission, as depicted in Figure 4.35. To avoid deafness, each data frame is anticipated by a long enough preamble, to make sure that all potential receivers will detect the preamble and wait for the data message that will be sent. The node turns on its radio to sample the channel, according to its duty-cycle periodically. If the node senses an idle channel, it goes back to sleep immediately. However, if a busy channel is detected, the node waits for the data message. After the reception of the data packet, the node goes to sleep mode.

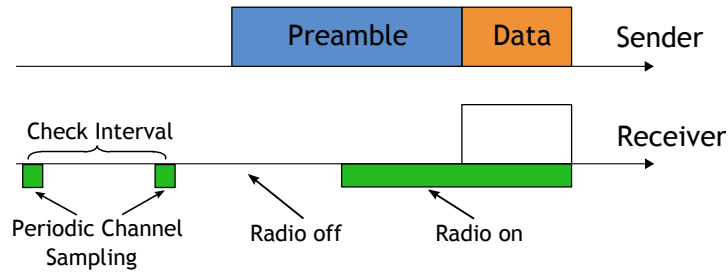


Figure 4.35: Preamble sampling mechanism.

4.7.3 Survey on Hybrid MAC protocols

IEEE 802.15.4 MAC

The IEEE 802.15.4 standard specifies the physical and MAC layer for low-rate wireless personal area networks (LR-WPANs). The MAC proposed by the IEEE 802.15.4 standard supports two types of network nodes. On the one hand, the Full-Function Device (FFD), can serve as the coordinator of the PAN and is able to form any type of topology. On the other hand the Reduced Function Device (RFD) can only form star topologies and they can only communicate with FFDs. These last ones can never act as coordinators. The IEEE 802.15.4 standard only allows for the networks to be built as either peer-to-peer or star networks. In every network, it needs at least one FFD to work as a coordinator of the network. In the peer-to-peer topology the multi-hop feature is not supported, but it can be added. Also cluster trees can be formed and can be extended as a generic mesh network, whose nodes are cluster tree networks, with a local coordinator in each cluster, in addition to the global coordinator. In the star topology, the coordinator is the central node. Since the IEEE 802.15.4 standard intends to offer a low-cost and low-speed ubiquitous communications between devices, the proposed MAC protocol must be flexible enough to guarantee the devices requirements. To achieve these objectives the MAC allows for two basic communication modes: 1) beacon-enabled; and 2) non-beacon modes. The latter one is simply the CSMA/CA MAC, and is very useful when the main purpose of the WSN is a simple sensing. The former one is more complex, since it involves the beacon transmission, whilst maintaining a slot structure. This one is similar to the scheduled-based MAC protocols. As the majority of the IEEE 802.15.4 features are used in the beacon-enabled mode, it will be briefly discussed below. As presented in Figure 4.36, the beacon-enabled mode employs a superframe structure, where the MAC frame is divided into two periods: the active and the inactive periods. Before each active period a beacon frame is transmitted by the coordinator at an interval BI , adjustable from 15 ms to 245 s. The length of the active period is determined by SD , while the duty cycle is calculated by $2^{SD}/2^{BI}$. The active period is further divided into

16 time slots of duration BP. The active period is composed by the beacon, a CAP and a CFP. The latter one is only available if GTs are allocated by the coordinator, but only 7 GTs are allowed in the CFP. First a node listens to the beacon to understand if a GTS has been reserved by the

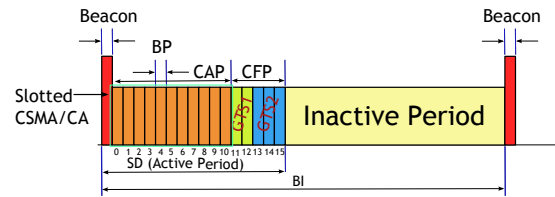


Figure 4.36: IEEE 802.15.4 beacon-enabled superframe structure.

coordinator or not. If so, then it remains powered of until its GTS is scheduled to initiate the transmission of data. If no GTS is reserved, then it uses the CSMA/CA during CAP, where typical back-off procedures are applied.

Scheduled Channel Polling-MAC

The Scheduled Channel Polling-MAC (SCP-MAC) protocol [YSH06] is an example of a duty-cycle based MAC protocol that specifies awake and asleep time periods within a frame. This duty-cycle based MAC protocol tries to reduce the energy consumption by introducing periodic listen and sleep cycles, while performing contention during the listening period. The SCP-MAC combines scheduling with channel polling in an optimal way, like in the LPL [PHC04] protocol. The SCP-MAC main contribution is the use of a double contention window. The SCP-MAC tries to eliminate the majority of the sources of energy waste: collisions, overhearing, control overhead and mainly, idle listening. It tries to solve packet collisions by using the two phase contention window scheme (when the sender node wants to transmit a data packet).

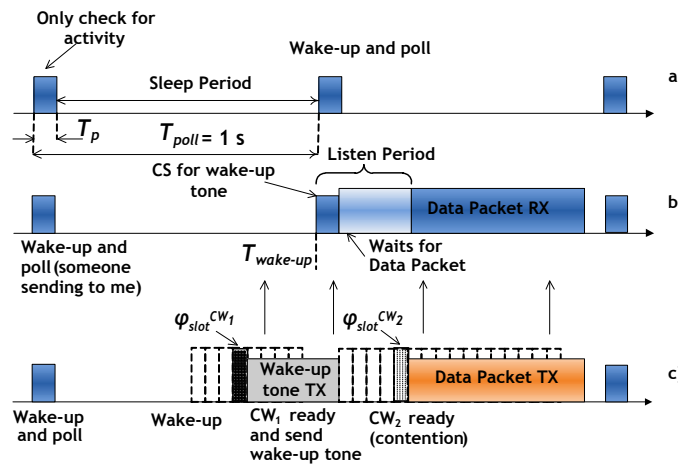


Figure 4.37: SCP-MAC two-phase contention window mechanism.

As depicted in Figure 4.37, if a node that wants to send a packet, it will choose a random slot within the first contention window (following a uniform distribution). The potential node that wants to send a packet switches on its radio, and checks the channel. If it senses the channel free it sends a preamble, which acts like a busy tone, and continues to send it until the end of the first contention window, announcing to other potential senders that a transmission is ongoing. After it sends the preamble, all nodes except the one that “won” the channel, will wake-up and poll the channel to sense the medium for a preamble. If the node detects a preamble it will stay awake to receive the packet. If no preamble is detected the node goes immediately to the sleep mode. The node that has gained the control of the channel will

perform another random slot choice into the second contention window and sense the medium. If it is free then the packet will be sent.

One of the applied techniques is the channel polling synchronization of the neighbouring nodes, using SYNC packets and optimal intervals for scheduling synchronization. This process of sending SYNC packets is repeated after a synchronization period, T_{sync} , but may be suppressed by piggybacking the schedules in the data packets when the packets exchanged are of the broadcast type.

Two contention windows are used because the collision probability is lower than the one obtained by using a single contention window whose size is the sum of the sizes from CW_1^{max} and CW_2^{max} . The two-phase contention window reduces the effective collision probability compared to a single contention window of equal duration, since only nodes that succeed in CW_1 will enter into the CW_2 . After the first phase of the contention, only the successful nodes from CW_2 contend in the CW_2 . With fewer contending nodes, the effective collision probability is greatly reduced. With periodic traffic, the energy cost can be minimized by using a scheduled listening algorithm, and the synchronization of the neighbour's channel polling time is maintained like in Sensor-MAC (S-MAC) [YHE04], while adjusting the duty cycle to variable traffic conditions. When the data rates are lower than synchronization periods, explicit SYNC packets are used. An adaptive channel polling mechanism can be used when it detects bursty traffic. This mechanism adds additional wake-ups in the interval between two regular wake-ups. However, this optional mechanism may increase idle listening in case the information transmitted can fit in a single packet, due to a node that receives a packet during its normal channel polling that systematically wakes-up in the subsequent adaptive slots.

Crankshaft

The main characteristic of Crankshaft [HL07] is the time being decomposed into frames, which are composed by slots. Some slots in the beginning of the frame are assigned for unicast traffic, while in the end of the frame some slots are assigned to broadcast traffic. The way how the slots are of type receiver-based, where each node has its own slot during which it wakes-up to receive data. When considering broadcast slots, all nodes wake-up. Crankshaft employs a collision avoidance mechanism that is employed prior to the transmission and each transmission is ended with an acknowledgement packet. This collision avoidance mechanism is similar to the one used in SCP-MAC protocol, where a sender transmits at randomly chosen times a preamble. The sender node that starts before the others to transmit wins the contention, because a carrier sense is performed before transmitting any packet to sense for the presence of a signal in the shared medium. If the channel is sensed as busy the contention is stopped. The slot's choice used to perform the carrier sense, gives preference to the higher order time slots (uses a skewed distribution). This leads to a reduction of the length of the preamble and therefore it reduces the energy consumption. Although Crankshaft reduces idle listening, some overhead is added when sampling all the broadcast slots, leading to an increase of the energy waste. Moreover, the use of a TDMA approach it decreases the flexibility of the protocol in the presence of sporadic traffic.

4.7.4 Survey on QoS MAC protocols

EQ-MAC

EQ-MAC [YBO08] is another MAC protocol with quality of service policies. It intends to reduce energy consumption, while providing QoS guarantees by using a service differentiation mechanism. EQ-MAC consists of two sub-protocols: the Classifier MAC (C-MAC), and the Channel

Access MAC (CA-MAC). The first one is responsible by the classification of the data collected among the sensor nodes based on the importance of the data, while storing it in the appropriate queue of the node's queuing system. The second one is a hybrid collision avoidance system of both scheduled and unscheduled schemes that allows for the node to save energy, and thus extending the network's lifetime. The energy savings comes from the different procedures that are applied, depending if the the exchanged messages are long or small. Long messages are assigned to scheduled slots with no contention, where time slots are only assigned to nodes that have data to send (leading to an energy reduction when using TDMA slots), while for small messages (periodic control messages) are assigned random access slots.

4.7.5 Survey on Cross-Layer MAC protocols

MERLIN

MERLIN [ROJ08] integrates MAC and routing features into a single architecture. Compared with other sensor network protocols, it employs a multicast upstream and multicast downstream approach that allows relaying packets to and from the gateway. Simultaneous reception and transmission errors are notified by using asynchronous burst ACK and negative burst ACK. The network is divided into time zones, together with an appropriate scheduling policy, enables the routing of packets to the closest gateway. MERLIN employs a TDMA/CSMA based approach, in which it divides the time into slots. A scheduling table allows allocating timeslots to the nodes in the network to assign periods of node activity and inactivity. The scheduling allows synchronizing neighbouring nodes for transmission and reception in the same time zones. All wireless nodes must be well synchronized between themselves and with the gateways. As a drawback, MERLIN suffers from the hidden terminal problem and collisions occur often in the network. Moreover, it needs more than one base station in the network in order to manage the input of user data into the network and presents high delays. In Figure 4.38 is presented the mechanism employed in MERLIN to avoid collisions when nodes try to access the medium to transmit data packets.

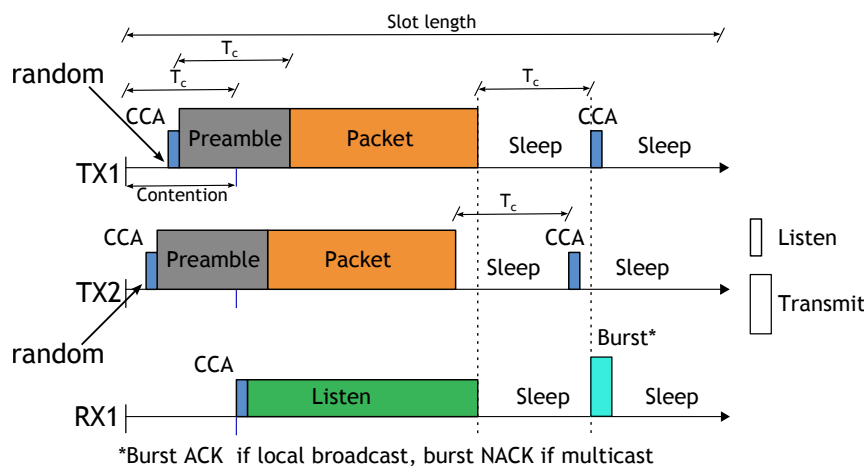


Figure 4.38: Transmission mechanism for collision avoidance of MERLIN.

4.7.6 Survey on Multiple based MAC protocols

1-hop MAC

1-hop MAC [WBD⁺06] protocol is based on communication architecture grouping MAC and routing layers which avoids 1-hop neighbourhood knowledge. It combines L2 (link) and L3 (network/routing) protocols. The basic procedure of 1-hop MAC protocol initiates with a node that sends out a request message and is received by its 1-hop neighbourhood. Each neighbour will answer this request after a time proportional to its metric. The requesting node can then elect the most suitable node based on when it has received the answers. Three 1-hop protocol variants are proposed, apart from the basic one. The first one tries to reduce the sender node listening period, the second one tries to avoid multiple ACK messages while the last one allows for sending data packets during the “do not answer anymore” message period of the protocol. It can dynamically swap between the 1-hop variant 1 and 1-hop variant 3, by following specific rules that allows for achieving energy efficiency. By using this approach, it can be viewed as a multi-mode protocol where the decision on which mode to use is distributed and no signalling messages are necessary.

4.8 Classification of MAC Protocols Characteristics

This section is dedicated to the description of some of the most prominent MAC characteristics that have been identified. These characteristics are related with several features that characterize a MAC protocol and allows for a user to distinguish between the MAC protocols. The tables for the MAC protocols taxonomy are presented in detail in Appendix G. The characteristics of the MAC protocols are as follows.

1. **Action against energy waste:** This characteristic is related to the main purpose of the MAC protocol or on what sources of energy waste it tries to mitigate. Possible values are the following:
 - Reducing collisions (Co);
 - Reducing Overhead (Ov);
 - Reducing Overhearing (Oh);
 - Reducing Idle Listening (Il);
 - Narrow Band Interference (Nal).
2. **Type of scheduling:** This feature concerns the type of scheduling protocol that the MAC protocol employs. Possible values are the following:
 - Global Schedule (Glob);
 - Centralized Scheduling (Cent);
 - Distributed Scheduling (Dist);
 - Localized Collision free based (Local);
 - Staggered based (Stag).

3. **Roles for the nodes:** This characteristic helps to identify if the sensor nodes have always the same functionality along the WSN. Possible values are the following:

- Rotative (Rt);
- Fixed (Fi);
- Adaptive (Adapt);
- Static (St).

4. **Node traffic change behaviour:** It establishes if the MAC protocol adapts to the traffic patterns variation. Possible values are the following:

- Adaptive (Adapt);
- Fixed (Fi).

5. **Node traffic exchange:** This characteristic defines if the traffic is variable or uniform. Possible values are the following:

- Uniform (Uni);
- Variable (Var).

6. **Slot assignment:** If the MAC protocol is slot-based type, this feature defines how the slot assignment is performed. Possible values are the following:

- Receiver-based (Rc);
- Neighbour-based (Nghb);
- On-demand based (On).

7. **Frequency allocation:** It defines if the MAC protocol utilizes one or more frequency bands.

- Single-frequency (Single);
- Multi-frequency (Multi);

8. **Frame subinterval time reduction:** It identifies what part(s) of the MAC frame protocol is reduced. Possible values are the following:

- Active Period (Act);
- Synchronization Period (Synch);
- Sleep Delay (Sleep);
- Schedules Period (Sched);
- Sampling Duration (Samp).

9. **Duty cycle tuning:** This feature is related to the way how the duty cycle is adjusted in MAC protocol. Possible values are the following:

- Statistical Function (Stat);
 - Utilization Function (Util);
 - Pre-defined sets of duty cycles (Pre);
 - Mobility adjust (Mob);
 - Range (Rang);
 - Application Demand (App);
 - Traffic Load (Tf).
10. **Preamble length reduction:** It defines the technique employed by the MAC protocol (if present) to reduce the preamble length. Possible values are the following:
- Packetization (Pack);
 - Piggybacking Synchronization Information (Pigg);
 - Data frame preamble (DpR);
 - Dynamic size (Dis).
11. **Channel allocation:** It defines how the channel allocation is performed in the MAC protocol. Possible values are the following:
- Single-Channel (Single);
 - Dual-Channel (Dual);
 - Multi-Channel (Multi).
12. **Preamble reception filtering:** It defines a special feature that may be employed by the MAC protocol in the preamble reception when Preamble Reception Filtering is present. The only possible value is the following:
- Micro-Frame (Micro).
13. **Communication modes:** This characteristic defines if the MAC protocol employs or not beacon packets. Possible values are the following:
- Beacon mode (Be);
 - Non-Beacon mode (n-Be).
14. **Multiplex (channel access) technique:** It defines the method by which multiple analog message signals or digital data streams share the medium and are possibly combined into one signal over the shared medium. Possible values are the following:
- CSMA;
 - TDMA;

- CDMA;
- FDMA.

15. **Wake-up techniques:** It defines what type of technique is employed in the MAC protocol that needs to be awakened. Possible values are the following:

- Wake-up radio (Radio);
- Wake-up tone (Tone);
- Wake-up schedule (Schd).

16. **Contention window sizes:** In contention-based MAC protocols it defines how many contention windows and if the size of the contention window is variable or not. Possible values are the following:

- Single CW & Fixed size (Sg & Fi);
- Single CW & Variable size (Sg & Var);
- Double CW & Fixed size (Db & Fi);
- Double CW & Variable size (Db & Var).

17. **Type of traffic:** This characteristic defines the type of traffic which is handled by the MAC protocol. Possible values are the following:

- Converge cast (Conv);
- Sensor (Sensor);
- Multimedia (Media).

18. **Traffic load:** This feature defines the traffic load supported by the MAC protocol. Possible values are the following:

- High Traffic (Hi);
- Medium traffic (Me);
- Low traffic (Lo).

19. **Cluster:** It defines if the MAC protocol allows for the sensor nodes to form clusters. Possible values are the following:

- Yes;
- No.

20. **Channel assignment:** This feature defines how the channel assignment is performed by the sensor nodes in multi-channel based MAC protocols. Possible values are the following:

- Receiver-based (Rc);

- Neighbour-based (Nghb);
- On-demand based (On).

21. **Synchronization:** It defines if the sensor nodes perform schedules synchronization. Possible values are the following:

- Yes;
- No.

22. **Channel technique:** It defines how the channel technique is employed by the MAC protocol to control the access to shared medium. Possible values are the following:

- Clear Channel Assessment (CCA);
- Preamble Sampling (PrS);
- Data Packet Sampling (DtS);
- Busy Tone (Busy);
- Carrier Sense (CS);
- Data Prediction (DaP);
- Framelets Division (FrD);
- Low Power Listening (LPL);
- Channel Assessment (CA);
- Schedule Channel Polling (ScP);
- Channel Detection (CD);
- Frequency hopping (FrH);
- Cross-Layer (CL);
- Node Activation based (NoB);
- Link Activation based (LiB).

4.9 Summary and Conclusions

A large amount of MAC protocols have been proposed in the literature to mitigate or try to solve several waste energy problems, whilst optimizing some performance parameters. We have classified key MAC protocols which were considered in the proposed taxonomy.

This research on MAC protocols can be categorized into many different ways. However for the purpose of this thesis, the classification of the MAC protocols into different categories is performed by the technique to access the channel being used in the protocol, along with the possibility of the MAC protocol to use multiple techniques.

Due to the large amount of work that has been produced over the past two decades on WSNs,

many of these categories apply more than one technique in the MAC layer. Hence, this taxonomy classification extends the classification of WSN MAC protocols for the new ones that employ multiple techniques to achieve the purposed objective.

Three main categories of MAC protocols stand out from the ones presented throughout this chapter: Unscheduled, Scheduled and Hybrid MAC protocols. The former category addresses the MAC protocols that allows for sensor nodes to operate independently, while it conserves energy due to the low complexity of the MAC protocol. The second category is related to the MAC protocols that organize the communication between sensor nodes in an ordered way, while reducing collisions and retransmissions by using synchronization mechanisms. The latter one considers different techniques to conserve energy among nodes, namely by adjusting their behaviour between techniques used in scheduled and unscheduled MAC protocols. Moreover, comparison tables for the considered MAC protocols are presented from Table G.3 to Table G.14 where the MAC characteristics (e.g., slot assignment, frequency bands allocation) are categorized for each one of the MAC protocols.

From this intensive analysis of the MAC techniques and protocols one of the most promising is SCP-MAC. Therefore, it is worthwhile to assume SCP-MAC as a solid basis for the future development of our own MAC protocol. These initial hypothesis are going to be further demonstrated in the following chapter by a simulation tool based on the OMNeT++ event driven simulator developed throughout the research, where different studies have been conducted to evaluate potential improvements for our new MAC protocol. There are three main reasons to choose the SCP-MAC protocol as a starting point to the development of a new MAC protocol:

- Employs two-contention windows to contend for the medium;
- Synchronized channel polling is combined with reservation mechanism;
- Low power listening protocol is considered.

Chapter 5

Scheduled Channel Polling MAC protocol

The SCP-MAC protocol is noteworthy to be analyzed in detail, to provide contributions to the design and proposal of a new MAC protocol. This chapter is divided into six sections. Section 5.1 gives the motivation to use the SCP-MAC protocol as a comparison protocol with other ones. Sections 5.2 and 5.3 describe in detail the SCP procedures, namely the two-phase contention window mechanism and the synchronization phase. In the fourth section is proposed a state transition diagram for the SCP protocol (Section 5.4). Section 5.5 describes how the implementation of the SCP in the simulation framework is carried out, in which the SCP simulator parameters and general definitions along with the description of the different SCP simulator layer modes available are presented and discussed. In Section 5.6 the chapter ends with a brief summary and considerations about this simulation implementation.

5.1 Context and Motivation

WSNs answer the need for nomadicity and mobility in the context of *in situ* event monitoring. The main purpose of this class of networks is to provide quick and easy access to the information gathered from a set of sensor nodes scattered in a geographical region.

In WSNs, energy efficiency is of primary importance since it is directly related to the lifetime of the network formed by mostly battery-powered nodes. Major sources of energy waste are idle listening, packet retransmissions (e.g., due to packet collision), unnecessary high transmission powers, overhearing and control overhead [YHE04, BDWL10]. Packet collision occurs when packets are transmitted by two nodes and collide at a common receiving node. This may occur if transmitting nodes are out of range of one another but within range of a common destination node (known as the hidden terminal problem). In this case, if both transmitters transmit at time intervals close enough for their packets to overlap in time, a collision happens at the receiving node. Both packets are corrupted and the physical layer is unable to decode them. Since they have not been received correctly, the packets need to be retransmitted, which increases the energy consumption.

In contrast to previous surveys that have focused on classifying MAC protocols according to the employed medium access scheme, [BDWL10] provides a thematic taxonomy in which protocols are classified according to the problems they address. Therefore, the MAC protocols can be classified as scheduled protocols, protocols with common active period, preamble sampling protocols and hybrid protocols. Hybrid protocols include protocols that employ contention-free or contention-based medium access.

Some MAC protocols that rely on contention-based medium access are based on slotted CW. Sensor-MAC (S-MAC) [YHE04] is one of the first proposed slotted CW protocols. It is based on network-wide periodic sleep and listening periods, which requires nodes to be synchronized. Synchronization is achieved by periodically exchanging synchronization packets between neighbour nodes.

SIFT [JBT06] was designed for low latency. Like S-MAC, SIFT adopts a fixed-size contention win-

dow. Instead of randomly picking a slot, nodes use a skewed distribution which gives preference to slots at the end of the contention window. Other MAC protocols, such as CrankShaft [HL07], have adopted a contention method with non-uniform distribution.

Timeout-MAC (T-MAC) [HvDL05] reduces idle listening by continuously adapting the length of the listening time of the frames. In T-MAC, nodes perform a procedure similar to the one from S-MAC. However, instead of adopting a fixed listen and sleep period durations, nodes adapt these depending on the frame length. Since all nodes wake-up simultaneously, if a node receives a packet during the listening time it waits for a certain time-out. If the node does not receive anything, it assumes that there are no more packets to be received, and goes to the sleep mode, reducing the inactive time compared to S-MAC.

In the aforementioned protocols, there only is one contention window (with possibly a variable duration). However, work has been performed for the IEEE 802.11 DCF protocol addressing the use of the two-phase collision avoidance mechanism with some modifications. The authors from [HNS⁺06] propose a two-phase collision avoidance scheme to reduce the collision probability and enhance the throughput performance. Contention among stations is resolved in two phases: SuperSlots and SubSlots. A truncated backoff mechanism is used to increase the throughput by reducing the idle time slots.

The work from [YV06] applies “pipelining” techniques to the design of multiple access control protocols so that channel idle overhead could be (partially) hidden, and the collision overhead reduced. In particular, an implicitly pipelined Dual-Stage Contention Resolution (DSCR) MAC protocol is proposed. The authors also propose partial pipelining where the two channels are used. The contention resolution procedure is split into two phases, where pipelined stage 1 includes only contention resolution phase 1 and is performed on the busy tone channel. Contention resolution phase 2 and packet transmissions are performed on the data channel in pipelined stage 2. With DSCR, only one channel is needed, while the scheme with busy tone is left aside. The fundamental difference between DSCR and conventional two-stage contention resolution algorithms is that, in DSCR, stage 1 proceeds in parallel with stage 2 which includes the contention resolution phase 2 and packet transmissions. In the case where the channel activities are observed, channel resources are only utilized in stage 2. In addition, contention windows have dynamic sizes, which depend on the success or failure of data packet transmission.

The Scheduled Channel Polling (SCP) [YSH06] protocol goes one step further by combining scheduling with channel polling to minimize energy consumption. Compared to [HNS⁺06, YV06], the SCP’s two-phase collision avoidance mechanism employs a wake-up tone on a single channel in between the two contention windows and does not distinguish the slots into SuperSlots and SubSlots. The wake-up tone works as a busy tone to inform the other listening nodes of an ongoing transmission. Potential senders that overhear this preamble will postpone their own transmissions.

SCP starts by dividing time into time frames. It achieves synchronization by piggybacking the schedules in broadcast data packets. Once neighbour nodes are synchronized, if a node has data in its Transmission (Tx) queue, it applies the two-phase contention window mechanism depicted in Figure 5.1. The data packet is transmitted in the next time instant the receiver node wakes-up, $T_{wake-up}$. By default, nodes wake up and poll the channel for activity. A sending node reduces the duration of the wake-up tone by starting it just before the receiver starts listening. SCP avoids packet collision by using a two-phase contention window scheme. By orchestrating senders to contend for channel access prior to a poll, SCP-MAC can operate very efficiently for low traffic loads. However, the main limitations of SCP-AC is that it does not provide no implicit mechanism to ensure fairness in the channel utilization, as well as

mechanism to cope with overhearing problems.

5.2 Two-Phase Scheduled Channel Polling mechanism

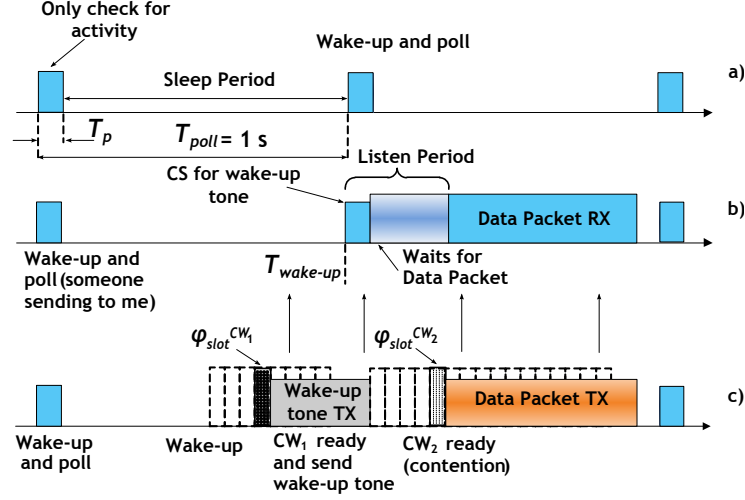


Figure 5.1: SCP time frame period structure.

SCP [YSH06] uses two contention windows, CW_1 and CW_2 . CW_1 is divided into CW_1^{max} time slots of equal duration, as shown in Figure 5.1. When a node wants to transmit a data packet, it randomly chooses a time slot $\varphi_{slot}^{CW_1}$ in CW_1 , with a uniform distribution, whilst sensing the shared medium for the duration of that time slot. The choice of the slot (from the ones available in the interval) follows a uniform distribution:

$$\varphi_{slot}^{CW_1} \in [1; CW_1^{max}] \quad (5.1)$$

All nodes contend to access the channel to transmit packets. If no channel activity is detected (idle channel), a node sends a wake-up tone. The wake-up tone is sent after the time slot chosen in CW_1 and has a minimum duration of 62 bytes (2ms @ 250 kbps). This length is extended for the duration of the remaining time slots (T_{subs_slots}) in CW_1 , as presented in Figure 5.2. This wake-up tone announces to other potential senders that a node is preparing to send data. The node enters CW_2 immediately after the wake-up tone transmission. The second contention window is divided into CW_2^{max} time slots of equal duration. Only the nodes which have data to be sent utilize the two-phase contention window mechanism, while the remaining ones poll the channel.

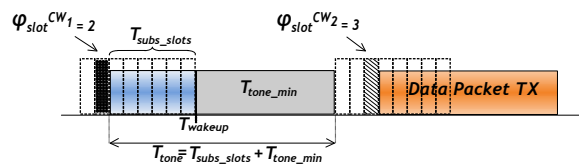


Figure 5.2: Wake-up tone duration as a function of the CW_1 chosen slot.

In both contention windows, a collision occurs if more than one node chooses the same slot (i.e., the wake-up tones collide, or simultaneous transmissions start in the same slot). Only

nodes that succeed in CW_1 enter CW_2 . When more than one node succeeds in CW_1 (at least two nodes transmit the wake-up tones in the same lowest order slot), “effective” data packet collision occurs in CW_2 if the nodes that have been successful in CW_1 randomly choose the same time slot in CW_2 . This simultaneous choice of a time slot corresponds to an effective data packet collision event.

If a node succeeds in sending the wake-up tone during CW_1 , it randomly chooses a slot $\varphi_{slot}^{CW_2}$ from CW_2 by using a uniform distribution:

$$\varphi_{slot}^{CW_2} \in [1; CW_2^{max}] \quad (5.2)$$

The node then starts a carrier sense procedure in CW_2 (with the same duration of CW_1), as shown in Figure 5.1. If the channel is sensed idle, it starts transmitting its frame.

After sending/receiving the data packet, the sender/receiver node checks whether there are any new data packets pending to be sent. If so, the node repeats the steps described above before going into sleep mode.

5.3 Synchronization Phase

The original SCP-MAC protocol distributes schedules as it was developed in S-MAC, where each node broadcasts its schedule in a SYNC packet to its neighbours every synchronization period. In our simulation framework, we defined a maximum time interval equal to 50 ms for the synchronization period. This time interval is used by the node to send a SYNC packet to its neighbours or to receive the SYNC packet from a neighbour node. When the SCP-MAC schedule algorithm is enabled and the sensor network simulation environment starts all nodes choose randomly a value between $t_{wake-up}$ and $t_{init_{CS}} = t_{wake-up} + t_{sync} - t_{CS}$:

$$t_{init_{CS}} \in [t_{wake-up}; t_{wake-up} + t_{sync} - t_{CS}] \quad (5.3)$$

where $t_{CS} = 2$ ms and $t_{sync} = 50$ ms. The value chosen by the sensor node, $t_{init_{CS}}$, corresponds to the simulation time when the sensor node performs the CS of the radio channel for collision avoidance. After performing the CS of the channel (it takes 2 ms) and if the medium is sensed to be free, the sender gets the medium and can start the SYNC packet transmission. This SYNC packet contains fields of the address of the sender and the time of its next wake-up. Initially when the nodes choose randomly a value for $t_{init_{CS}}$ the one that chooses the smallest value is the one that initiates and finishes first the CS gaining the opportunity to transmit the SYNC packet to its neighbours. Immediately after the CS the sensor node transmits the SYNC packet (18 Bytes). Since no nodes have any information about their neighbour's schedules, each node listens to the channel for a certain amount of time. The sensor node wakes-up at time $t_{wake-up}$ and the CC1100 transceiver initiates in RX mode, but it only starts performing the CS at time $t_{init_{CS}}$, as presented in Figure 5.3. The scheme proposed in our simulation framework divides the listen interval into two parts: i) interval for receiving SYNC packets, and ii) interval for CS and send SYNC packet, if an idle channel is detected.

The first part of the interval is time variable because it depends on the value of $t_{init_{CS}}$ chosen randomly by the sensor node and is given by Equation 5.4:

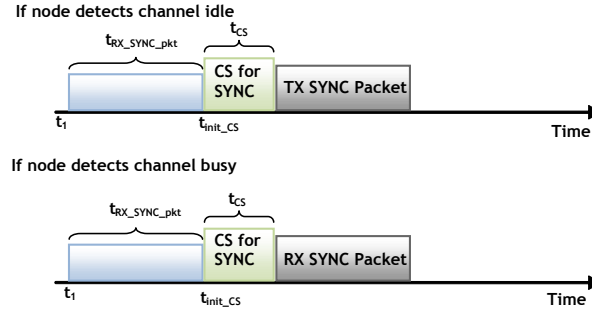


Figure 5.3: SCP Synchronization phase.

$$t_{RX\_SYNC\_pkt} = t_{init\_CS} - t_{wake-up} | t_{init\_CS\_max} = t_{wake-up} + t_{sync} - t_{CS} \quad (5.4)$$

If the sensor node detects a signal during the first interval it receives the packet and verifies what type of packet was received by the sensor node. If the type of packet received was a SYNC packet the node updates the schedule table, while storing the time of the next wake-up from the synchronizer node and assuming the schedule from the synchronizer node as his schedule until the next synchronization period. This schedule table is a timetable for recording neighbours' working schedules. When the timeout timer for synchronization period triggers the nodes will choose again a random value for t_{init_CS} and the one that chooses the smallest value is the one that initiates and finishes the CS first, gaining the opportunity to transmit the SYNC packet to its neighbours.

The original SCP protocol for schedule synchronization offers to all sensor nodes the opportunity to be the synchronizer node. The schedule synchronization mechanism implemented in our simulation framework for the distribution of schedules follows all the same procedures described above. However, when the node chooses a random value for t_{init_CS} and if it gains the opportunity to transmit the SYNC packet to its neighbours, this node will be always the synchronizer node while the others are the follower's nodes, until the end of the simulation. In our simulator this mode is called as the *sync slave* mode. The follower node sets its synchronization timer and its wake-up schedule according to the information sent by the synchronizer. Then, the node will rebroadcast the schedule to its neighbours. Nodes that receive the rebroadcasted packet with synchronization information while having the same schedule value as the received SYNC packet, discard these packets and will not rebroadcast the SYNC packet (in order to prevent from message flooding).

Some nodes may miss the synchronization with other nodes at beginning of the synchronization period due to signal collisions that could occur on the radio channel. These nodes can be synchronized by using SYNC packets rebroadcasting scheme. However, in our simulation, since we are evaluating a small scale network this feature is disabled. This feature is designated for networks that present a large density of sensor nodes (per unit of area) since the probability of two or more nodes to choose the same t_{init_CS} value is higher. By periodically updating each of their schedule tables a long-time clock drift will be prevented.

This process of sending SYNC packets is repeated after a synchronization period, T_{sync} , but can be suppressed by piggybacking the schedules in the data packets when the packets exchanged are of the broadcast type. After the wake-up schedules of all the neighbour nodes from synchronizer node are synchronized, the nodes will wake-up after a certain channel polling period, T_p , and poll the channel for activity sensing. However, maintaining schedule synchronization

leads to a penalty in the overall consumption of the node, as the node must resynchronize after some time, in order to have very little accuracy errors between the schedules clock of all the nodes.

This verification for activity lasts 2 ms for the CC1100 or CC2420 transceivers. If the node detects an idle channel and there is no data to be sent, the node will schedule its next wake-up time instant and goes immediately to the sleep mode after verifying the TX MAC queue. If the node has data in the MAC queue it schedules all the process, as described in Figure 5.1, enabling the data packet transmission in the next time instant the node wakes-up, $t_{wake-up}$, where scheduling the next wake-up (before going to the sleep mode again).

Other type of packet that could be added to overcome the control overhead problem is the SYNC one. Nevertheless, all these explicit SYNC packets can be suppressed by employing the piggybacking technique, when the network is exchanging broadcast traffic. This technique is used to minimize the cost of synchronization by avoiding the explicit SYNC packets. SCP-MAC piggybacks the synchronization information in broadcast packets without increasing the size of the packet length. The SCP-MAC header includes the following three fields: packet type, source address and destination address. In this case, the address field is used to piggyback the schedule information. This technique is more efficient.

5.4 State Transition Diagram for SCP

Before we started to implement the SCP [YSH06] in the Mobility Framework we had proposed a possible Finite State Diagram (FSM). The objective of this FSM is to give a detailed specification of why and how the simulator changes between the different states, while explaining the associated actions and events as shown in Figure 5.4. The corresponding transition events and actions are listed in Table 5.1. This state machine is based on seventeen states, described as follows:

- **START:** The node is switched on;
- **WAIT_SYNC:** The node is waiting for SYNC packets;
- **SYNC:** If the node does not receive a SYNC packet it performs a CS; if detects an idle channel it sends a SYNC packet for the neighbouring nodes;
- **SLEEP:** The node “turns off” the radio and puts CPU in low power;
- **IDLE:** The node is waiting for a task to perform;
- **READING_FRAME:** After receiving a frame, the node has to check if it was successfully received;
- **NAV_SLEEP:** The node goes to the sleep mode until the end of the remaining transmissions (after receiving a wake-up tone not for itself);
- **READING_WAKEUP_TONE:** After receiving the wake-up tone, the node has to check the destination address contained in the wake-up tone packet;
- **CHECK_MAC_HEADER:** To avoid overhearing, the node performs a MAC header checking when it starts receiving the frame;

Table 5.1: SCP-MAC events and actions.

Events	Actions
1	State: WAIT FOR SYNC Schedule: WAIT_RX_SYNC_TRANSMISSION; SYNC_TIMEOUT_START; Save: Node_ID;
2	State: SYNC Schedule: TIMER_TRANSITION_TO_IDLE; FINISH_SYNC; SYNC_BACKOFF; Checks if the sync broadcast packet was received with success.
3	State: SYNC Schedule: SLEEP_TIMEOUT
4	State: IDLE Schedule: TIMER_TRANSITION_IDLE
5	State: SYNC Schedule: IDLE_TO_SYNC Update: Schedule table
6	State: SLEEP Schedule: WAKEUP_TIMEOUT
7	State: BACKOFF_SELECT Schedule: SELECT_BACKOFF Save: Type of packet (unicast or broadcast), CW ₁ slot, CW ₂ slot
8	State: BACKOFF Schedule: BACKOFF_REQUEST;
9	State: IDLE Schedule: BACKOFF_TIMEOUT; TRANSMIT_FRAME After backoff timeout, it returns to IDLE state
10	State: TRANSMIT Schedule: BACKOFF_COMPLETE; TRANSMIT_FRAME
11	State: TRANSMIT Schedule: REQUEST_TRANSMIT_FRAME
12	State: WAKEUP_TONE Schedule: CONTENTION_WINDOW_1_INITIATE Save: The wake-up tone length. Update: For each data packet sent the receiver adds three slots time. Performs CS, chooses a slot time for the CW ₁ .
13	State: IDLE Schedule: STOP_IDLE
14	State: NAV_SLEEP Schedule: COMMUNICATION_ONGOING; NAV_TIMEOUT
15	State: IDLE Schedule: MEDIUM_BUSY Stops the transmission of the frame and goes do IDLE and starts to receive.
16	State: VERIFY_FRAME_FINISH if (unicast_packet== true && channel_still_idle==true && cw1_length_finish==true && data_piggyback_info_ready==true) Checks if the unicast packets were correctly transmitted if (broadcast_packet==true && channel_still_idle==true && data_piggyback_info_ready==false) Complete the transmission of the broadcast packets Schedule: CONTENTION_WINDOW_2_INITIATE;
17	State: WAIT_RESPONSE if (unicast_packet==true) wait for the CTS due to RTS and ACK due to DATA This event is optional. Only if RTS/CTS/DATA/ACK mechanism is enabled.
18	State: VERIFY_FRAME_FINISH Schedule: WAIT_ACK; PERFORM_BACKOFF; TRANSMIT_FRAME The frame transmitted could be SYNC/WAKEUP_TONE/CTS/RTS/ACK/DATA
19	State: TRANSMIT Schedule: TRANSMIT_FRAME Save: NUM_ATTEMPTS
20	State: IDLE Schedule: IDLE_TO_SYNC; UNICAST_PACKET_COMPLETE Save: NUM_ATTEMPTS=0
21	State: IDLE Schedule: BROADCAST_PACKET_COMPLETE; TRANSMIT_FRAME

(continued in next page)

Table 5.2: SCP-MAC events and actions (cont.).

Events	Actions
22	State: READING_FRAME Schedule: MEDIUM_BUSY; RECEIVE_FRAME SYNC_TIMEOUT_START; Save: Node_ID;
23	State: READING_WAKEUP_TONE Schedule: RECEIVE_FRAME
24	State: READING_WAKEUP_TONE if (unicast packet == true) Check if MAC header is correct Schedule: RTS/CTS_OFF
25	State: SLEEP Schedule: UNICAST_PACKET_FOR_OTHER; TIMER_TRANSITION_IDLE
26	State: RXDATA_&_PIGGYBACK_INFO_CHECK Schedule: RX_DATA_&_PIGGYBACK_EXTRACT; SEND_ACK (if enabled) Save: Data packet Update: Schedule table from the piggyback info (piggyback enabled). Schedule table from the SYNC packet received periodically.
27	State: SENDING_ACK if (RTS/CTS mechanism == true) Send ACK packet Schedule: SEND_ACK
28	State: IDLE Schedule: WAKEUP_TIMEOUT; IDLE_TO_SYNC
29	State: IDLE Schedule: RTS/CTS_OFF; PIGGYBACK_EXTRACT Save: Data packet Update: Schedule table (piggybacking info from the data packet)
30	State: BACKOFF_SELECT Schedule: PERFORM_BACKOFF; TRANSMIT_FRAME
31	State: VERIFY_FRAME_FINISH Schedule: WAKEUP; CHECK_MAC_QUEUE This event occurs when the packet is not a data packet.

- **BACKOFF:** The node activates the “backoff time”;
- **BACKOFF_SELECT:** The node selects a “backoff time” depending on the contention window or if it has data or not in MAC queue to send;
- **TRANSMIT:** The node transmits the frame;
- **WAKEUP_TONE:** The node transmits the wake-up tone;
- **VERIFY_FRAME_FINISH:** After sending the packet, the node verifies if the frame was correctly transmitted;
- **WAIT_RESPONSE:** When the RTS/CTS/DATA/ACK mechanism is enabled the node waits for a confirmation of a successful transmission; if the mode is disabled it directly do idle state and goes to sleep;
- **RX_DATA_&_PIGGYBACK_INFO_CHECK:** The node receives the data packet and extracts the schedule information included in the broadcast packet (due to the use of the piggybacking technique), suppressing the sending of explicit SYNC packets;
- **SENDING_ACK:** The node sends an ACK packet to the node that sends the data packet to it, in order to confirm the successful reception; it only sends the ACK if the RTS/CTS/DATA/ACK mechanism is enabled.

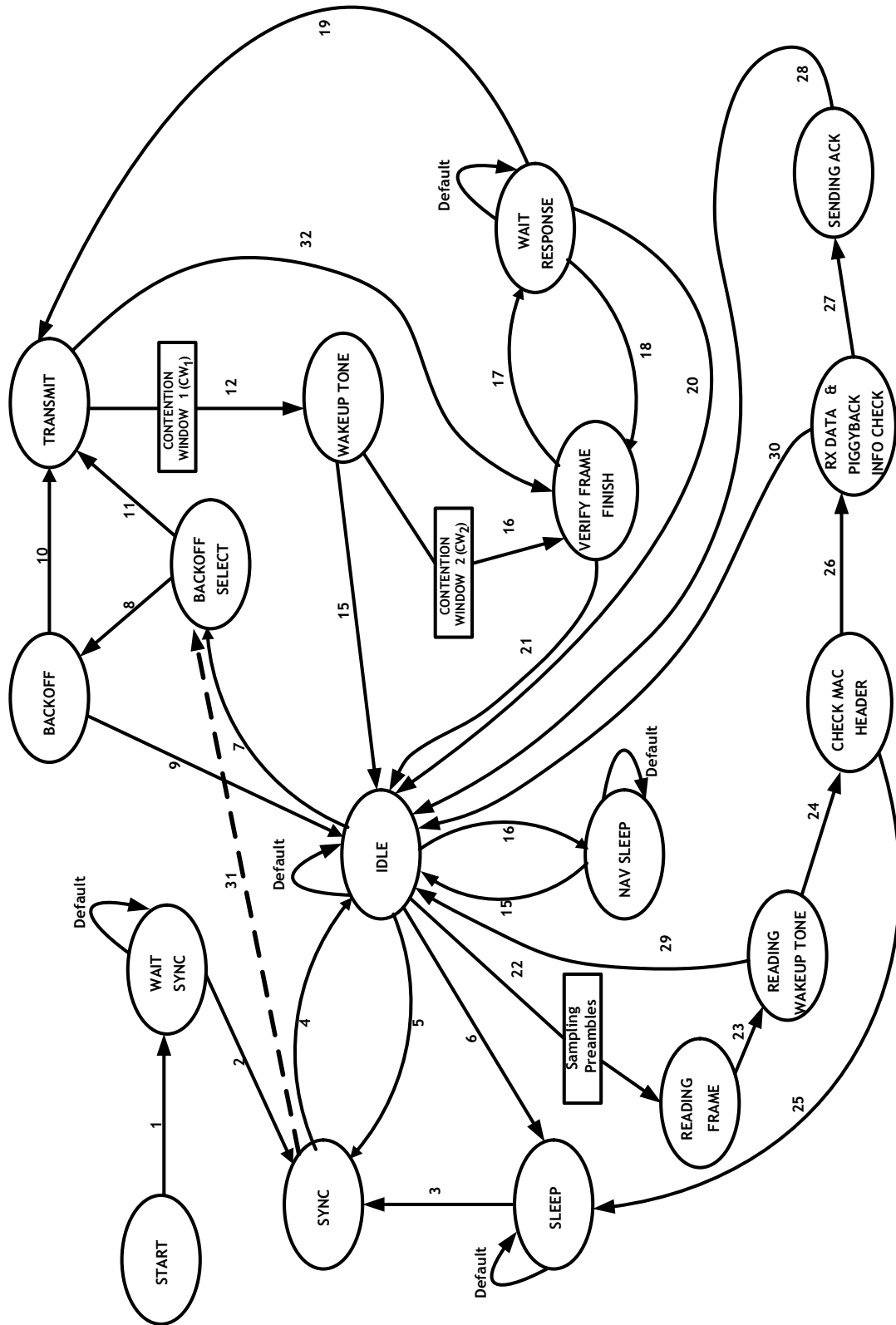


Figure 5.4: SCP State Transition Diagram.

5.5 Implementation of the SCP Simulation Framework

5.5.1 SCP Simulator Parameters and General Definitions

SCP was implemented in the OMNeT++ simulator [VH08, Var10], using the Mobility Framework from [REHD08]. This Mobility Framework supports the CC1100 [CC107] and CC2420 [CC207] radio energy consumption models, as well as several propagation models. We use the free space propagation model, and implemented the two-phase contention window mechanism. Our simulator considers single and multi-hop network topologies. However, to test the two-phase contention window collision avoidance mechanism, the considered topology was single-hop, where the number of contending nodes is increased until there are 100 % of packet collisions, and all the nodes are simultaneously sink and sources (whilst sending broadcast packets). The nodes may communicate only with reachable neighbour nodes.

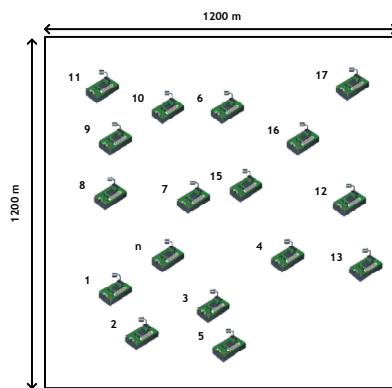


Figure 5.5: Node's deployment example.

Nodes are deployed randomly, and the positions are generated by a Matlab script for a deployment area of $1200 \times 1200 \text{ m}^2$, as shown in Figure 5.5. We vary the number of contending nodes.

For each deployment, with a certain number of contending nodes, a set of six seeds are chosen for the random generator of SCP. All the seeds were chosen such that they guarantee the full delivery of the data packets. The maximum simulation time depends on the last packet to be received by a node.

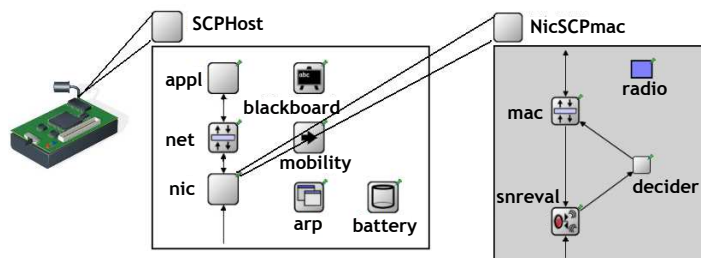


Figure 5.6: OMNeT++ SCP protocol stack and the different layers from a sensor node.

Other parameters are also defined in the simulation configuration file, as presented in Table 5.3 and Table 5.4. Figure 5.7 presents the sensor node protocol stack employed in the simulation framework. Each module is connected with the higher and lower layers. *APPL*, *NET* and *NIC* stand for the application, network and PHY/MAC layer modules, respectively.

Besides these modules, a battery module is included in order to simulate the network or node lifetime, while varying the capacity of the batteries. Nodes are assumed static. In our set of SCP

Table 5.3: Parameters defined in the configuration file for the different sensor node layers.

Module	Parameter	Value
ChannelControl [REHD08]	carrierFrequency	868 MHz
	pMax	110.11 mW
	Sat	-120 dBm
SnrEvalRadioAccNoise3 [REHD08]	transmitterPower	1.0 mW
	thermalNoise	-110 dBm
	snrThresholdLevel	10 dB
	channelModel	free-space
	propagation_coef	2
DeciderRadioAccNoise3 [REHD08]	berLowerBound	10^{-8}
SCPMacLayer [REHD08]	busyRSSI	-97 dBm
	queueLength	50 packets
	poll_period	Varying

simulations, we consider the radio transceivers available in the Mobility Framework [REHD08] and MiXiM [WSKW09], the CC1100 and CC2420, which have a maximum bit rate of 250 kbps. The CC1100 does not necessarily comply with the IEEE 802.15.4 standard and has the lower energy consumption; it operates at 868 MHz.

pMax corresponds to the maximum transmission power allowed in the channel; *sat* one is the signal attenuation threshold (in dBm) which controls the transmission distance. *transmitterPower* is the transmission power, while *thermalNoise* is the electronic noise generated by the thermal agitation. *snrThresholdLevel* is used to decide whether a frame is received correctly. Only when *snr* is less or equal than *snrThresholdLevel* the frame is lost. *channelModel* is the propagation model used in the channel, while *propagation_coef* is the propagation coefficient for the free-space path loss formula. *berLowerBound* is the lower bound of the bit-error-rate, and *busyRSSI* is used to evaluate whether the channel is busy: only if the RSSI is less than *busyRSSI* the channel is clear. *queueLength* is the maximum number of packets waiting to be transmitted allowed in the queue. *poll_period* is the time interval between each time the node wakes up and checks the channel for activity. In our simulation, the CC1100 radio model (from OMNeT++) does not include the poll state [VH08, Var10]: when a node wakes-up and does not have data packets in its MAC queue, it polls the channel during T_{poll} , while the power consumption is the same as in the receiving state. The main differences between the CC1000 and the CC1100 radio transceiver is the maximum data rate achievable by each radio, the CC1100 can be put into sleep mode from which it wakes automatically on receiving any signal, and the CC1100 consumes three times less energy per each bit it receives or sends. For the CC1000 the maximum data rate is 76.8 kbps while for the CC1100 is 500 kbps. The CC1100 radio chip we use in our simulation is the sub-GHz equivalent of the 2.4 GHz CC2420 used in the original SCP.

5.5.2 SCP Simulator Layer Modes

As the SCP was being implemented in OMNeT++, we identified the need of implementing some modes in the simulator, in order to optimize the simulator. These modes are employed to conduct diverse types of experiments regarding single and multi-hop topologies, different traffic patterns generated by the application layer (heavy and periodic), and the need of sending acknowledgement packets as a response to successful reception of data packets. These requirements lead to the addition of the following modes in our simulator.

RTS/CTS mode

The overhearing avoidance problem is solved by the MAC frame headers. The receiver node

Table 5.4: Symbols used in radio analysis, and typical values for CC1100 radio working at 868 MHz and at full data rate.

Symbol	Meaning	CC1100
t_{cs1}	Average carrier sense time [ms]	7
t_{p1}	Average time to poll channel [ms]	3
T_p	Channel polling period [s]	Varying
T_{data}	Data packet period [s]	Varying
λ_{data}	Data packet rate [$1/T_{data}$]	Varying
L_{data}	Data packet length [Bytes]	50
t_{tone}	Duration of the wake-up tone [s]	Varying
r_B	Bit rate (max.) [kbps]	250
n	Number of nodes	Variable
P_{tx}	Power in transmitting [mW]	50.7
P_{sleep}	Power in sleeping [μ W]	60
$P_{rx} = P_{listen}$	Power in receiving/ listening [mW]	49.2
P_{poll}	Power in channel polling [mW]	0.0294
L_{sB}	Piggybacked bytes length	2
L_{sync}	SYNC packet length [Bytes]	18
λ_{sync}	SYNC packet rate [$1/T_{sync}$]	Varying
T_{sync}	SYNC packet period	Varying

examines the destination address of the packet immediately after receiving its MAC header. If the packet destination is for other node, it immediately stops receiving the packet and goes to sleep.

Since control packets cause protocol overhead, for the control overhead problem, SCP has the option to enable or disable the RTS/CTS/DATA/ACK, or simply the DATA/ACK exchange scheme for unicast traffic. When the RTS/CTS mechanism is enabled, overhearing avoidance is performed in the same way as in S-MAC. In our simulator, this option is named as the *acknowledgement packet* one.

Throughput mode

Another mode that is implemented in the application layer of the SCP simulator is named as the *throughput* one. It is useful to test the network's response capacity as the number of transmitting nodes increases. When this mode is enabled, the application layer generates a data packet, then sends it to the lower layer, until it reaches the MAC layer, where it is stored in the TX MAC queue. Then, the node schedules the next wake-up to send the data packet received from the upper layers as quickly as possible, starting to send the next packet as soon as the prior packet is sent. As soon as the node sends the packet the physical layer informs the MAC layer that the transmission has finished. With the *throughput* mode enabled, the MAC layer sends the message which indicates the end of packet transmission to the application layer. When the application layer receives this message it builds another data packet and sends it to the lower layers until it reaches the MAC layer, repeating all the scheduling process that is needed to send a data packet through the network.

Synchronization mode

In our SCP simulator there are two modes to choose the synchronization type: the *sync slave* mode, which uses explicit SYNC packets, and the *piggyback* mode, which piggybacks the schedule information into the broadcasted data packets.

Multi-hop mode

Another mode available in our SCP simulator is the *multi-hop* one, which enables the nodes to organize themselves as presented in Figure 5.7.

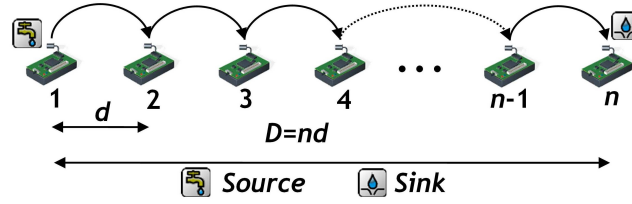


Figure 5.7: Simple linear chain wireless sensor network.

Figure 5.7 presents a linear chain of a WSN, where d is the distance between the sensor nodes, D is the distance between the source and sink, and n is the number of nodes. Only the application layer from node 1 generates data packets to be sent to other nodes, the node n receives data packets and answers with ACK packets when a data packet is received correctly. The remaining nodes are the so called forwarder's nodes, which receive and forward the data packets as well as it sends and receives ACK packets. For this mode, we defined which node was the source and which one was the sink. The remaining ones only had to forward the packets to next sensor node with the identifier i_d+1 .

5.6 Summary and Conclusions

This chapter, provides a detailed description of the mechanisms employed in SCP, along with the lessons learned during our own experience trying to implement the SCP protocol in the Mobility Framework. Moreover, the possible SCP state transition diagram offers to the user the chance to follow closely how the simulator changes between the different simulations states. In order to conduct diverse types of experiments regarding single and multi-hop topologies, different traffic patterns generated by the application layer (heavy and periodic), and the need of sending acknowledgement packets as a response to successful reception of data packets, different modes of simulation were implemented in the simulator. The use and functioning of these modes was described throughout this chapter.

Chapter 6

SCP Performance Evaluation

This chapter presents one of the main contributions of this PhD work, in which the SCP protocol is implemented in a simulator and its performance is evaluated. This chapter is divided into six sections. Section 6.1 starts by presenting the simulation results for single-hop topology in terms of power consumption (with and without piggyback), energy consumed and throughput performance, whilst considering heavy and periodic traffic patterns. Section 6.2 addresses the multi-hop (in a linear chain scenario) performance for the node energy consumption and latency metrics. Section 6.3 introduces a lifetime analysis (enabling piggyback synchronization) for the SCP protocol, by considering a simple battery discharge model, given by Peukert's equation. Section 6.4 addresses the proposal of a stochastic model for the collision probability in the collision avoidance mechanism with two contention windows utilized in the SCP protocol, whilst considering the saturated and unsaturated cases. Analytical results are matched against simulation results for both saturated and unsaturated regimes. A discussion of the results is also provided. Section 6.5 introduces another main contribution of this PhD work. The proposed model for the collision probability is applied to theoretically derive the average MAC service time for a successful transmission as well as the achieved throughput. Numerical results for both service time and throughput are verified by simulation and conclusions are extracted at the end of the section. Finally, in Section 6.6, a comparison of the performance metrics of the SCP while considering an IEEE 802.15.4 compliant and IEEE 802.15.4 agnostic physical layer is presented. Section 6.7 presents final remarks for these tests.

6.1 Single-hop Performance results

The authors from SCP [YSH06] define the expected energy consumption per node, for both LPL and SCP, as the sum of the expected energy spent in each state, as follows:

$$\begin{aligned}\overline{E_{cons}^{SCP}} &= \overline{E_{listen}^{SCP}} + \overline{E_{tx}^{SCP}} + \overline{E_{rx}^{SCP}} + \overline{E_{poll}^{SCP}} + \overline{E_{sleep}^{SCP}} \\ &= P_{listen}t_{CS} + P_{tx}t_{tx} + P_{rx}t_{rx} + P_{poll}t_{poll} + P_{sleep}t_{sleep}\end{aligned}\quad (6.1)$$

This analytical model is based on three assumptions: i) polling time is set to its optimal value, if the traffic rate is known (an unrealistic hypothesis), ii) channel access failures during contention windows are neglected, and iv) the setup times between operation modes in radio are also neglected.

Considering the best case, all the synchronization information is piggybacked on the data packets. The authors define that all synchronization information can be included in the data packet when $r_{data} \geq r_{sync}$. We define both the lower and higher bound for the energy consumption in scheduled channel polling with piggybacked synchronization, considering the maximum and minimum contending times each node can wait. The lower bound for the energy consumption with piggybacked synchronization is given by:

Lower Bound: $\varphi_{slot}^{CW_1}=8 \wedge \varphi_{slot}^{CW_2}=1$

$$\begin{aligned}
\overline{E_{cons\_lw}^{SCP}} &= P_{listen} 2t_B \lambda_{data} \\
&+ P_{tx}(t_{tone} + L_{data} t_B) \lambda_{data} \\
&+ n P_{rx}(t_{tone} + \varphi_{slot}^{CW_2} t_B + L_{data} t_B) \lambda_{data} \\
&+ P_{poll} t_{p1} / T_p \\
&+ n P_{sleep} [1 - 2t_B \lambda_{data} + (t_{tone} + L_{data} t_B) \lambda_{data} \\
&+ n(t_{tone} + \varphi_{slot}^{CW_2} t_B + L_{data} t_B) \lambda_{data} + t_{p1} / T_p]
\end{aligned} \tag{6.2}$$

The upper bound for the energy consumption with piggybacked synchronization is given by:

Upper Bound: $\varphi_{slot}^{CW_1}=1 \wedge \varphi_{slot}^{CW_2}=16 \wedge CW_1^{max}=8$

$$\begin{aligned}
\overline{E_{cons\_hg}^{SCP}} &= P_{listen} 2t_B \lambda_{data} \\
&+ P_{tx}(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1}) t_B + (\varphi_{slot}^{CW_2} - 1) t_B + L_{data} t_B) \lambda_{data} \\
&+ n P_{rx}(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1}) t_B + \varphi_{slot}^{CW_2} t_B + L_{data} t_B) \lambda_{data} + P_{poll} t_{p1} / T_p \\
&+ P_{sleep} [1 - (2t_B \lambda_{data} + (t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1}) t_B \\
&+ (\varphi_{slot}^{CW_2} - 1) t_B + L_{data} t_B) \lambda_{data} + n(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1}) t_B \\
&+ \varphi_{slot}^{CW_2} t_B + L_{data} t_B) \lambda_{data} + t_{p1} / T_p)]
\end{aligned} \tag{6.3}$$

In the worst case, if no piggybacking is possible, all the synchronization must be performed with SYNC packets. The authors from SCP [YSH06] also define the optimal synchronization period time. In this work, we define both the lower and upper bounds for the energy consumption in SCP without piggybacked synchronization, considering the maximum and minimum contention times for each node. The lower bound for the energy consumption without piggybacked synchronization is given by:

Lower Bound: $\varphi_{slot}^{CW_1}=8 \wedge \varphi_{slot}^{CW_2}=1$

$$\begin{aligned}
\overline{\overline{E_{cons\_lw}^{SCP}}} &= P_{listen}(t_B \lambda_{data} + t_{cs1} \lambda_{sync}) \\
&+ (P_{tx} + n P_{rx})(t_{tone} + L_{data} t_B) \lambda_{data} \\
&+ (P_{tx} + n P_{rx})(t_{tone} + L_{data} t_B) \lambda_{sync} \\
&+ P_{poll} t_{p1} / T_p \\
&+ P_{sleep} [1 - ((t_B \lambda_{data} + t_{cs1} \lambda_{sync}) + (n + 1)(t_{tone} + L_{data} t_B) \lambda_{data} \\
&+ (n + 1)(t_{tone} + L_{data} t_B) \lambda_{data} + t_{p1} / T_p)]
\end{aligned} \tag{6.4}$$

In turn, the upper bound for the energy consumption without piggybacked synchronization is given by:

Upper Bound: $\varphi_{slot}^{CW_1}=1 \wedge \varphi_{slot}^{CW_2}=16 \wedge CW_1^{max}=8$

$$\begin{aligned}
\overline{E_{cons\_hg}^{SCP}} = & P_{listen}(2t_B\lambda_{data} + t_{cs1}\lambda_{sync}) \\
& + (P_{tx} + nP_{tx})(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{data} \\
& + (P_{tx} + nP_{tx})(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{sync} \\
& + P_{poll}t_{p1}/T_p \\
& + P_{sleep}[1 - ((2t_B\lambda_{data} + t_{cs1})\lambda_{sync}) \\
& + (n+1)(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_1} - 1)t_B \\
& + L_{data}t_B)\lambda_{data} + (n+1)(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B \\
& + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{data} \\
& + (n+1)(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B \\
& + L_{data}t_B)\lambda_{data} + (n+1)(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B \\
& + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{sync} + t_{p1}/T_p)] \tag{6.5}
\end{aligned}$$

6.1.1 Power Consumption without Piggyback and periodic traffic

It is worthwhile to compare simulation and analytical results for the average power consumption for each node. When no piggybacking is considered after we defined the “adapted” analytical model (lower and upper bounds), we ran the simulator and extracted the values. For these tests the network is composed by five nodes arranged in star topology. In this simulations, the *sync slave* mode is enabled, the synchronization time is defined as $t_{sync}=50$ ms and the inter arrival period is variable. Moreover the simulator also considers, t_{sync} , the synchronization period, which depends on the inter arrival period (already defined by the authors from [YSH06]), T_{sync} . As the synchronization period increases the wake-up tone duration also increases. We consider that the maximum contention window sizes is $CW_1^{max}=8$ and $CW_2^{max}=16$. For this experiment, all five nodes from the network are placed onto a single-hop configuration, where each node generates and broadcasts 50 data packets (50 Bytes each). Since the inter arrival period varies between 50 and 300 s, the traffic load is considered to be light. Simulations are run five times for each of the six seeds, generating a total of 30 experiences. For each experiment the average power consumption of each node is obtained, as shown in Figure 6.1. The achieved standard deviations are negligible.

Figure 6.1 presents a comparison between the simulations and analytical results (higher and upper bound), as a function of the inter arrival period. Considering $CW_1^{max}=8$ and $CW_2^{max}=16$, it can be observed that the simulation curve is similar to the lower bound curve defined by the analytical model. Besides, the Mean Square Error (MSE) is calculated with respect to the analytical lower bound curve, and a value of 4.8155×10^{-6} mW is achieved. This shows a high similarity between the simulation and the analytical results.

Another comparison between the simulation and the upper/lower bound curves is the absolute error for each analytical bound, as shown in Figure 6.1. As the error decreases while the inter arrival period is increasing, the similarity between the simulation and the analytical lower bound results increases.

To show how the t_{sync} parameter influences the power consumption with no piggybacking performance results, changed its value from 50 to 60 ms, whilst maintaining the remaining param-

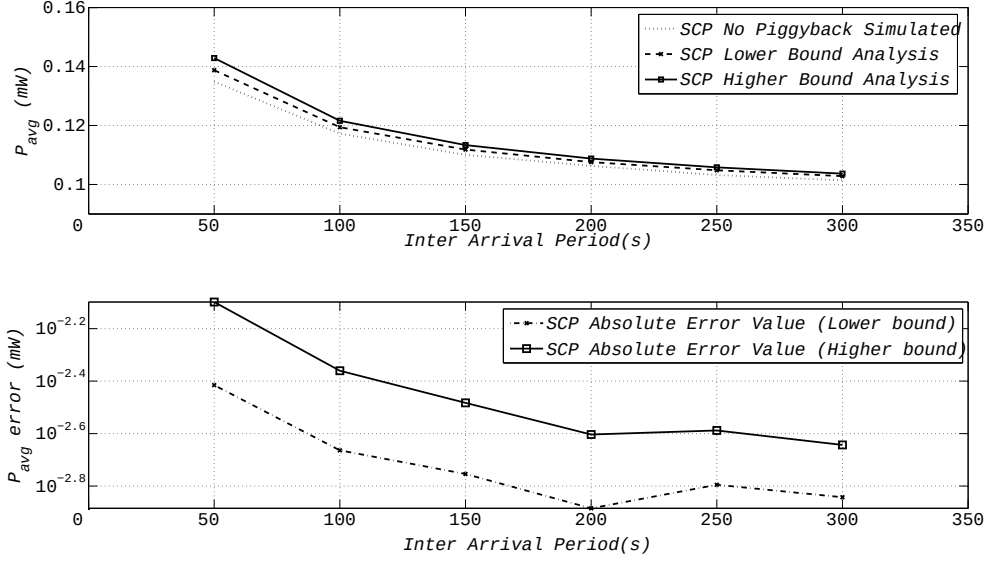


Figure 6.1: Comparison between the lower/upper bound and the simulation results for the power consumption per node set of SCP simulations with no piggybacking.

eters. With this modification, the simulation results for the power consumption becomes closer to the lower bound (in comparison to the ones obtained when $t_{sync} = 50$ ms). We also computed the MSE for $t_{sync} = 60$ ms, obtaining a value of 1.2808×10^{-6} mW. From these results, one may conclude that the power consumption with the *sync slave* mode enabled presents better results when $t_{sync} = 60$ ms. However, for values of t_{sync} lower than 50 ms it was not possible to achieve stable results with the SCP simulations. Finally, it is worthwhile to note that for values of t_{sync} longer than 60 ms higher values for the SCP power consumption are achieved.

6.1.2 Power Consumption with Piggyback and periodic traffic

The lower and upper bound for the adapted analytical model are also defined for the case when synchronization schedules are piggybacked. The simulator topology and MAC parameters considered for this test are the same as the ones previously considered. However, since all the exchanged traffic is of the broadcast type, all the SYNC packets can be suppressed and the schedule synchronization is performed by using the piggyback technique. Hence, the *piggyback* mode is enabled for this experiment. There is no need to define the values for the parameter t_{sync} , as the schedule information is already piggybacked into the data packets. Therefore, since the time spent during SYNC packets exchange is not wasted in this experiment, there is an increase of the efficiency. This leads to a consequent node energy consumption diminishing. For this set of simulations, we define the synchronization period as $T_{sync} = T_{data}$, meaning that the wake-up tone duration is inversely proportional to T_{data} , i.e., as T_{data} increases, the wake-up tone duration decreases. The dependence of the average power consumption of each node on the inter arrival period is shown in Figure 6.2, where the simulations and analytical results (upper and lower bounds) are also presented for comparison purposes. The standard deviations are negligible.

For $CW_1^{max} = 8$ and $CW_2^{max} = 16$, the obtained simulation results are similar to the lower bound curve defined by the analytical model until the inter arrival period achieves 150 s. For a inter arrival period longer than 150 s, the simulation results are similar to the upper bound curve.

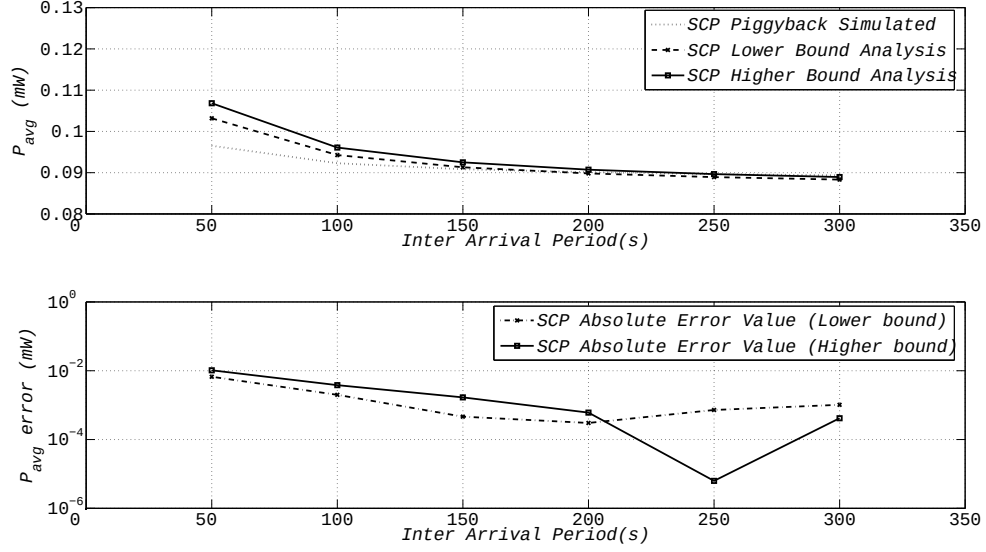


Figure 6.2: Comparison between the lower/upper bound and the simulation results for the power consumption per node set of SCP simulations with piggybacking.

The MSE value obtained for this experiment with respect to the lower bound curve is equal to 8.3763×10^{-6} mW. This value is higher than the one obtained with explicit SYNC packets. This is due to the simulation results similarity with the lower bound, which only occurs until an inter arrival period of 150 s. For inter arrival periods longer than 150 s, the simulation results diverges from the analytical lower bound, leading to an increase of the MSE (with respect to lower the bound).

The absolute error between the simulation values and the upper and lower analytical bound curves is also determined as the error decreases (while the inter arrival period is increasing), the similarity between simulation and analytical lower bound results increases.

By comparing the power consumptions with explicit SYNC packet and with piggyback synchronization, we observe that the piggyback technique is truly efficient, since the power consumption with piggybacking achieves lower values than the one with explicit SYNC packets.

To show how the size of the wake up influences the simulation results performance, we define the wake-up tone duration always equal to 2 ms. The only variable parameter is $T_{data} \in \{50; 100; 150; 200; 250; 300\}$.

With this modification, the value of the MSE decreases to 7.9825×10^{-6} mW. By comparing the power consumptions in the presence and absence of a fixed wake up tone duration, the energy saving obtained with a fixed wake-up tone duration are adequate (approximately 0.005 mW).

6.1.3 Throughput Performance with heavy traffic load

In the previous sections, the simulations were performed by applying periodic traffic load. However, in real world applications, WSNs do not have the capability to predict what type of traffic load is being exchanged with high accuracy. For example, in an healthcare scenario, the sensor nodes deliver the monitoring data from the vital signs of the patients at a lower data rate (in usual situations). However, when a patient presents anomalies in his/her vital signs, the sensor node may deliver data at a higher rate, leading to the need for higher network throughput.

For this set of experiments, we have enabled the *throughput* mode at the application layer. This is useful to test the network's response capability when the number of transmitting nodes increases. By varying the number of transmitting nodes, the contending time of the network will increase, leading to an increase of the collision probability. Each node generates 20 packets (with 100 Bytes each). For these tests the a network is composed by five nodes arranged in star topology. In these experiences the nodes could operate at a duty cycle of 0.2 %, when there is no data to be sent or received, while polling the channel each second. Besides the variation of the number of transmitting nodes, the CW_1 and CW_2 contention window sizes also vary. Figure 6.3 shows the average throughput for three experiments: the first one considers $CW_1^{max} = 8$ and $CW_2^{max} = 16$, second one considers $CW_1^{max} = CW_2^{max} = 78$, while the third one considers $CW_1^{max} = CW_2^{max} = 100$.

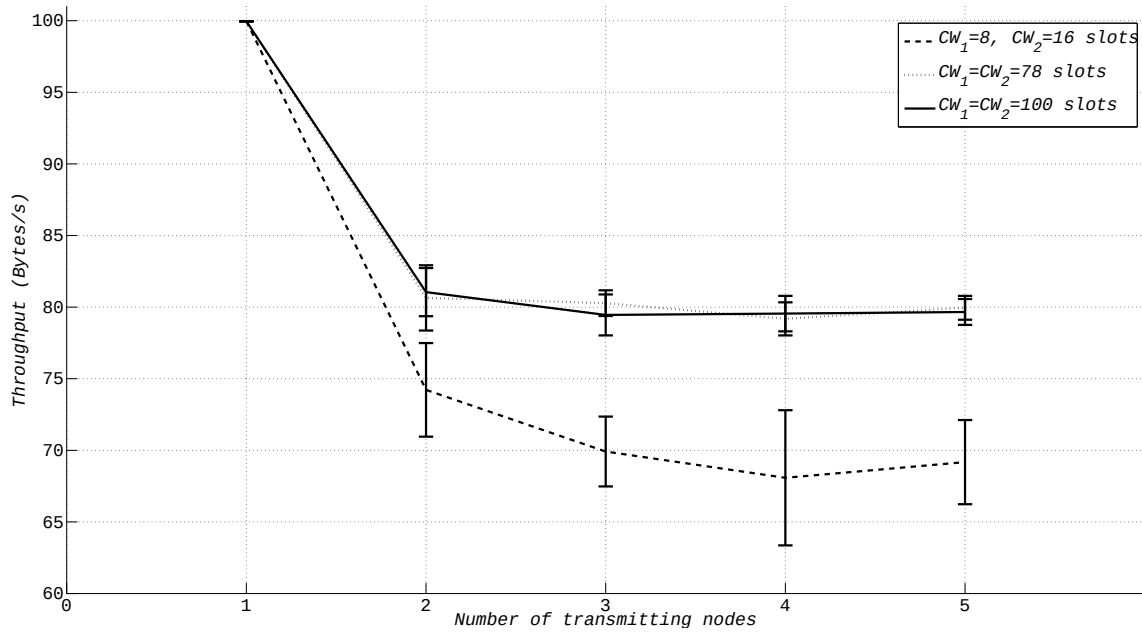


Figure 6.3: SCP-MAC throughput performance considering high traffic load for different contention windows sizes configurations and number of transmitting nodes.

By analysing Figure 6.3, the throughput achieves its maximum (for all contending time configurations) when there is only one node transmitting, as expected, since there is no more nodes competing for the channel to send packets. When two nodes are competing for the channel, the throughput drops to 20 - 25 % of the maximum achievable throughput, because there is more than one node trying to transmit the data packet. As the number of transmitting nodes increases, the contending time will also increase, leading to a collision probability increase.

For a $CW_1^{max} = 8$ and $CW_2^{max} = 16$ configuration the throughput curve is lower than the other ones, because for this configuration there is less contention window time slots, increasing the chance of nodes to choose the same time slot and therefore increase the collision probability. For a $CW_1^{max} = CW_2^{max} = 78$ and a $CW_1^{max} = CW_2^{max} = 100$ contention windows configuration the throughputs achieved are higher and more stable (80 B/s) than the first one. This is due to the larger maximum contention windows sizes.

The standard deviations are presented for all the experiments. The curve that presents higher deviations is the one that presents lower values for the throughput (first experiment).

6.2 Multi-hop Energy Efficiency - Linear Chain Scenario

For this set of experiments, we intend to evaluate the SCP energy and end-to-end latency performance for multi-hop networks in a linear topology for the nodes. Besides the energy consumption per node, curves for the multi-hop experiments (obtained from our simulator), an analytical model is proposed for multi-hop communications in the linear chain. It accounts for the MAC protocol contention time.

For multi-hop experiments we enabled the *multi-hop* mode in the SCP protocol stack, where only the application layer from node 1 generates data packets to be sent to the other nodes. The node n receives data packets and answers with ACK packets when a data packet is received correctly. The remaining nodes are the so called forwarder's nodes, which receive and forward the data packets and the answer and receive ACK packets through the linear chain (see Figure 5.7). In the evaluation of the analytical model the parameter T_{sync} is equal to zero, meaning that the wake-up tone duration is always equal to 2 ms. The polling interval for this analytical evaluation is set to one second.

In addition to the energy model derived for the single-hop topology in [YSH06], we can derive the energy model boundaries (higher and lower bound) for a multi-hop topology in a linear chain. In our analytical model for a linear multi-hop chain, we define (in the equation) the X's nodes as source(s), the Y's nodes as forwarders, and Z's nodes as sink(s). In our topology we deploy $(n-2)$ Y nodes, one Z node, and one X node. For the multi-hop evaluation the acknowledgement packets were enabled with data packet re-transmissions up to three retries.

For the energy consumption lower bound in a linear multi-hop chain, we consider that all the packets are sent at the first time. The energy consumption with piggybacked synchronization in a linear multi-hop chain lower bound for the energy consumption with piggybacked synchronization in a linear multi-hop chain with the maximum timeout to receive de ACK packet, $t_{to_{ack}}$, is given by:

Lower Bound: $\varphi_{slot}^{CW_1}=8 \wedge \varphi_{slot}^{CW_2}=1 \wedge t_{to_{ack}}=10 \times 10^{-3}s$

$$\begin{aligned}
 \overline{E_{multi\_lw}^{SCP}} &= (n-2)(P_{tx}Y_{tx}^{d\_ack} + P_{rx}Y_{rx}^{d\_ack} + P_{listen}Y_{listen}^{data} + P_{poll}Y_{poll}^{data}) \\
 &+ (P_{tx}X_{tx}^{data} + P_{listen}X_{listen}^{data} + P_{poll}X_{poll}^{data} + P_{rx}X_{rx}^{ack}) \\
 &+ (P_{rx}Z_{rx}^{data} + P_{listen}Z_{listen}^{data} + P_{poll}Z_{poll}^{data} + P_{tx}Z_{tx}^{ack}) \\
 &+ P_{sleep}[1 - ((n-2)(Y_{tx}^{d\_ack} + Y_{rx}^{d\_ack} + Y_{listen}^{data} + Y_{poll}^{data}) \\
 &+ (X_{tx}^{data} + X_{listen}^{data} + X_{poll}^{data} + X_{rx}^{ack}) \\
 &+ (Z_{rx}^{data} + Z_{listen}^{data} + Z_{poll}^{data} + Z_{tx}^{ack})))] \\
 Y_{tx}^{d\_ack} &= \frac{(t_{tone} + (L_{data} + L_{ack})t_B + t_{to_{ack}})}{T_p}, \\
 Z_{tx}^{ack} &= \frac{L_{ack}t_B + t_{to_{ack}}}{T_p}, \\
 X_{tx}^{data} &= (t_{tone} + L_{data}t_B)\lambda_{data}, \\
 Y_{rx}^{d\_ack} &= \frac{(t_{tone} + (L_{data} + L_{ack})t_B + t_{to_{ack}})}{T_p}, \\
 X_{rx}^{ack} &= (L_{ack}t_B + t_{to_{ack}})\lambda_{data},
 \end{aligned}$$

$$\begin{aligned}
Z_{rx}^{data} &= \frac{t_{tone} + L_{data}t_B}{T_p}, \\
X_{listen}^{data} &= 2t_B\lambda_{data}, \\
Y_{listen}^{data} &= Z_{listen}^{data} = \frac{P_{listen}2t_B}{T_p}, \\
X_{poll}^{data} &= Y_{poll}^{data} = Z_{poll}^{data} = \frac{t_{p1}}{T_p}
\end{aligned} \tag{6.6}$$

We consider the worst-case scenario for the energy consumption higher bound in a linear multi-hop chain higher bound, we consider the worst scenario, when all the nodes reach the maximum number of retries, ι_{ret} , meaning that each data packet is send or forward after three retries. The higher bound consumption for the energy consumption with piggybacked synchronization in a linear multi-hop chain is given by:

Higher Bound: $\varphi_{slot}^{CW_1}=1 \wedge \varphi_{slot}^{CW_2}=16 \wedge CW_1^{max}=8 \wedge \iota_{ret}=3$

$$\begin{aligned}
\overline{E_{multi\_hg}^{SCP}} &= \iota_{ret}[(n-2)(P_{tx}\widehat{Y_{tx}^{d\_ack}} + P_{rx}\widehat{Y_{rx}^{d\_ack}} + P_{listen}\widehat{Y_{listen}^{data}} + P_{poll}\widehat{Y_{poll}^{data}}) \\
&+ (P_{tx}\widehat{X_{tx}^{data}} + P_{listen}\widehat{X_{listen}^{data}} + P_{poll}\widehat{X_{poll}^{data}} + P_{rx}\widehat{X_{rx}^{ack}}) \\
&+ (P_{rx}\widehat{Z_{rx}^{data}} + P_{listen}\widehat{Z_{listen}^{data}} + P_{poll}\widehat{Z_{poll}^{data}} + P_{tx}\widehat{Z_{tx}^{ack}}) \\
&+ P_{sleep}(1 - ((n-2)(\widehat{Y_{tx}^{d\_ack}} + \widehat{Y_{rx}^{d\_ack}} + \widehat{Y_{listen}^{data}} + \widehat{Y_{poll}^{data}}) \\
&+ (\widehat{X_{tx}^{data}} + \widehat{X_{listen}^{data}} + \widehat{X_{poll}^{data}} + \widehat{X_{rx}^{ack}}) \\
&+ (\widehat{Z_{rx}^{data}} + \widehat{Z_{listen}^{data}} + \widehat{Z_{poll}^{data}} + \widehat{Z_{tx}^{ack}})))] \\
\widehat{Y_{tx}^{d\_ack}} &= (t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + (L_{data} + L_{ack})t_B + t_{to_{ack}})/T_p, \\
\widehat{Z_{tx}^{ack}} &= \frac{L_{ack}t_B + t_{to_{ack}}}{T_p}, \\
\widehat{X_{tx}^{data}} &= (t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{data}, \\
\widehat{Y_{rx}^{d\_ack}} &= (t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + \varphi_{slot}^{CW_2}t_B + (L_{data} + L_{ack})t_B + t_{to_{ack}})/T_p, \\
\widehat{X_{rx}^{ack}} &= (L_{ack}t_B + t_{to_{ack}})\lambda_{data}, \\
\widehat{Z_{rx}^{data}} &= \frac{t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + \varphi_{slot}^{CW_2}t_B + L_{data}t_B}{T_p}, \\
\widehat{X_{listen}^{data}} &= 2t_B\lambda_{data}, \\
\widehat{X_{poll}^{data}} &= \widehat{Y_{poll}^{data}} = \widehat{Z_{poll}^{data}} = \frac{t_{p1}}{T_p} \\
\widehat{Y_{listen}^{data}} &= \widehat{Z_{listen}^{data}} = \frac{P_{listen}2t_B}{T_p}
\end{aligned} \tag{6.7}$$

In multi-hop networks, there is no optimal working point. Hence, network performance depends on what application is supported by the network. The users configure the MAC layer according to the application needs while, depending on the tradeoffs that can be established between the maximum end-to-end latency and the energy consumption, in order to obtain the network or node lifetime (suitable for the application).

Another feature that is still not implemented in our simulator is the adaptive channel polling.

It allows for sending a stream of packets from the source to the sink by switching to high duty cycles (it is designed to reduce the latency of the packets). This also enables the transmission of multiple packets in one polling interval.

The topology used in this set of experiences is the one presented in Figure 5.7, with a network composed by a 9-hop linear topology with ten nodes (each one with a separation of 50 m from each other). The source node will generate 20 packets (50 bytes each), with a variable inter arrival period between 0 and 10 s. Nodes will rebroadcast the data packets along the linear chain until they reach the most distant node from the chain. All the packets are sent as unicast ones and the RTS/CTS mechanism is not enabled. Only the *acknowledgement* mode, with up to three retries, is enabled in our simulations.

In this experiment, the maximum sizes for the contention windows are variable, increasing or diminishing the probability of packet collisions. Each node polls each second. For comparison purposes (with the SCP original multi-hop experiment [YSH06]), we defined $CW_1^{max}=CW_2^{max}=208$, so that the maximum contending time of our simulations could be more or less equal to the original SCP maximum contending time. The other contention windows size configurations presented here were the ones that we achieved better results.

Considering the inter arrival time equal to zero means the application layer generates a data packet, and sends it to the lower layers, until it reaches the MAC layer, where it is stored in the TX MAC queue. Then, the node schedules the next wake-up to send the data packet received from the upper layers the fastest way possible, starting to send the next packet as soon as the prior packet is sent. When the node sends the packet, the physical layer informs the MAC layer that the transmission had finished and with the *throughput* mode enabled the MAC layer sends the message that indicates the end of packet transmission to the application layer. If the application layer receives this message it will generate another data packet and will send it to the lower layers until it reaches the MAC layer, repeating all the scheduling process needed to send a data packet throughout the network. This evaluates the performance of the multi-hop network when non periodic traffic is generated (near the real world). In order to test the multi-hop network performance for periodic traffic, the inter arrival periods vary between 1 and 10 s.

By observing Figure 6.4, the energy curve for $CW_1^{max}=CW_2^{max}=208$ is the one that presents a higher energy consumption per node, because of the maximum contending time used by the nodes to avoid the packets collisions. When comparing with the energy consumption per node for multi-hop experiments in the original paper [YSH06], our energy consumptions are lower. The others contention windows configurations, present a lower energy consumption per node (less than 0.05 J). For all the configurations the energy consumption behaviour is more or less stable as the inter arrival time is increasing.

6.3 Lifetime Analysis with piggyback (periodic traffic)

In this section we describe a model that allows us to calculate and set SCP-MAC's parameters with the purpose of optimize the overall energy consumption. Using the model, we intend to illustrate the effect of different application variables such as the contention window maximum sizes, inter arrival periods, network density, and polling period.

To calculate the lifetime of an application that employs the SCP-MAC protocol with piggybacked synchronization, we consider a periodic sensing application that sends data to a base station. There are various definitions for the WSN lifetime. The WSN lifetime could be sensor node

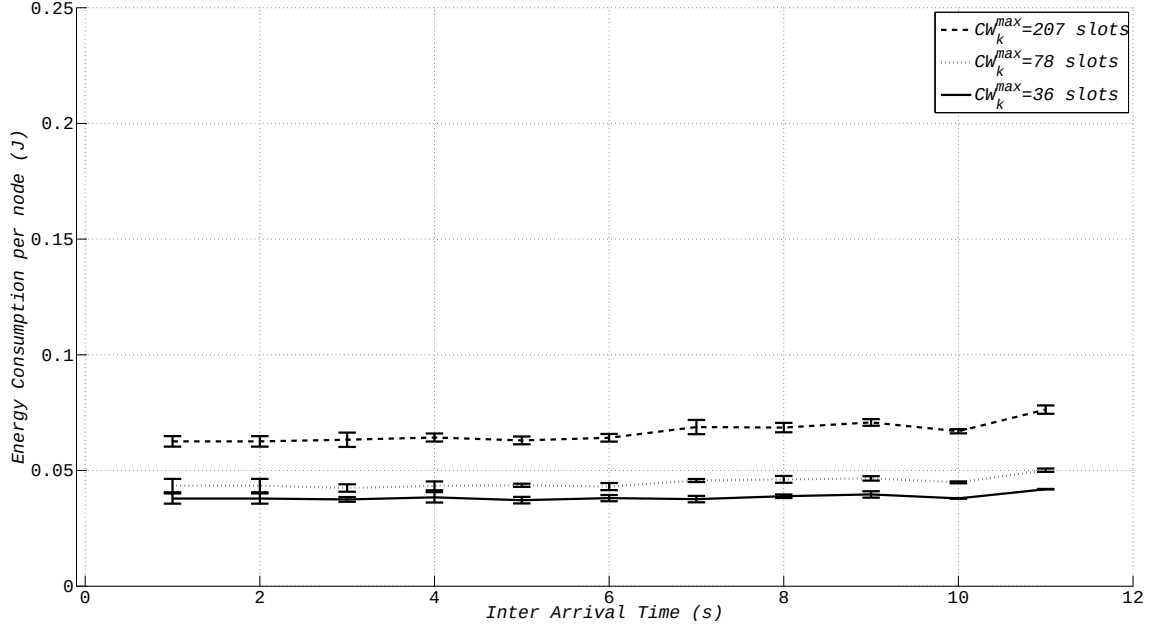


Figure 6.4: Mean energy consumption per node for multi-hop experiments with different contention windows sizes configurations (20 data packets over 9 hops), $k \in \{1, 2\}$.

related or network related. Authors that have a sensor node related interpretation define the WSN lifetime as the time until the first sensor node “dies” and stops transmitting/receiving packets. For the authors that have a network related interpretation, the WSN lifetime is defined as the time until a certain percentage of sensor nodes “dies” and stops receiving/transmitting packets.

The node’s lifetime is given by the overall energy consumption, which is defined in millijoules per second, or milliwatts. The total energy consumed by the node can be obtained by multiplying the energy ($\overline{E}_{cons}^{SCP}$) by the node lifetime, t_{node} . Since we want to calculate the maximum lifetime a sensor node can achieve, when employing the SCP-MAC protocol with piggybacked synchronization, we also need to add the energy consumed by the sensors, which are attached to the Mica2 mote. Considering the application deployed from [MCP⁺02] and also mentioned by the authors in [YSH06], where the node’s lifetime with BMAC protocol is estimated, we also assume that each node takes 1100 ms to start, sample, and collect the data from its sensors. For this test we defined that data is sampled every minute ($r_{dat} = 1/(1 \times 60) \text{ min}^{-1}$).

Therefore the total energy consumption is given by:

$$\begin{aligned}
 \overline{E}_{cons}^{SCP} &= \overline{E}_{listen}^{SCP} + \overline{E}_{tx}^{SCP} + \overline{E}_{rx}^{SCP} + \overline{E}_{poll}^{SCP} + \overline{E}_{sleep}^{SCP} + \overline{E}_{sensor}^{SCP} \\
 &= P_{listen}t_{CS} + P_{tx}t_{tx} + P_{rx}t_{rx} + P_{poll}t_{poll} + P_{sleep}t_{sleep}
 \end{aligned} \tag{6.8}$$

To calculate the energy consumption of the sensors (and the node’s lifetime) we need to specify the amount of current that is drained by the sensors. These values are presented in Table 6.1.

The energy associated with the sampling data, $\overline{E}_{sensor}^{SCP}$, is given by:

$$\begin{aligned}
 t_{dat} &= t_d \times r_{dat} \\
 \overline{E}_{sensor}^{SCP} &= t_d i_{dat} V_{cc}
 \end{aligned} \tag{6.9}$$

Table 6.1: Parameters for a monitoring application that uses Mica2 motes.

Symbol	Parameter	Value
C_{batt}	Capacity of the battery [mAh]	2500
V_{cc}	Voltage [V]	3
i_{dat}	Sample sensors [mA]	20
i_{tx}	Send a byte [mA]	16.9
i_{rx}	Receive a byte [mA]	16.4
i_{sleep}	Sleep [μ A]	20
t_{dat}	Time to sample sensors [s]	1.1

The energy consumed by the other components that contribute to the overall energy consumption of the sensor node have also been calculated, considering the higher bound equation of the SCP protocol with piggybacked synchronization. The energy consumed during the node listening process is given by:

$$t_{listen} = 2t_B \lambda_{data}$$

$$\overline{E}_{listen}^{SCP} = t_{listen} i_{rx} V_{cc} \quad (6.10)$$

The energy consumed during the node transmission process is given by:

$$t_{tx} = (t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{data}$$

$$\overline{E}_{tx}^{SCP} = t_{tx} i_{tx} V_{cc} \quad (6.11)$$

For the node reception process, the energy consumption is given by:

$$t_{rx} = n(t_{tone} + (CW_1^{max} - \varphi_{slot}^{CW_1})t_B + (\varphi_{slot}^{CW_2} - 1)t_B + L_{data}t_B)\lambda_{data}$$

$$\overline{E}_{rx}^{SCP} = t_{rx} i_{rx} V_{cc} \quad (6.12)$$

The energy consumption during the node polling process is given by:

$$t_{poll} = t_{p1}/T_p$$

$$\overline{E}_{poll}^{SCP} = t_{poll} i_{rx} V_{cc} \quad (6.13)$$

And finally, the energy consumed during the sleeping time of a sensor node is given by:

$$t_{sleep} = 1 - (2t_B \lambda_{data}(t_{tone} + L_{data}t_B)\lambda_{data} + n(t_{tone} + \varphi_{slot}^{CW_2}t_B + L_{data}t_B)\lambda_{data} + t_{p1}/T_p)$$

$$\overline{E}_{sleep}^{SCP} = t_{sleep} i_{sleep} V_{cc} \quad (6.14)$$

The lifetime of a sensor node, t_{node} , depends on the total energy consumption, $\overline{E}_{cons}^{SCP}$, and the capacity of the battery. Therefore, we can establish a boundary with respect to the available capacity of the battery:

$$t_{node} = \frac{C_{batt} \times V_{cc}}{E_{cons}^{SCP}} \times 60 \times 60 \quad (6.15)$$

This equation is considered when assuming an ideal battery, where there are no battery recovery phenomena or other phenomena related with battery discharge.

One of the simplest models that describes the battery discharge is given by the Peukert's equation, which takes into account the rate capacity effect but does not take into account the recovery effect. Peukert equation showed numerically how discharging at higher rates removes more power from the battery, than discharging at lower rates. The Peukert's battery model is simple but it has some flaws, such as the overestimation of battery lifetime for most cases [JH09]. The original formula is written like,

$$I^{n_{peuk}} T = C_{batt} \quad (6.16)$$

where I is the discharge current in ampere, T is the time in hour, C_{batt} is the capacity of the battery in ampere hour, and n_{peuk} is the Peukert's exponent for that particular battery type. Peukert's equation, as it is, has to be used on batteries specified at the "Peukert Capacity". It means the capacity of the battery when discharged at 1 A. Rarely the batteries are quoted like this. To account for the way the battery capacity is quoted we need to modify the formula transforming the original Peukert's equation into the following one:

$$T = \frac{C_{batt}}{(I / (\frac{C_{batt}}{R}))^{n_{peuk}}} \times \left(\frac{R}{C_{batt}} \right) \quad (6.17)$$

where R is the battery hour rating.

The battery hour rating in 99 % of the batteries is equal to 20 h. Depending on the type of battery the hour rating changes, as stated by the authors in [SK11]. The Peukert's exponent is directly related with the internal resistance of the battery and varies between 1 and 1.4. The higher the internal resistance is, the higher the losses while charging and discharging are, especially at higher currents. Therefore, it means that the faster a battery is discharged, the lower is its capacity.

By solving Equations 6.8 to 6.14, and considering the parameters from Table 6.1, we can estimate the maximum energy needed for a given network configuration. Lifetime is going to be estimated based on the estimated overall energy consumption, considering a variable inter arrival time (from 50 s to 200 s) while varying the number of neighbour nodes. We consider a polling interval T_p equal to 62 s, because the data is sampled every minute. Therefore, there is no need to scan for data during a time interval lower than the 62 s. Setting the polling interval to value mentioned will decrease significantly the energy consumption of a node using the SCP MAC protocol, because of the low duty cycle that it will follow. We define that all synchronization information can be included in the data packet when $r_{data} = r_{sync}$.

By observing Figure 6.5, with an ideal battery, the expected lifetime is decreasing as the number of neighbouring nodes increases, as expected. Since this is an ideal battery, the discharge process removes the same power from the battery both at higher or lower rate of discharge. When comparing the upper graphic with the lower one that models the lifetime by the Peukert's equation with $n_{peuk}=1.2$, it is observed that the node will last three times more than using

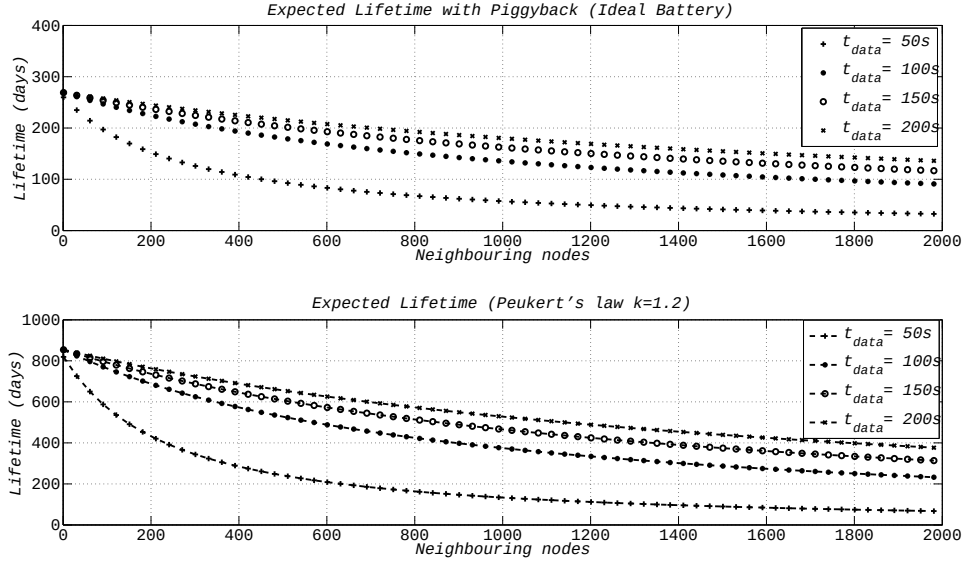


Figure 6.5: Expected lifetime with piggyback (higher bound), while considering $CW_1^{max} = 8$ and $CW_2^{max} = 16$ for different inter arrival periods, with $n_{peuk} = 1.2$.

the ideal battery model. As the inter arrival time decreases the expected lifetime decreases, because of the low inter arrival time that causes the node to wake-up more times to send or receive data packets than with a higher inter arrival time where the node will wake-up fewer times to send or receive the data packets.

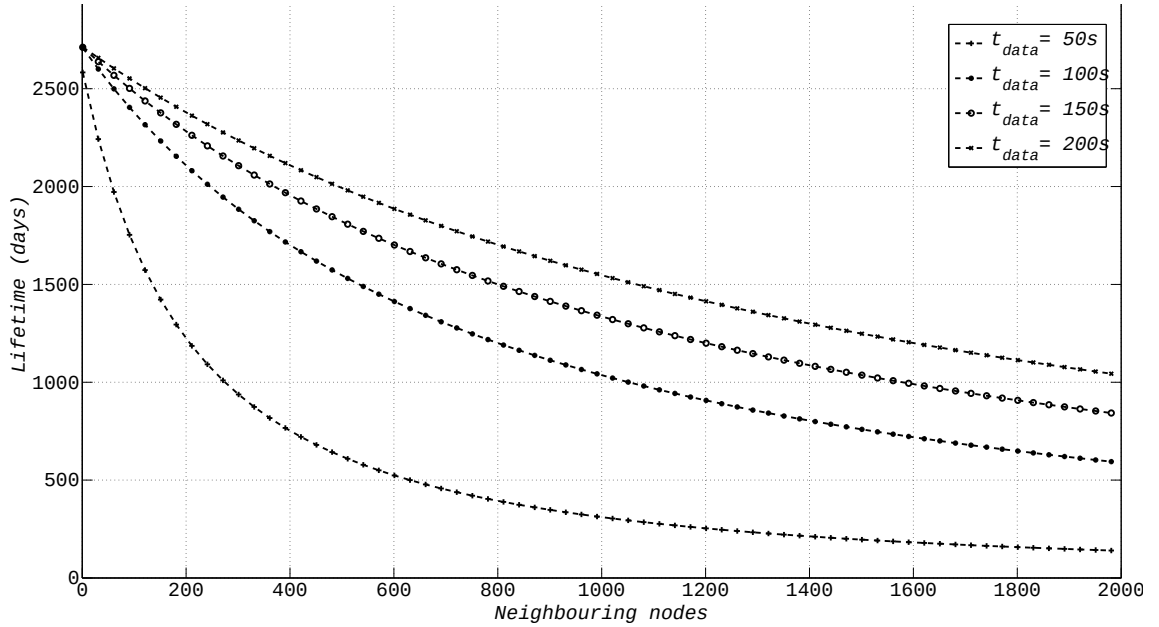


Figure 6.6: Expected lifetime with piggyback (higher bound), while considering $CW_1^{max} = 8$ and $CW_2^{max} = 16$ for different inter arrival periods, with $n_{peuk} = 1.4$.

Comparing Figures 6.5 and 6.6, with the increase of the Peukert's exponent until it reaches the maximum value there is an increase of the expected lifetime.

The battery "dies" when it reaches a minimum voltage which does not allows to the radio transceiver (or other sensor node components) to work properly. We define that the critical component in our sensor node is the radio transceiver, because it needs a minimum voltage

supply of 1.8 V. Although the radio transceiver stops working properly below 1.8 V, the micro-controller could continue to work. However, the communication capability from the sensor node will be turned off from the sensor node. To observe how the battery voltage drops, until it reaches the critical zone, we choose a fixed number of neighbour nodes, while varying the inter arrival time, the maximum size of the contention windows, and incrementing the time until it reaches the critical zone.

We consider the following equation for the battery voltage dropping model:

$$V_{drop} = V_{cc} - \frac{P_{node}}{\left(\frac{R(\frac{C_{batt}}{R})^{n_{peuk}}}{T} \right)^{1/n_{peuk}}} \quad (6.18)$$

where P_{node} is the power consumed with a fixed number of neighbouring nodes, a fixed maximum size for the contention windows, and a fixed inter arrival time.

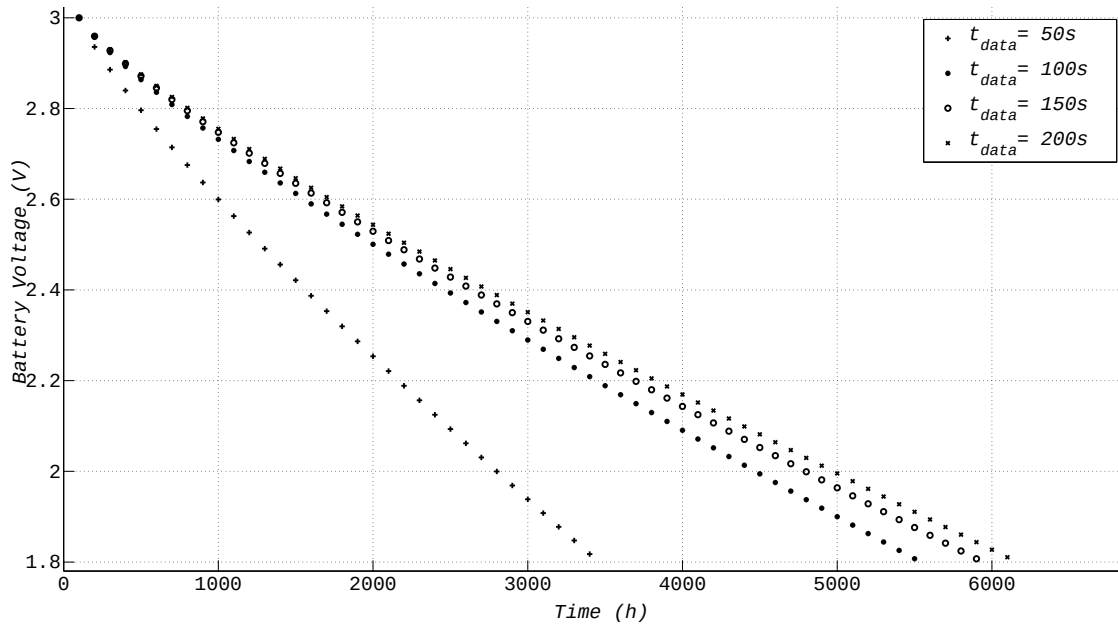


Figure 6.7: Battery voltage discharge, while considering $CW_1^{max} = 8$ and $CW_2^{max} = 16$ for different inter arrival periods, with $n_{peuk} = 1.2$ and $n = 211$.

By observing Figure 6.7, the battery voltage decreases faster when the inter arrival time is the shortest, and decreases slower when the inter arrival time is the largest. Therefore, the node that sends or receives data every 50 s will reach the critical zone after ≈ 3500 h. In turn, a node that receives data every 200 s will reach the same region after ≈ 6200 h.

By changing the number of neighbouring nodes to 91, one expects to increase the lifetime of the node. By observing Figure 6.8 and comparing it with Figure 6.7, we conclude that the node will reach the critical region only after ≈ 4800 h when considering an inter arrival time equal to 50 s (an increase in lifetime of ≈ 1300 h). If the inter arrival time is equal to 200 s, the node will reach the same region after ≈ 6500 h (a lifetime increase of ≈ 300 h). Another parameter that could lead to changes in the battery voltage drop, and consequently on the expected lifetime, is the maximum size of the contention windows.

For the **first experiment**, we have set the $CW_1^{max} = CW_2^{max} = 208$, and have defined the number of neighbouring nodes equal to 211 nodes. When comparing this experiment with the one that employs the same number of neighbouring nodes ($n = 211$), but different maximum

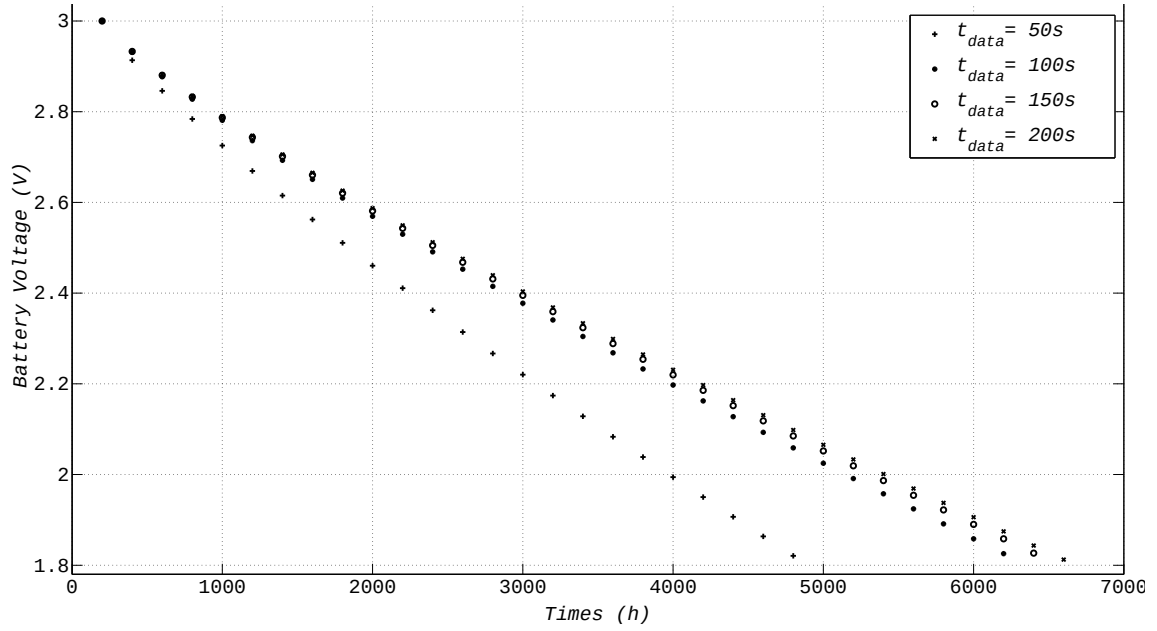


Figure 6.8: Battery voltage discharge, while considering $CW_1^{max} = 8$ and $CW_2^{max} = 16$ for different inter arrival periods, with $n_{peuk} = 1.2$ and $n = 91$.

contention windows sizes, a lower lifetime is obtained for the node, because of the increase of the maximum contention time.

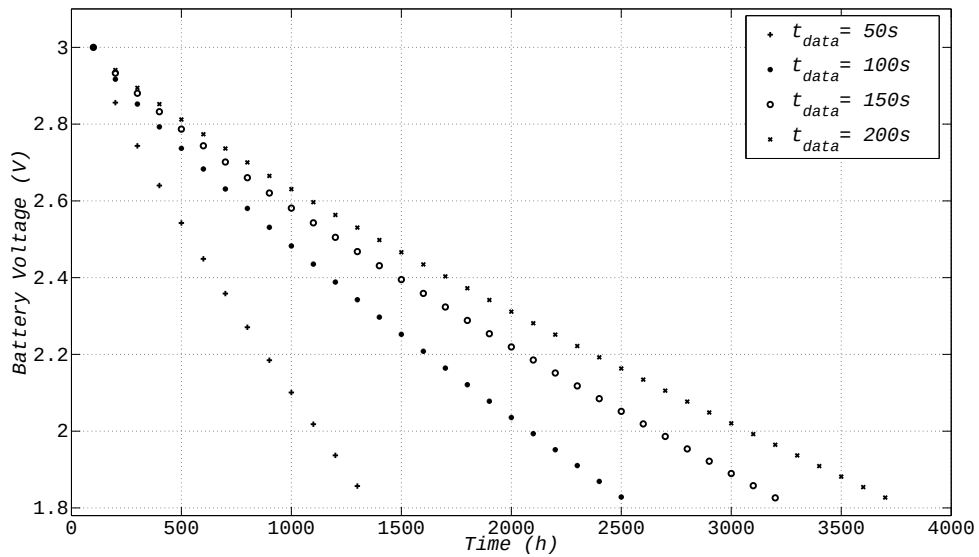


Figure 6.9: Battery voltage discharge, while considering $CW_1^{max} = CW_2^{max} = 208$ for different inter arrival periods, with $n_{peuk} = 1.2$ and $n = 211$.

By observing Figure 6.9, we can conclude that the node that employs a larger maximum contention windows size presents a lower lifetime. When the inter arrival time is equal to 50 s, the node is expected to last ≈ 1300 h. For an inter arrival time equal to 200 s, the node is expected to last ≈ 3700 h.

For the **second experiment**, the 208 slots were maintained in each contention window, and the number of neighbouring nodes was defined to be 91 nodes. When comparing this experiment with the one that employs the same number of neighbouring nodes ($n = 91$), but with different

maximum contention windows sizes it is expected to obtain a lower lifetime of the node, because the increase of the maximum contention time, even if the number of neighbouring nodes decrease.

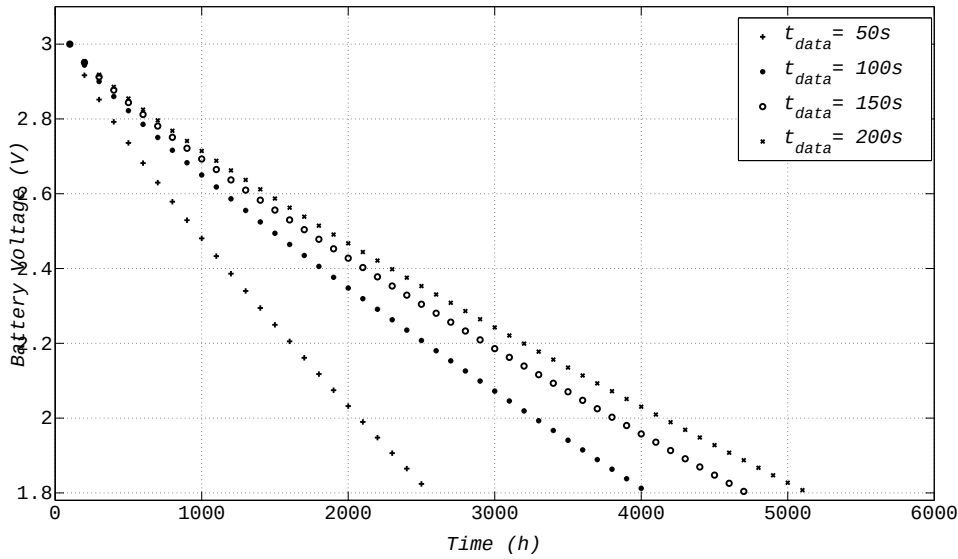


Figure 6.10: Battery voltage discharge, while considering $CW_1^{max} = CW_2^{max} = 208$ for different inter arrival periods, with $n_{peuk} = 1.2$ and $n = 91$.

By observing Figure 6.10, we conclude that the sensor node reaches the critical zone quicker for an inter arrival time equal to 50 s (than when considering the same inter arrival time but with a smaller maximum contention windows sizes). For an inter arrival time equal to 200 s the node will reach the critical zone $\approx 20\%$ faster when considering the 208 slots in each contention window.

6.4 Performance Analysis of a Two-Phase Contention Scheme for Scheduled Channel Polling

6.4.1 Motivation for Using Two Contention Windows

As presented in Section 5.2, the two-phase contention scheme for scheduled channel polling (SCP) considers two contention windows, CW_1 and CW_2 , divided into CW_1^{max} or CW_2^{max} time slots of equal duration. The choice of the slot to be used in the CW_1 and CW_2 follows a uniform distribution, as already mentioned in the aforementioned section. With two contention stages (CW_1 and CW_2) the collision probability decreases relatively to the case when a single contention window with equivalent size (sum of the sizes of CW_1 and CW_2) is adopted. Only the nodes succeeding in CW_1 enter CW_2 . This procedure causes a decrease in the number of nodes effectively accessing the medium after the second contention stage. After the first phase of the contention procedure, only the successful nodes from CW_1 (the first one(s) that transmit the wake-up tone) contend in CW_2 . With fewer contending nodes, the effective collision probability is drastically reduced. The motivation that drives us is that to the best of our knowledge, no work has addressed the analytical formulation for the collision probability in a two-phase contention window mechanism, which is characterized here for the collision avoidance mechanism

employed by the SCP-MAC protocol [YSH06].

6.4.2 Overview for the Saturated Regime

Usually, the performance analysis of wireless communication protocols is done in the saturated regime, since it significantly simplifies the analysis. In this case, the analysis is easier than in the unsaturated regime, in which the number of contending nodes is varying in time, depending on the packet arrival time instant at the application layer and the packet service time. Performing contention under saturated traffic conditions implies that nodes always have at least one data packet to be transmitted. An example of an application with saturated traffic conditions is a WSN with a high frequency event-based data dissemination scheme [YBO09]. This type of application is characterized by a set of nodes that simultaneously detect a high frequency phenomenon, which may drive the network to saturated traffic conditions for a given period of time. We analyze the impact of the two-phase contention window mechanism on the collision probabilities for different values of the size of the contention windows, CW_k^{max} , with $k \in \{1, 2\}$. This analysis is performed as a function of the number of contending nodes. In the remainder of this work we consider that the transmission period includes the first and second contention periods, although a frame transmission can be postponed to future transmission periods due to the need of retransmissions. This is mainly because the probability of collision is defined for a single transmission period, and retransmissions can be viewed as new transmissions originated by previous collisions.

For the saturated regime, the following assumptions are considered:

1. The sensor nodes only remove a data packet from the queue after gaining access to the medium and transmitting it;
2. Each transmitting node adopts the contention values within the interval $[1, CW_1^{max}]$ and $[1, CW_2^{max}]$, depending on the CW (CW_1 or CW_2 , respectively);
3. If there is only one node which succeeds to pass from CW_1 to CW_2 , the CW_2 collision probability is zero;
4. All the nodes have the same traffic load.

6.4.3 Overview for the Unsaturated Regime

The focus of the above description is the saturated regime, where every node in the network always has a packet ready for transmission. This means that the number of nodes contending for the channel is always the total number of nodes present in the network, n . However, from the application point of view, the saturated regime is unlikely to be realistic in real world applications, due to queue overflow and infinite queueing time [BGdMT06]. Hence, we also consider the unsaturated traffic condition of the network, which is more realistic, in practice. In the unsaturated regime, nodes with an empty queue do not contend for the channel. Therefore, the average number of contending nodes varies between 1 and n , depending on the offered traffic load for each node. In the unsaturated regime we assume that the sensor nodes have one attempt to transmit each data packet. Otherwise, if the sensor node senses a busy channel, it discards the packet and waits for the next (generated) one.

For unsaturated traffic, we have tested CBR arrival traffic with a given inter-arrival time value, T_{tR} . The starting times for the CBR traffic are uniformly distributed over a certain percentage

of the average inter-arrival time period (i.e., the drift rate, θ), for different simulation rounds. After the first uniformly generated inter-arrival time, the remaining ones are generated periodically during each traffic generation inter-arrival time.

Moreover, since Scheduled Channel Polling involves synchronization, the polling period time, T_{poll} , needs to be defined (in this work it is set to 1 s), while the polling duration, T_p , is set to 2 ms. The sensor nodes wake-up each second in order to dispatch the packets, which can exist in the Tx queue, as quickly as possible. Since the nodes wake-up each second, the initial times are allocated uniformly over five possible time intervals (with duration of one second each), for $\theta = 0.1$. As the drift increases, the number of intervals also increases, while the probability of a node to generate packet(s) in one of the intervals decreases. The dependence of this probability decay on θ and T_{tR} is analyzed in detail in Section 6.4.5

6.4.4 Stochastic Collision Probability Model for the Saturated Regime

In the stochastic model for the collision probability, n is the number of nodes simultaneously competing for time slots in CW_1 , ($n > 0$) and m is the number of successful nodes in CW_1 that enter CW_2 , whilst simultaneously competing for the time slots in CW_2 , ($m > 0$). Considering CW_1^{max} and CW_2^{max} as the number of time slots in CW_1 and CW_2 , respectively, the respective n or m nodes choose their time slot from the following set:

$$\varphi_{slot}^{(CW_k)} = \{a_i, i = 1, \dots, CW_k^{max}\} \quad (6.19)$$

where a_i represents the slot and $k \in \{1, 2\}$.

The probability of success in CW_1 is the probability of a successful wake-up tone, i.e., it excludes the cases where two or more nodes choose the lowest order slot (although it still may lead to success in CW_2). Considering the slot selection events, A_i , which occur from the set of slots in CW_1 , the set of possible slots is given by:

$$S_{CW_1} = A_1 \cup \dots \cup A_{CW_1^{max}} \quad (6.20)$$

As the events are equiprobable, the probability of choosing a slot i , p_i , is given by:

$$p_i = \frac{1}{CW_1^{max}}, \forall i = 1, \dots, CW_1^{max} \quad (6.21)$$

Firstly, the probability that l nodes choose the slot i , is expressed by the binomial distribution of l nodes choosing the slot i , with probability p_i in a sequence of n nodes, and is denoted as

$$P(X_i = l) = \frac{n!}{l!(n-l)!} p_i^l (1-p_i)^{(n-l)}, \forall i = 1, \dots, CW_1^{max} \quad (6.22)$$

where X_i represents a random variable which corresponds to the number of nodes that choose the slot i (to start the transmission of the wake-up tone).

The probability that one slot i in CW_1 is chosen by more than u ($u \geq 0$) nodes is given by the sum of the probabilities of having $u + 1$ nodes choosing the slot i . The sum of the probabilities is therefore given by:

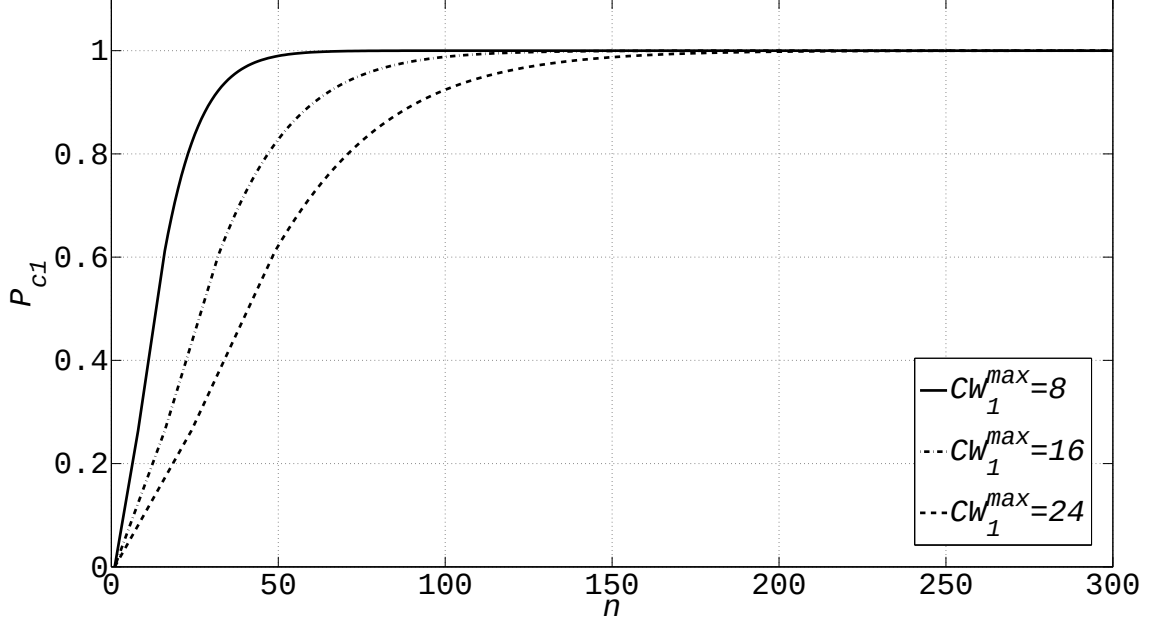


Figure 6.11: CW_1 collision probability as a function of n .

$$P(X_i > u) = \sum_{k=u+1}^n P(X_i = k), \forall i = 1, \dots, CW_1^{max} \quad (6.23)$$

Since a collision occurs when two or more nodes access the medium in the same slot, and because the nodes choose a given slot with the same probability, the probability of collision in the first contention period, CW_1 , is given by:

$$P_{c1} = P(X_i > 1) = \sum_{k=2}^n P(X_i = k), \forall i = 1, \dots, CW_1^{max} \quad (6.24)$$

Figure 6.11 represents the CW_1 collision probability (P_{c1}) as a function of the number of contending nodes, n , with CW_1^{max} as a parameter. A comparison between both traffic regimes is presented in section 6.4.5, where the differences are noticeable.

The expected number of contending nodes in CW_2 , $E[S]$, depends on the probability that the i -th lowest order slot in CW_1 is chosen by one or more nodes. At least one node successfully passes from CW_1 to CW_2 if $n \geq 1$. The expected number of contending nodes in CW_2 therefore includes the nodes that had chosen the lowest order slot in CW_1 (slot i) and is given by:

$$E[S] = \sum_{k=1}^n kP(X_i = k), \forall i = 1, \dots, CW_1^{max} \quad (6.25)$$

Figure 6.12 plots $E[S]$ for different numbers of contending nodes and sizes of contention window CW_1 . As the size of CW_1 increases, the expected number of nodes in CW_2 , $E[S]$, decreases. This behaviour is due to the higher dilution of the nodes by the contention slots. By enlarging CW_1 , for the same number of nodes, the expected number of nodes transmitting in each slot decreases, leading to fewer nodes that successfully pass from CW_1 to CW_2 .

By comparing Figure 6.11 and Figure 6.12, we conclude that the CW_1 collision probability increases as the number of contention nodes increase. Two distinct zones can be identified in

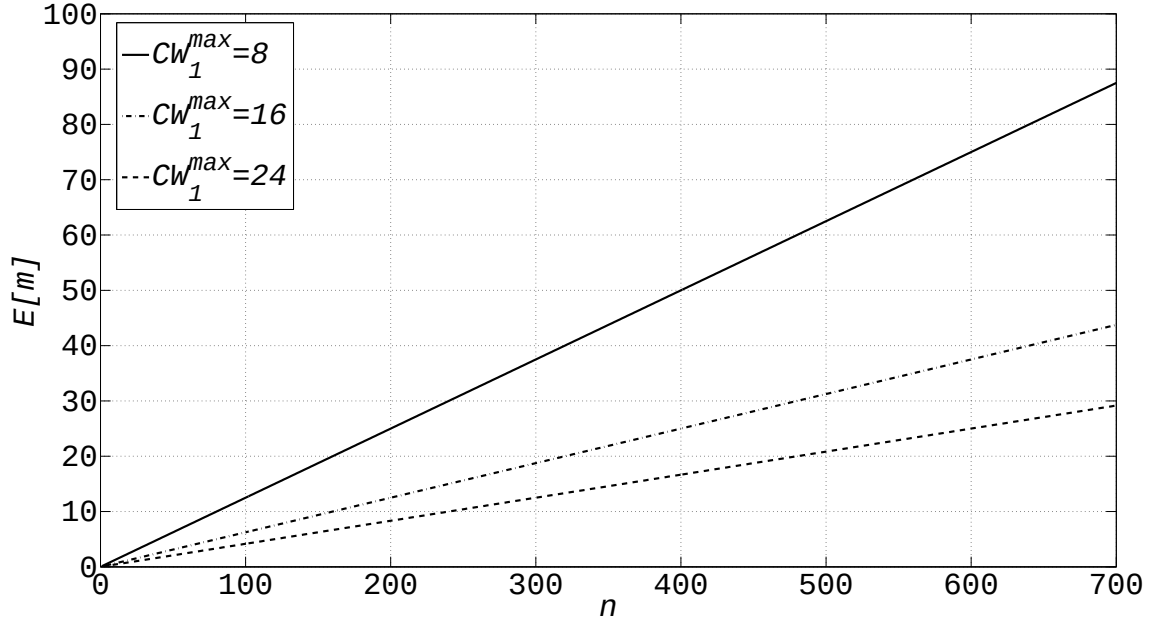


Figure 6.12: Expected number of nodes that successfully pass from CW_1 to CW_2 .

Figure 6.11:

- i) a rising zone where $0 \leq P_{c1} \leq 1 - \varepsilon, \forall n$;
- ii) a flat zone where $1 - \varepsilon < P_{c1} \leq 1, \forall n$.

The variable ε is such that the slope of the derivative of the collision probability curve from Figure 6.11 is close to zero in the flat zone. In the rising zone the expected number of nodes that pass from CW_1 to CW_2 is always smaller than the number of contending nodes. While in the flat one the CW_1 collision probability (P_{c1}) achieves the maximum collision ratio. From this point forward, as the number of contending nodes that compose the network increases, all nodes successfully pass to CW_2 .

In this work, the numerical solution of the collision probability for the second contention window is defined by two different approaches: (i) individual slot state analysis approach, or (ii) a combinatorics approach. The former is based on the combination of the different slots' probabilities, namely the probability of finding a slot idle, or the probabilities of finding a slot busy due to a collision and full transmission success. The latter can be described as a "bins and balls occupancy" problem [Fel68], which is going to be further developed in this section. Both approaches are presented in this paper, to show the available possibilities to define the model for the CW_2 collision probability.

To define the collision probability in the second contention (CW_2), we must consider the slot selection events (denoted as C_i) which occur from the set of slots in CW_2 , and are expressed by:

$$S_{CW_2} = C_1 \cup \dots \cup C_{CW_2^{max}} \quad (6.26)$$

As the events are equiprobable (as in CW_1), the probability that a node chooses a given slot i is the same for all nodes and is given by:

$$\tau = P(Y_i = l) = \frac{1}{CW_2^{max}}, \forall i = 1, \dots, CW_2^{max} \quad (6.27)$$

where Y_i represents a random variable which corresponds to the number of nodes that choose the slot i to start the transmission of the data packet. Assuming a network composed by n nodes, where $E[S]$ nodes successfully passed from CW_1 to CW_2 , the probability that one node finds the channel idle (when performing a carrier sense in the chosen slot), is related with all the $E[S]$ nodes that do not start transmitting in the same slot. Consequently, the probability of a slot being idle is given by:

$$P_{Sidle} = (1 - \tau)^{\lceil E[S] \rceil} \quad (6.28)$$

where the function $\lceil x \rceil$ denotes the ceiling function. We note that the effective data packet collision in CW_2 only happens if the nodes that successfully pass from CW_1 to CW_2 randomly choose the same time slot in CW_2 . This event corresponds to an effective data packet loss due to collision. Therefore, the successful slot probability in CW_2 depends on the number of nodes that choose a slot to transmit while the remaining $E[S] - 1$ nodes on its radio range do not start a transmission in the same time slot. Thus, the probability of occurring a successful transmission in a given slot of CW_2 is given by:

$$P_{Ssuc} = E[S] \tau (1 - \tau)^{\lceil E[S] - 1 \rceil} \quad (6.29)$$

By combining Equations 6.28 and 6.29, we are able to derive the probability of multiple accesses occurrences in the same slot (collision), which is expressed as follows:

$$P_{Scol} = 1 - P_{Sidle} - P_{Ssuc} \quad (6.30)$$

Finally, a collision can occur in any slot of CW_2 . It occurs in the first frame's slot with probability P_{Scol} . It only occurs in the second slot if the first slot is idle. This probability of collision for the second slot is an intersection of the events of occurring a collision in the second slot (with probability P_{Scol}) and the event of not having nodes accessing in the first slot (with probability P_{Sidle}). Consequently, applying the same rationale for the remaining slots, the probability of occurring a collision in the second window CW_2 is expressed by:

$$P_{cF} = \sum_{k=1}^{CW_2^{max}} P_{Scol} P_{Sidle}^{(k-1)} \quad (6.31)$$

Figure 6.13 plots the probability of a collision occurring in CW_2 . Given that a node broadcasts a packet, its success depends only on channel occupancy. Therefore, a collision occurs in CW_2 if more than one node choose the lowest order slot and transmit data packets simultaneously. Hence, the curves referred to the CW_2 collision probability are the numerical solutions for the P_{cF} expression.

P_{cF} increases as the number of contending nodes increases. As the contention window size increases, the maximum collision probability value is attained for higher number of contending nodes. Moreover, as the size of CW_2 increases (for the same number of contending nodes) the P_{cF} value sharply decreases. This is due to the two-phase contention window mechanism. Since the first contention window performs a first selection of nodes that pass to CW_2 (by means of contention), the second contention window handles fewer nodes. These nodes select a slot in CW_2 and try to transmit the data packet with success. In the flat zone, all the nodes that contend in CW_1 contend in CW_2 , causing the CW_2 collision probability to reach the maximum

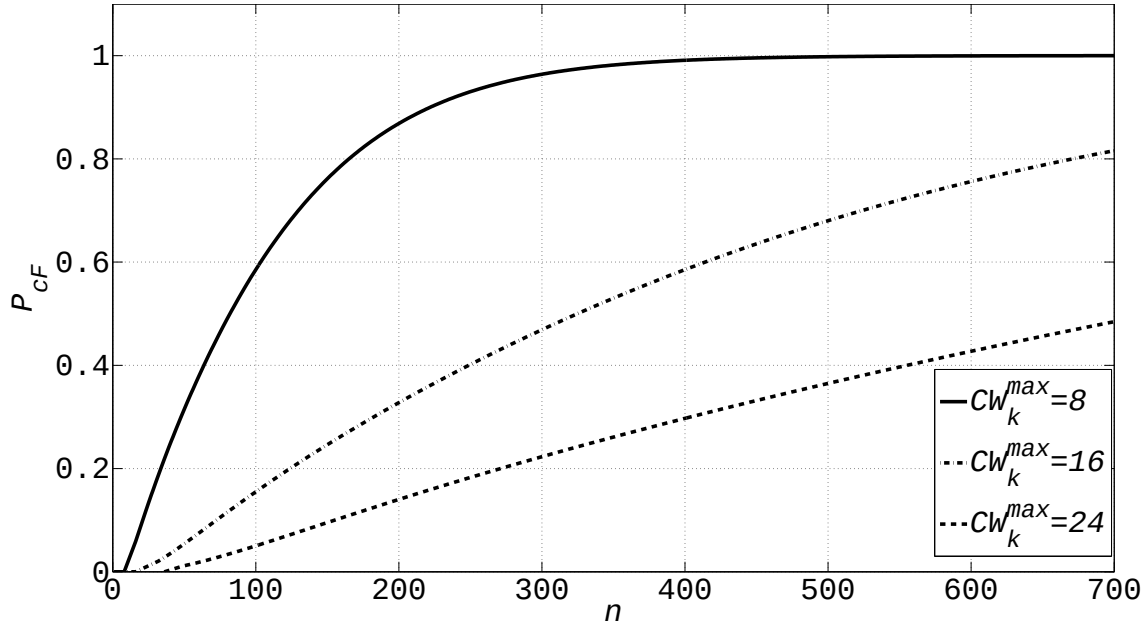


Figure 6.13: CW_2 collision probability under saturated regime considering a individual slot state analysis, $k \in \{1, 2\}$.

collision probability value ($P_{cF} = 1$). This occurs because the nodes have a higher probability of accessing the channel when packets are broadcast (as plotted in Figure 6.13), which originates more collisions.

If we consider the combinatorics approach, the collision probability for the second contention window is partially based on the birthday paradox [Fel68]. In the *birthday paradox*, bins are distinguishable and balls are indistinguishable. However, in our model bins and balls are both indistinguishable. This means that besides the amount of balls that are inside of the lowest order bin, the number of the ball also matters. For the sake of simplicity, we assume that each of the m balls represents a node, while each of the p bins is a CW_2 time slot. Hence, the envisaged success probability may be defined as the probability that the lowest order bin contains more than one ball and the remaining balls should be distributed for the remaining (highest order) bins. The remaining bins may contain more than one ball, and no ball should remain outside a bin. If the lowest order (first) bin does not contain any balls, then the next order bin is treated as the lowest order bin. The expected number of contending nodes in CW_2 is given by Equation 6.25. Although the expected values of contending nodes in CW_2 from Equation 6.25 may not be an integer value, for our combinatorics solution, all the involved variables should be treated as integer values. Hence, the following rounding function must be applied to it:

$$E[m] = \lfloor E[S] \rfloor \quad (6.32)$$

The $\lfloor x \rfloor$ function is used to round down to the nearest integer value of $E[m]$, to avoid possible overestimation of probability values that may lead to higher deviation errors. To begin with, the number of different arrangements in CW_2 (with and without collision) for the assignment of nodes by the time slots is obtained by arrangements with repetition. As any of the CW_2^{max} slots often occur repeatedly (so that it can be chosen several times) one must consider arrangements with repetition.

The total number of possibilities, given by Equation 6.33, assumes that any number of nodes

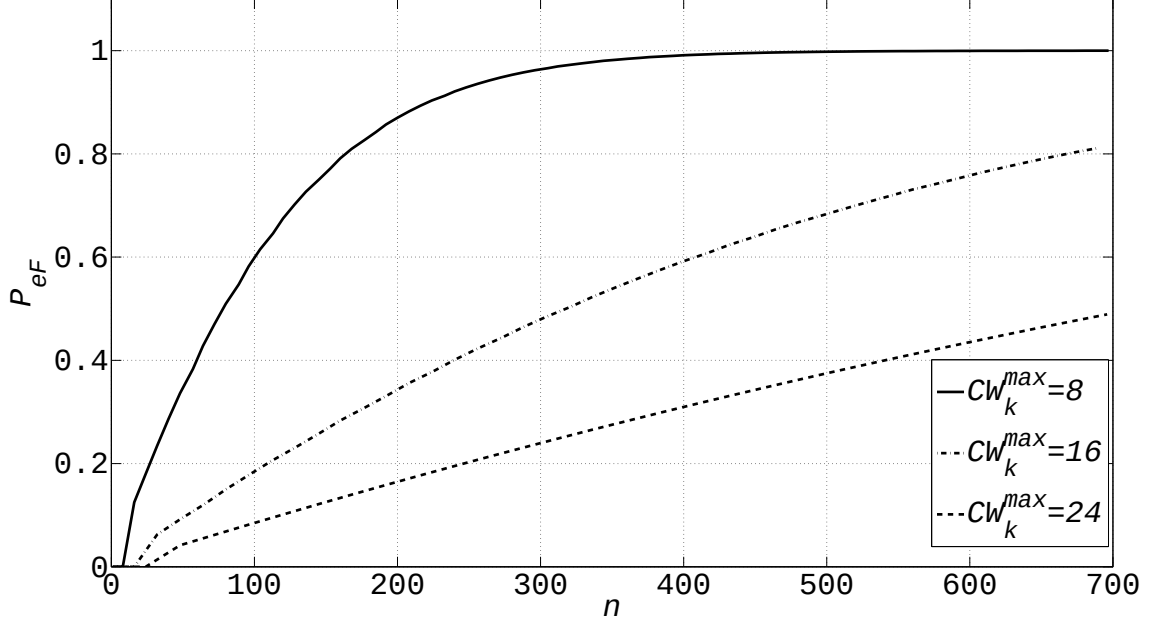


Figure 6.14: CW_2 collision probability considering saturated regime using a combinatorics approach, $k \in \{1, 2\}$.

can be put in a slot:

$$A_t(m) = (CW_2^{max})^{E[m]} \quad (6.33)$$

The number of possibilities that exactly one node chooses the i -th lowest order slot and the remaining ones choose the subsequent slots is also given by arrangements with repetition. If the lowest order slot is selected by only one node then the number of different possibilities is given by an arbitrary assignment of the $E[m] - 1$ remaining nodes to the $CW_2^{max} - r$ remaining slots. The variable r is the number of the lowest order slot that is selected by only one node and varies between 1 and CW_2^{max} . Therefore, the arrangements, A_s , corresponding to the choice of the lowest order slot by exactly one node is expressed by:

$$A_s(m) = E[m] \sum_{j=1}^{CW_2^{max}-1} (CW_2^{max} - j)^{(E[m]-1)} \quad (6.34)$$

In turn, the number of possibilities for the lowest order slot to be chosen by more than one node is given by:

$$A_f(m) = (CW_2^{max})^{E[m]} - E[m] \sum_{j=1}^{CW_2^{max}-1} (CW_2^{max} - j)^{(E[m]-1)} \quad (6.35)$$

The probability of a collision occurring in CW_2 results from the ratio between the number of possibilities for the lowest order slot to be chosen by more than one node, given by Equation 6.35, and the total number of possibilities to distribute n nodes by CW_2^{max} slots. given by Equation 6.33 As a consequence, the CW_2 collision probability, P_{eF} , is given by:

$$P_{eF}(m) = \frac{A_f(m)}{A_t(m)} \quad (6.36)$$

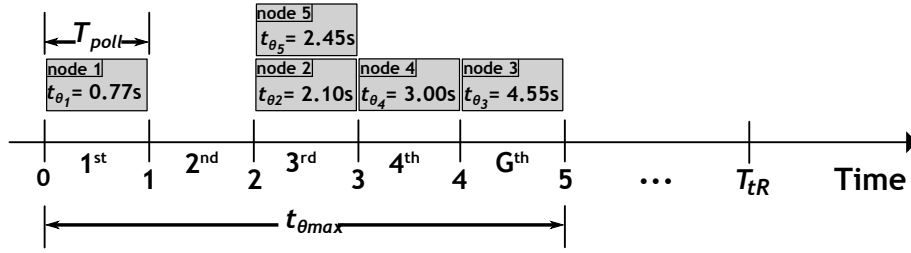


Figure 6.15: Uniform distribution example of nodes over the intervals.

Figure 6.14 shows the CW_2 collision probability as a function of the number of contending nodes, with the contention window size as a parameter. By comparing the curves obtained for the CW_2 collision probability between each approach (Figures 6.13 and 6.14), the values are similar with a Mean Absolute Error (MAE) close to 0.5 %. The main difference between the two approaches is the slope at the rising zone. For a number of contending nodes higher than the ones that correspond to the beginning of the CW_1 collision probability flat zone, the CW_2 collision probabilities are almost identical. These differences between the different approaches is due to the rounding function that is applied to the expected number of nodes that pass from CW_1 to CW_2 (to compute the numerical solution for the CW_2 collision probability according to the second approach).

6.4.5 Stochastic Collision Probability Model for the Unsaturated Regime

In the saturated regime, all sensor nodes have packets ready for transmission. As a consequence, the number of contending nodes with non-empty queues in the network is constant and known by all nodes. This fact is advantageous for the analysis of the collision probability under saturation conditions. In the latter case, the number of contending nodes varies continuously based on the packet arrival rates. Although the unsaturated regime is more complex to analyze, for the sake of simplicity, we only analyze uniformly distributed generation arrival times. The generation of unsaturated traffic at node n_i , $i \in 0, \dots, n$, is modelled by a uniformly distributed packet generation probability, P_{u_G} . The node n_i uniformly chooses the initial instant value for the first data packet generation, t_{θ_i} . The maximum drift rate, θ , varies between 0 and 1 ($\theta \in [0; 1]$). The packet generation initial instant value (given in seconds), t_{θ_i} , follows a uniform distribution, that is repeated at each inter-arrival time, as given by:

$$t_{\theta_i} \in [0; t_{\theta_{max}}], \forall i = 1, \dots, n \quad (6.37)$$

where $t_{\theta_{max}}$ is the maximum time of the interval when the packet generation times are chosen (in the experiments we considered $\theta_{max} = 5$ s). $t_{\theta_{max}}$ depends on the values chosen for the θ and T_{tR} parameters and is given by $t_{\theta_{max}} = \theta \cdot T_{tR}$. Since the nodes wake-up every second ($T_{poll} = 1$ s), the drift rate reflects the number of intervals the inter-arrival period is divided in. Figure 6.15 depicts how the time frame is subdivided into a uniform number of time intervals (of one second duration each). Figure 6.15 also presents, an example of how the nodes are distributed among the generation intervals, depending on the chosen packet generation time, t_{θ_i} .

The interval order, G , is expressed as $G \in [1; \Pi_{max}]$, where Π_{max} is the highest interval order, given by the combination of values of θ , T_{tR} , and polling period time, T_{poll} , parameters. Hence, $\Pi_{max} = \left\lfloor \frac{t_{\theta_{max}}}{T_{poll}} \right\rfloor$. In Figure 6.15, we assume $\theta = 0.1$, $T_{tR} = 50$ s, and $T_{poll} = 1$ s, which, in turn,

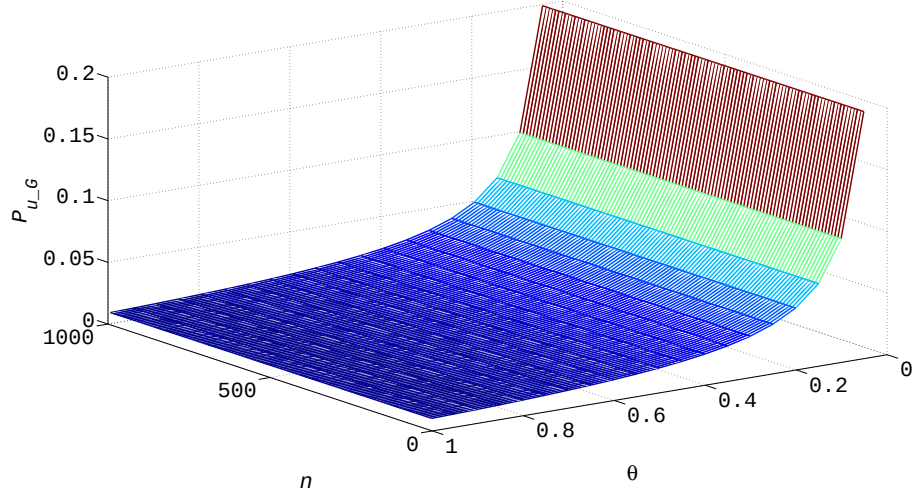


Figure 6.16: Probability of a node to choose one of the G possible intervals as a function of θ and n , for $T_{tR} = 50$ s.

leads to $\Pi_{max} = 5$ (by dividing $t_{\theta_{max}}$ by T_{poll}).

From the uniform distribution, the probability of a given node to choose one of the G intervals is expressed by:

$$P_{u_G} = \frac{T_{poll}}{t_{\theta_{max}}}, G \in [1; \Pi_{max}] \quad (6.38)$$

Figure 6.16 shows the probability of a node to choose one of the G possible intervals as a function of the drift rate per node, θ , and of the network size n , for $T_{tR} = 50$ s. The surface shows two distinct generating probability zones. For values of θ higher or equal to 0.2, the generating probability decreases as θ increases. Hence, the probability P_{u_G} is independent of the number of contending nodes for a given value of inter-arrival time, T_{tR} . When the drift rate decreases ($\theta < 0.2$), P_{u_G} sharply increases. This sharp increase occurs because of the reduced number of possible intervals that leads to a higher probability of a node to fall into an interval.

Considering the unsaturated regime and a deployment of n nodes in a given area, the expected number of nodes starting a data packet generation in the interval G , $\hat{E}[n]$, is represented by:

$$\hat{E}[n] = \lceil P_{u_G} \cdot n \rceil, G \in [1; \Pi_{max}] \quad (6.39)$$

$\hat{E}[n]$ is given by the ceiling integer value, since the expected number of nodes should not be decimal. Figure 6.17 shows the respective expected number of nodes that choose one of the G possible intervals, $\hat{E}[n]$. Unlike Figure 6.16, in Figure 6.17, $\hat{E}[n]$ is not independent from the number of contending nodes. Since the generating probability varies only when θ increases or decreases, for a pre-set θ value, $\hat{E}[n]$ increases as the number of possible generating nodes (n) increases. This proportional behaviour is depicted in the surface presented in Figure 6.17, where two distinct zones are identified. The first one ($\theta \geq 0.2$) presents an expected number of contending nodes varying between 0 and 25 nodes. The smallest $\hat{E}[n]$ values match with the highest values of θ . The second one ($\theta < 0.2$) corresponds to the highest values of $\hat{E}[n]$, where the $\hat{E}[n]$ varies between 0 and 200 nodes. The highest values of $\hat{E}[n]$ correspond to the reduced number of possible intervals that a node may choose to start the packet generation.

For the unsaturated regime, Equation 6.24 is rewritten as follows:

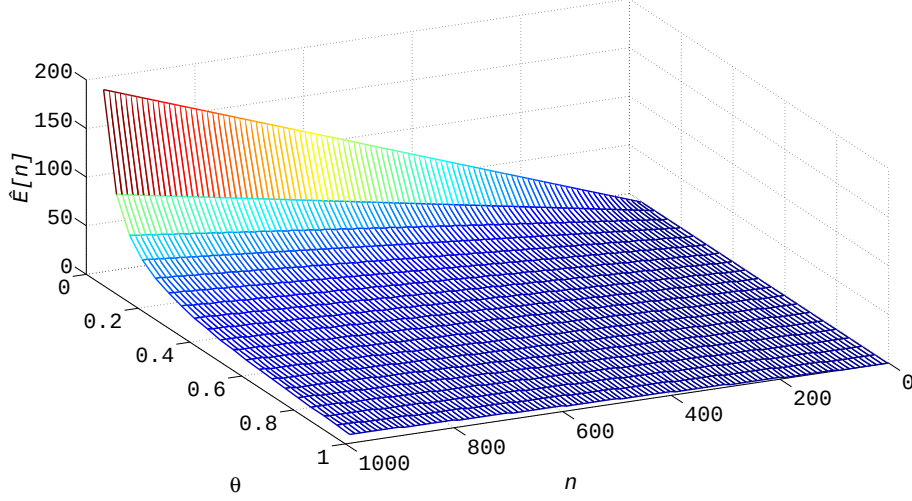


Figure 6.17: Expected number of nodes to choose one of the G possible intervals as a function of θ and n , for $T_{tR} = 50$ s.

$$\widehat{P}_{c1} = \sum_{k=2}^{\widehat{E}[n]} \binom{\widehat{E}[n]}{k} p_i^k (1-p_i)^{(\widehat{E}[n]-k)}, \quad \forall i = 1, \dots, CW_1^{max} \quad (6.40)$$

which defines the probability that at least two nodes choose the same time slot in CW_1 , for the expected number of nodes that choose one of the G possible intervals ($\widehat{E}[n]$).

Moreover, for the unsaturated case, Equation 6.25 is rewritten as follows:

$$\widehat{E}[S] = \sum_{k=1}^{\widehat{E}[n]} k \binom{\widehat{E}[n]}{k} p_i^k (1-p_i)^{(\widehat{E}[n]-k)}, \quad \forall i = 1, \dots, CW_1^{max} \quad (6.41)$$

where $\widehat{E}[S]$ is the expected number of contending nodes in CW_2 under the unsaturated regime. As in the saturated case, two distinct zones can be identified in Figure 6.18:

- i) a rising zone where $0 \leq \widehat{P}_{c1} \leq 1 - \varepsilon, \forall n$;
- ii) a flat zone where $1 - \varepsilon < \widehat{P}_{c1} \leq 1, \forall n$.

For the rising and flat zones the variable ε is characterized in the same way as in the saturated regime. Therefore, by following the first approach to obtain the collision probability in CW_2 (individual slot state), $E[S]$ in Equations 6.28, 6.29 and 6.30 is now equivalent to $\widehat{E}[S]$. Besides, if the second approach (combinatorics) is considered in Equations 6.33, 6.34 and 6.35, $E[m]$ is now equivalent to $\widehat{E}[m]$. Finally, the collision probability in CW_2 is obtained by the first approach (see Equation 6.31) under the unsaturated regime, and is represented by $\widehat{P}_{cF}$ as follows:

$$\widehat{P}_{cF} = \sum_{k=1}^{CW_2^{max}} \widehat{P}_{Scol} \widehat{P}_{Sidle}^{(k-1)} \quad (6.42)$$

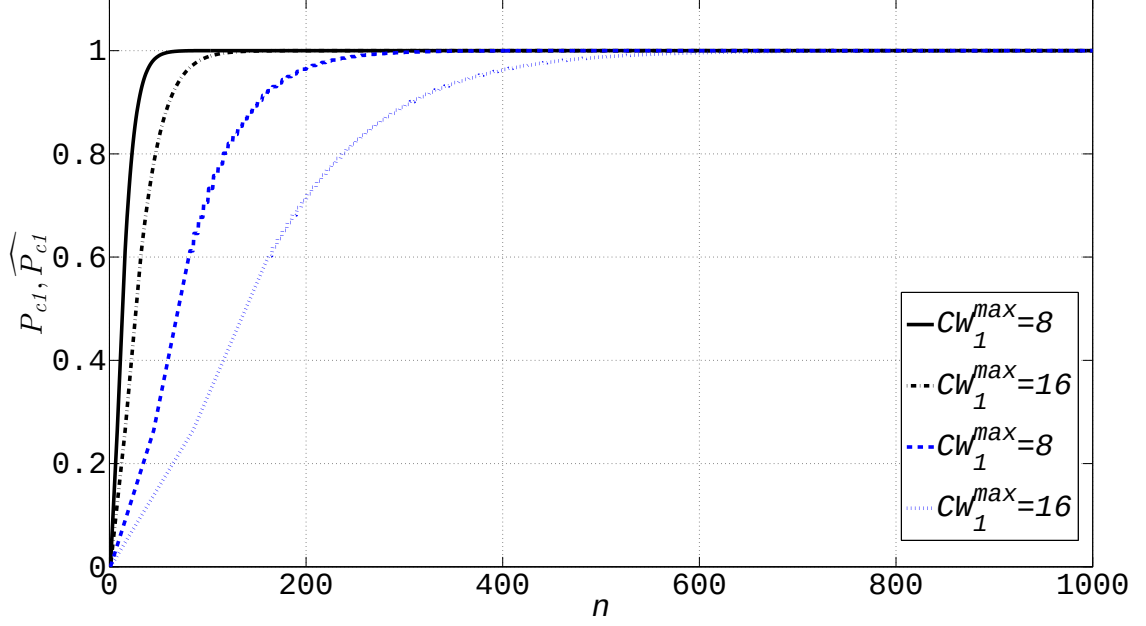


Figure 6.18: CW_1 collision probability for the saturated (black solid and dash-dot lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n , for $\theta = 0.1$.

For the combinatorics approach the CW_2 collision probability under the unsaturated regime, given by Equation 6.36, is expressed by

$$\widehat{P_{eF}}(m) = \frac{\widehat{A_f}(m)}{\widehat{A_t}(m)} \quad (6.43)$$

Figure 6.18 shows the characterization of the collision probability in CW_1 , for different number of contending nodes, n , and for different CW_1^{max} values. The saturated and unsaturated regimes have been considered. The purpose of this analysis is to verify the validity of the model for different number of contending nodes, contention window sizes and levels of traffic load (saturated and unsaturated). In both regimes, one can observe that, for a given value of CW_1^{max} , the collision probability increases as the number of contending nodes increases, i.e., the ratio of non-interfering time slots per node decreases. Moreover, as the contention window size increases, the collision probability decreases, as expected.

However, for the unsaturated case, the CW_1 collision probability does not increase as fast as for the saturated one. The P_{u_G} values for the unsaturated case explains why the CW_1 collision probability reaches a value of 1 for a higher number of possible contending nodes.

Figure 6.19 presents the variation of the expected number of successful nodes that pass from CW_1 to CW_2 as a function of n . Both the saturated and unsaturated regimes are considered. By comparing these results with the ones in the saturated conditions, we conclude that the number of successful nodes in CW_1 increases, in saturated regime.

For different contention windows sizes, the expected number of successful nodes in CW_1 , $E[m]$ for the saturated regime and $\widehat{E}[m]$ for the unsaturated one, increases linearly. By comparing both traffic regimes with respect to the contention window size, the expected number of successful nodes that pass to CW_2 , $\widehat{E}[S]$, is lower in the unsaturated case. This is due to the low number of nodes that will choose one of the G -th intervals and contend for the channel.

Figure 6.20 shows the variation for the CW_2 collision probability with n (which, in turn, is related with the number of contending nodes in the CW_1 that succeed into reaching the CW_2) for the saturated and unsaturated regimes. The results are presented for different values of

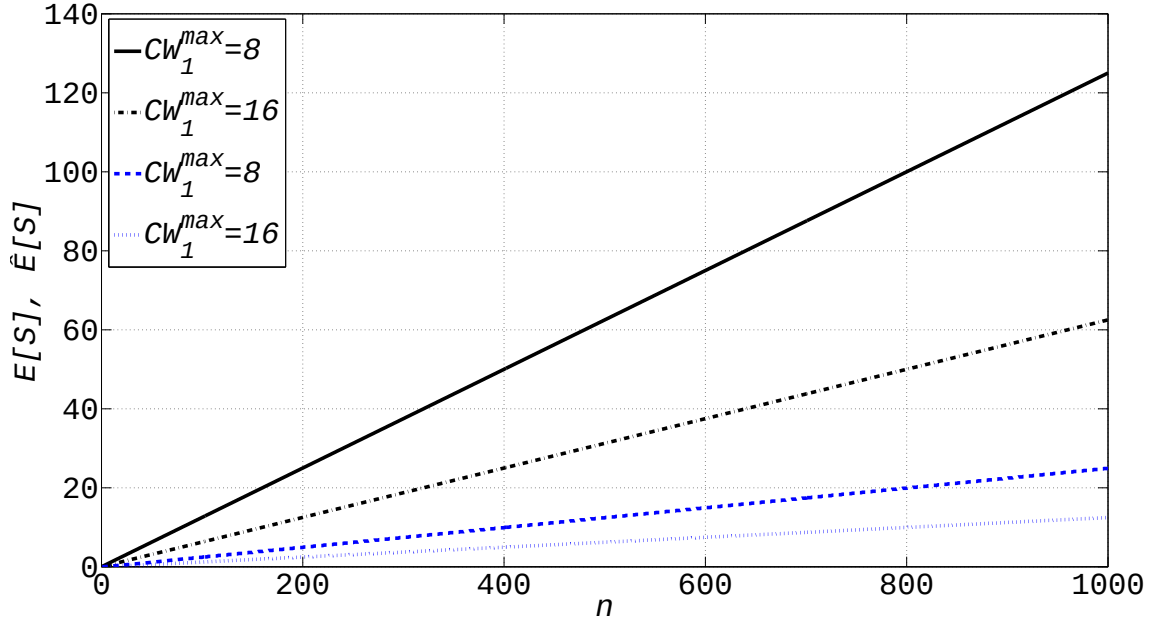


Figure 6.19: Expected number of successful nodes from CW_1 to CW_2 for the saturated (black solid and dash-dot lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n , for $\theta = 0.1$.

the contention window sizes, CW_1^{max} and CW_2^{max} .

When only one successful node enters into CW_2 the collision event never happens. Moreover, since $\hat{E}[S]$ is lower in the unsaturated case. Then, the CW_2 collision probability in the latter regime is always lower than in the saturated regime, as shown in Figure 6.20.

6.4.6 Simulation Scenario

In this section, we evaluate the impact of the number of contending nodes on the packet collision of the two-phase contention window mechanism, using both analytical and simulation approaches, under saturated traffic conditions. We evaluate the proposed model through OMNeT++ [Var10] simulations. The Mobility Framework from [REHD08] is used with our SCP protocol implementation, whilst considering different model parameters like n , CW_1^{max} and CW_2^{max} , as well as different values for the traffic generation rate, λ . In these simulations, we consider an ideal wireless channel, i.e., the network performance is not degraded by the physical layer impairments such as fast fading and shadowing, as free-space propagation mainly in line-of-sight is assumed. The ideal wireless channel assumption may be adequate to capture the general behaviour of the mechanism. The node topology represents a tight cluster of dense deployed wireless nodes, which is a worst-case situation in terms of collisions. We assume that the sensor nodes do not move (an example of node deployment is shown in Figure 6.21). The number of contending nodes is kept constant during the simulations, in order to properly evaluate the effective data packet collision. Nodes are deployed using a 2D Poisson process on a $300 \times 300 \text{ m}^2$ area (i.e., x and y coordinates are randomly and uniformly chosen within $[0, 300]$). All sensor nodes are simultaneously sink and sources (whilst sending broadcast packets). Since broadcast packet transmission is performed by plain carrier sensing with duration of a time slot (in both contention windows), this setup is prone to the “hidden terminal” problem. To avoid this problem, we assure that all nodes can sense each other. To give a more realistic behaviour to our simulations, the accumulative SNIR interference model [KSEG⁺08] is considered. With this interference model, the SNIR of the given signals is recalculated each

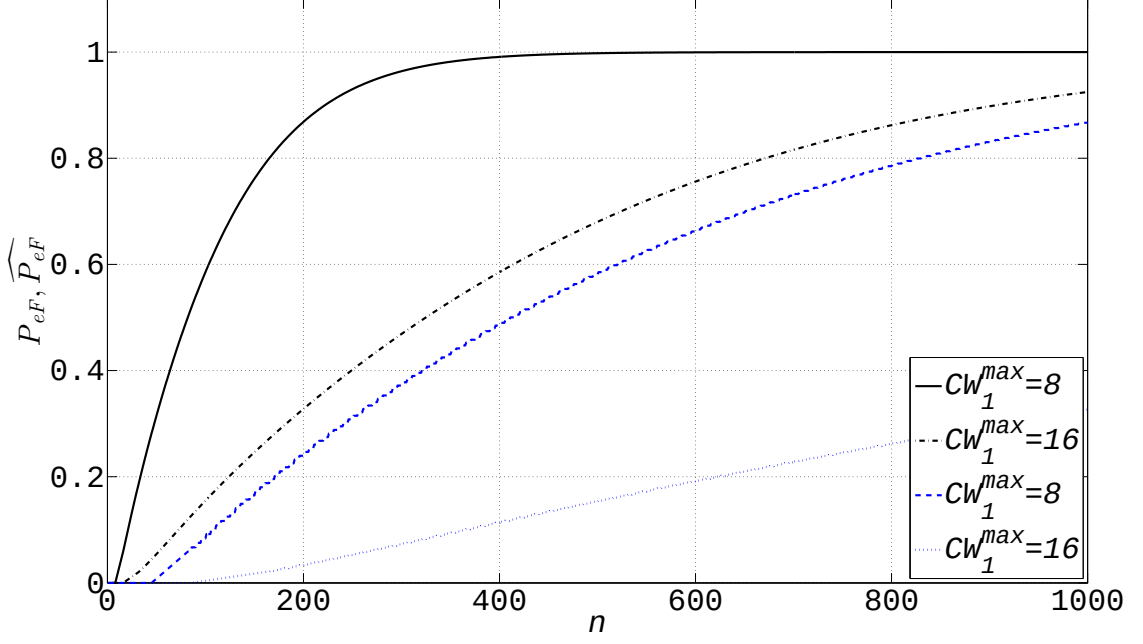


Figure 6.20: CW_2 collision probability for the saturated (black lines) and unsaturated (blue dashed and dotted lines) regimes as a function of n for $\theta = 0.1$, $k \in \{1, 2\}$.

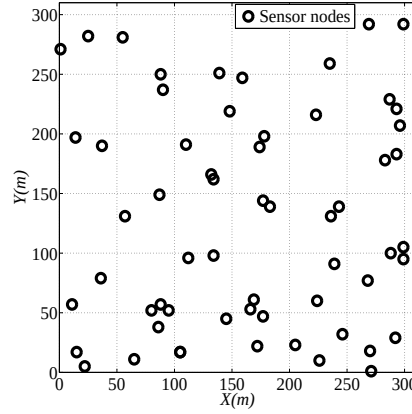


Figure 6.21: Homogeneous uniform WSN deployment simulation.

time the receiver predicts the change in the interference power. This model is frequently used in wireless communication simulations and is included in the Mobility Framework [REHD08]. For each deployment with n contending nodes, a set of 6 seeds (corresponding to 300 simulation rounds for each seed) is chosen for the random number generator used by SCP (which has six degrees of freedom). In our set of SCP simulations, we consider the Texas Instruments CC1100 low-power radio transceiver, available in the Mobility Framework [REHD08], with a transmission rate of 250 kbps. Packets are periodically generated at the application layer with a certain packet time interval parameter (50 or 100 s). System parameters are listed in Table 6.2.

6.4.7 χ^2 Test in the unsaturated traffic regime

The Pearson's chi-square test (χ^2) is used to assess the goodness-of-fit which allows to infer whether an observed distribution differs or not from the theoretical one. We have applied the Pearson chi-square test to the simulation results obtained for the unsaturated regime. The

Table 6.2: Simulation parameters.

Parameter	Value	Parameter	Value
TX/RX range	> 1 m	Packet length	50 bytes
Data rate	250 kbps	Slot time	32 μ s
Channel model	Free-space	CW_k^{max} , $k \in \{1, 2\}$	[8; 16]
Node number	2~440	Poll period	{1, 5} s
Node placement	Uniform	Number of packets	50

procedure is as follows: the sample space is divided into the union of G disjoint intervals. The probability that a data packet is generated in the G -th interval under the postulated distribution, p_i , $i = 1, \dots, G$, is calculated. The expected number of outcomes that fall in the G -th interval in n possible contending nodes of the network simulation is given by $e_i = n \cdot p_i$. The chi-square statistic is defined as the weighted difference between the observed number of generation times (f_i) in the G -th interval, and the expected theoretical frequency (e_i), given by:

$$Q^2 = \sum_{i=1}^G \frac{(f_i - e_i)^2}{e_i} \quad (6.44)$$

The hypothesis is rejected if $Q^2 \geq \chi^2$, where χ^2 is the critical point determined by a given level of significance. Otherwise, the fit is accepted. When expected frequencies are large, there is no problem with the assumption of normal distribution. However, the smaller the expected frequencies are, the less valid are the results of the chi-square test. Therefore, if the events show very low raw observed frequencies (five or below), the expected frequencies may also be too low for chi-square test to be appropriately used. To guarantee that the approximation to the chi-square is appropriate, the expected frequencies must not be too low. One must ensure that the following inequality is fulfilled [CL54]:

$$n \cdot p_i \geq 5, \quad i = 1, \dots, G \quad (6.45)$$

To validate the model for the collision probabilities in the unsaturated regime, it is fundamental to test if the times when the packets are generated can be modelled by a uniform distribution. We denote this hypothesis as H_0 . In the simulations, we consider $\theta = 0.1$, which implies $G = 5$ possible disjoint intervals. A level of significance $\alpha = 0.05$ is assumed to ensure that condition in Equation 6.45 is verified. The condition in Equation 6.45 establishes that in a network that defines 5 possible disjoint intervals for packet generation, with a uniform distribution, the network must have at least 5 nodes. This way, each of the 5 intervals corresponds theoretically to one node. In order to fulfil the latter condition, the given inequality is used to calculate the minimum number of n possible contending nodes. Hence, the probability that a data packet is generated in the G -th interval under the uniform distribution is obtained by dividing one packet by the maximum number of possible intervals, $p_i = 1/5 = 0.2$. Manipulating the inequality, we obtain $n \geq 25$ for the minimum number of contending nodes, which verifies the condition in Equation 6.45. Since we consider network sizes lower than 25 nodes in our simulations, we can not rely on the chi-square table to obtain the critical point in these cases. To obtain the critical point we have performed Monte Carlo simulations with the IBM SPSS software, whilst considering $\alpha = 0.05$, for $n = \{5, 10, 20\}$ nodes. From the Monte Carlo simulations we have

Table 6.3: Monte Carlo simulation results for different seeds, $n = 10$.

f_i	27377	56190	63086	39755	53720	21803
1	3	2	3	2	4	4
2	4	2	2	3	3	2
3	1	3	2	2	1	2
4	1	2	2	2	1	1
5	1	1	1	1	1	1
χ^2	0.4	1	1	1	4	3
Φ	0.527	0.910	0.910	0.910	0.406	0.558
Ω	0.75	0.989	0.989	0.987	0.476	0.683

concluded that, for $n < 10$ nodes, it is not possible to adopt the χ^2 test. Table 6.3 shows the results for different seeds and $n = 10$ nodes. By analysing the Monte Carlo simulation results from Table 6.3 the hypothesis is accepted if the asymptotic significance value (Φ) is less than or equal to Monte Carlo significance level (Ω). Otherwise, H_0 is rejected.

For network sizes $n > 25$, the chi-square test was carried out to determine the goodness-of-fit between the H_0 and the simulation results. Since we consider $G = 5$, in our simulations, the critical point for $G - 1 = 4$ degrees of freedom (with a 5 % of significance level) is given by $\chi^2(\alpha = 0.05, V = 4) = 9.4877$. For $n > 25$, the goodness-of-fit of H_0 to the simulations results is guaranteed for all the seeds. For example, for a seed with a corresponding network size equal to $n = 30$ we have obtained $Q^2 = 6.6667$, which is well within the critical point, $Q^2 < \chi^2(\alpha = 0.05, V = 4)$. Hence, we conclude that the simulation results are in good agreement with Equation 6.42.

6.4.8 Discussion of the Results

In this section, the CW_1 and CW_2 collision probabilities are obtained as a function of the number of nodes, whilst considering the contention window size as a parameter.

Six different random simulations are considered and the 95 % confidence intervals are represented. Figures 6.22 and 6.23 show the validation results for the expected number of nodes that pass from CW_1 to CW_2 . Both traffic load regimes (saturated and unsaturated) are considered for two different contention window sizes, $CW_1^{max} = CW_2^{max} = \{8, 16\}$. The difference between the modelling and the simulation results “is insignificant” for all the range of n , which validates the model (for the expected number of nodes that pass to CW_2). Despite a smaller model accuracy for smaller number of nodes, as n increases, the curve for the simulation results converges to the curve plotted for the numerical solution of the expected number of nodes that pass from CW_1 to CW_2 .

Figures 6.24 and 6.25 present the verification of the validity of the CW_1 collision probability, under the saturated and unsaturated traffic regimes. The difference between the simulation and modelling results is less noticeable for the saturated regime than for the unsaturated one. Nevertheless, as the number of contending nodes, n , increases the simulation curves converge to the model curves, which allows for verifying our model for the CW_1 collision probability. This initial deviation between the model and simulation results was already previously mentioned. We verify that, in all the cases presented in Figures 6.24 and 6.25, the collision probability increases with the increase of the number of contending nodes. Collisions become more frequent as the number of competing nodes increases. The results obtained for the CW_1 collision probability are consistent by the ones from [vHH09], which presents a similar analysis for the

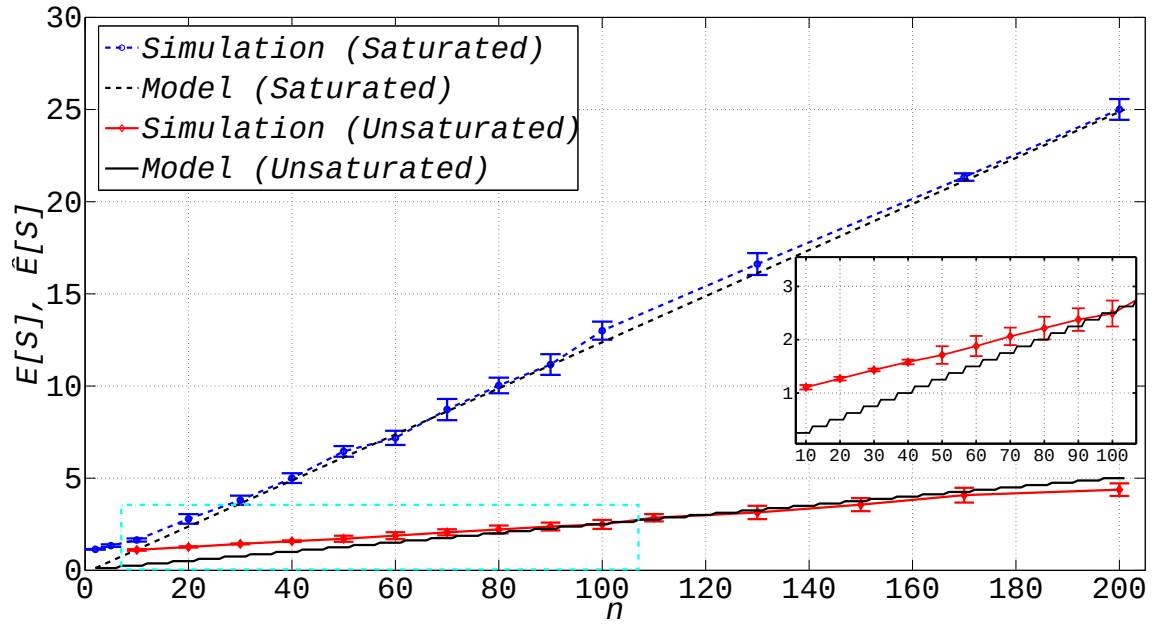


Figure 6.22: Simulation and analytical results for the $E[S], \hat{E}[S]$ in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max} = 8$.

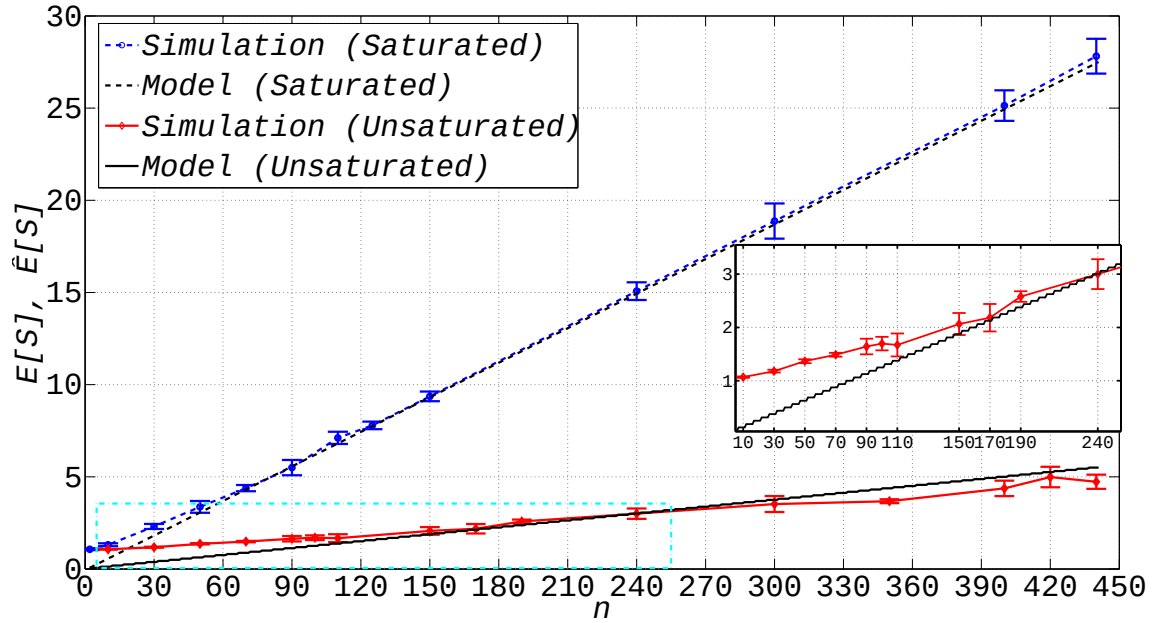


Figure 6.23: Simulation and analytical results for the $E[S], \hat{E}[S]$ in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max} = 16$.

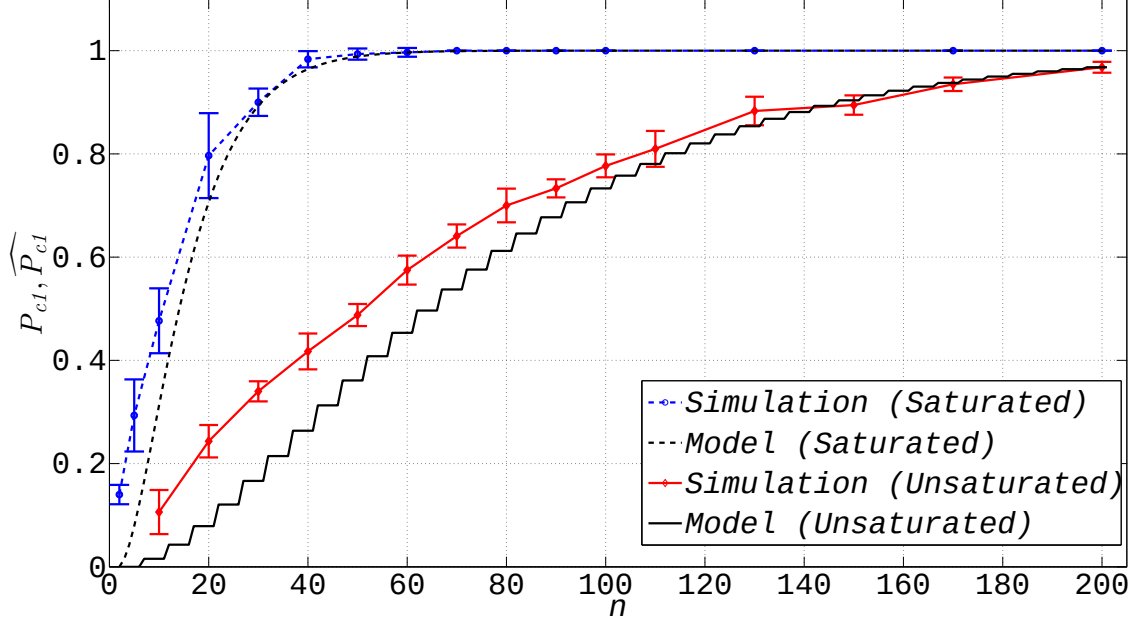


Figure 6.24: Simulation and analytical results for the CW_1 collision probability in the unsaturated (solid line) and saturated (dashed line) regimes, for $CW_1^{max} = 8$.

collision probability (but for the case of a single contention window).

The deviation that is observed in Figures 6.24 and 6.25 for the unsaturated regime can be explained by the number of nodes that are present in the lowest order slot in the CW_1 . In each one of the aforementioned figures, a close-up of the chart area is presented, showing the deviation between the model and simulation results. For the case of $CW_k^{max} = 8$, $k \in \{1, 2\}$, the model underestimates the number of nodes that are able to pass from CW_1 to CW_2 , i.e. the number of nodes that have chosen the lowest order slot in CW_1 . The deviation observed for $\hat{E}[S] < 2.5$ nodes, which corresponds to a network with 100 nodes. For $CW_k^{max} = 16$, $k \in \{1, 2\}$, the close-up presented in Figure 6.25 shows that the model underestimates the value of $\hat{E}[S]$ as well. For this value of CW_k^{max} , a deviation is also observed for an expected number of nodes, $\hat{E}[S]$, up to 2.5. This value matches to a network size of $n = 240$ nodes. Numerically, the CW_1 collision probability is only meaningful when two or more nodes pass from CW_1 to the CW_2 . While this condition is not verified, the model presents this kind of deviations due to the decimal to integer rounding procedure. Hence, due to the underestimation of the expected number of nodes that pass from CW_1 to CW_2 this leads to errors that can reach a maximum of 12 %. With our model and the presented values, we obtain MAE values of 5.19 % and 5.62 % for the unsaturated regime and of 3.60 % and 2.76 % in the saturated case, for $CW_k^{max} = 8$ and 16, $k \in \{1, 2\}$, respectively.

Figures 6.26 and 6.27 present a comparison between simulation and analytical results for the collision probability in CW_2 as a function of n for two different values of the contention window sizes $CW_k^{max} = \{8, 16\}$, $k \in \{1, 2\}$. The saturated and unsaturated regimes are considered. For comparison purposes, the numerical model for the CW_2 collision probability that uses the combinatorics approach is considered. Figure 6.26 considers $CW_k^{max} = 8$, $k \in \{1, 2\}$. We observe that the analytical curves are similar to the simulation ones, except for $n \leq 20$ and $n \leq 70$, for the saturated and unsaturated regimes, respectively, where the range of the 95 % confidence interval does not superimpose the analytical curves. For higher values of n , the numerical model for the CW_2 collision probability is very accurate, compared with the simulation values. Figure 6.27 shows the results for $CW_k^{max} = 16$, $k \in \{1, 2\}$. One also verifies

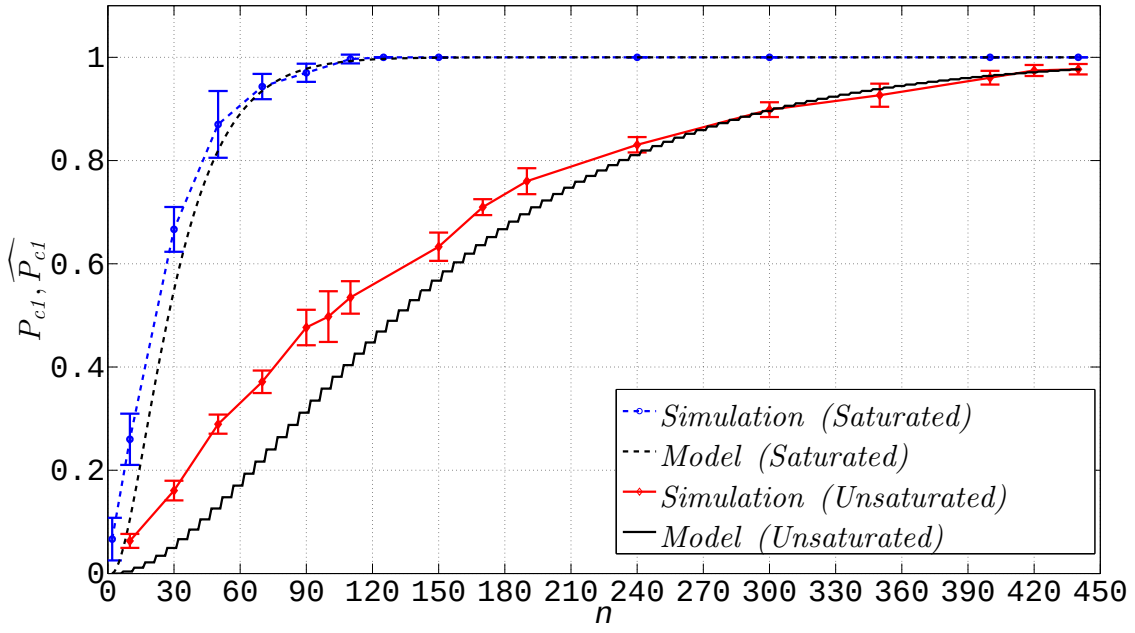


Figure 6.25: Simulation and analytical results for the CW_1 collision probability for $CW_1^{max} = 16$ in unsaturated (solid line) and saturated (dashed line) regimes.

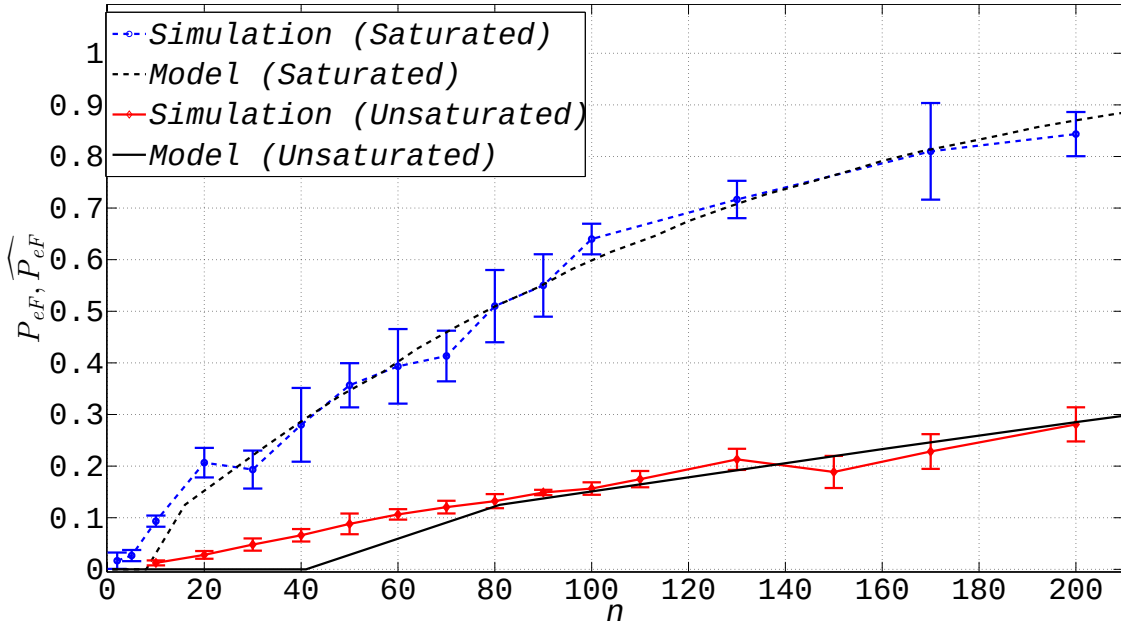


Figure 6.26: Simulation and analytical results for the CW_2 collision probability for $CW_k^{max} = 8, k \in \{1, 2\}$ in unsaturated (solid line) and saturated (dashed line) regimes.

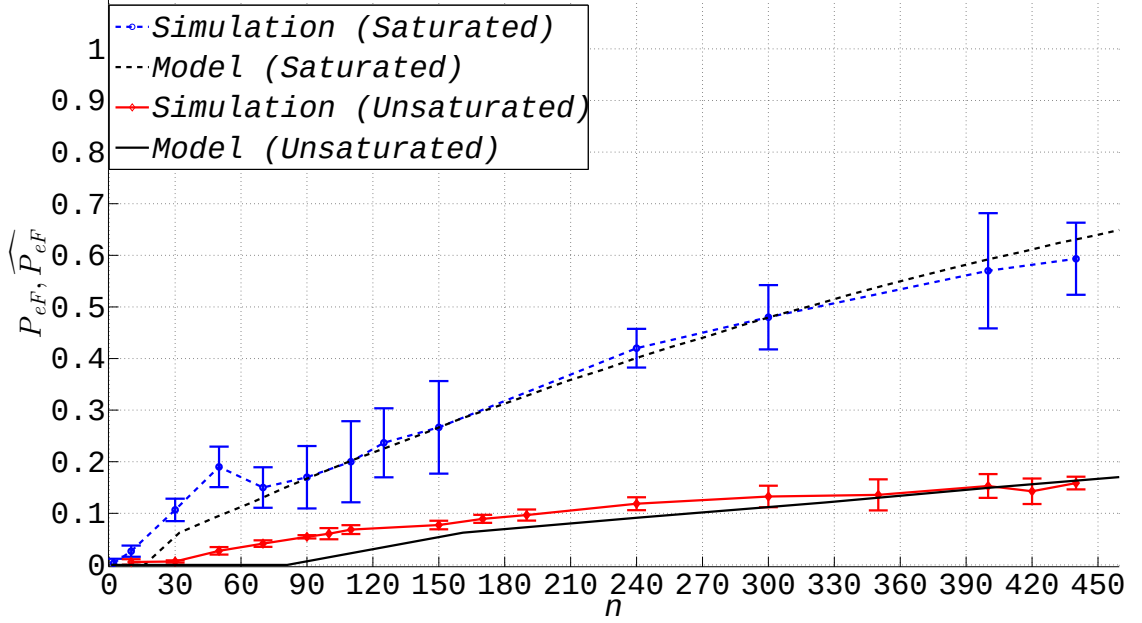


Figure 6.27: Simulation and analytical results for the CW_2 collision probability for $CW_k^{max} = 16, k \in \{1, 2\}$ in unsaturated (solid line) and saturated (dashed line) regimes.

that the results for the saturated regime are more accurate than the ones for the unsaturated one. Furthermore, we observe that the analytical results are similar to the simulation ones, except for $n \leq 40$ in the saturated regime. For larger values of the number of contending nodes, the simulation curves are well fitted by the analytical ones. However, for the unsaturated regime, the analytical results present some deviation from the simulated ones for larger number of contending nodes. Nevertheless, the analytical curve fits the simulation results, for the largest network sizes. The analytical model underestimates the simulated collision probability in CW_2 , presenting a maximum deviation of approximately 0.05 from the simulated value. The similarity between the two curves for the CW_1 and CW_2 collision probabilities and the expected number of nodes that pass from CW_1 to CW_2 verifies the validity of the proposed models for the CW_1 and CW_2 collision probabilities in the SCP two-phase contention window mechanism.

6.5 Service Time and Throughput Theoretical Model for a Two-Phase Contention Window Mechanism

6.5.1 Stochastic Service Time and Throughput Model for the Saturated Regime

In this section, we apply the proposed model for the collision probability in the two-phase contention window mechanism to derive the average MAC service time ($\overline{T_{sv}}$) for a successful transmission as well as the achieved throughput ($\overline{\vartheta_s}$). We provide numerical results for both service time and throughput, verified by simulation. The simulations mimic the two-phase contention window mechanism implemented in the Mobility Framework [REHD08], which provides the required traces for the service time and throughput.

We define the MAC service time as the time needed by the MAC protocol operation time between the instant when a frame is withdrawn from the MAC queue to be transmitted until the end of the transmission process, i.e., until the instant the MAC layer is ready to withdraw

another frame from the MAC queue. A data packet is removed from the queue when one of the following events occurs: after being successfully received at the destination node or after being transmitted but involved in a collision. To investigate the asymptotic behaviour of the service time and throughput unlimited retransmissions attempts (ζ), $\zeta \rightarrow \infty$, are assumed. Even though we consider unlimited retransmissions attempts, a packet transmitted by a node is always bounded by a finite number ζ of retransmissions attempts.

We consider the following two events in the definition of the service time, $\overline{T_{sv}}$:

- The event of dropping data packets due to a transmission of a packet involved in a collision at the receiver, is given by P_{cF} defined in Equation 6.29;
- The event of a successful data packet transmission after i -th transmission attempts after $i - 1$ consecutive transmission failures, for $i = 1, \dots, \zeta$, $\forall \zeta \rightarrow \infty$, is given by P_{sF} as follows.

During channel carrier sensing, if a node detects an occupied channel during CW_1 or CW_2 , it keeps the packet in the queue and tries to send it in the next frame. To define the probability of no collision occurrence in the second contention window CW_2 , the same rationale from the Equation 6.29 is applied. As a consequence, the probability P_{sF} is given by:

$$P_{sF} = 1 - \sum_{k=1}^{CW_2^{max}} P_{Scol} P_{Sidle}^{(k-1)} \quad (6.46)$$

The average service time $\overline{T_{sv}}$ is given by the ratio between the initial size of the network, n , and the total number of nodes per slot, n_{tx} , that effectively transmit the data packet (with and without collisions at the receiver node). Here, it is assumed that the two-phase contention mechanism is repeated after T_{poll} seconds. Recall that T_{poll} is the length of the cycle between two consecutive frames and is referred as the polling or renewal interval. A more general analysis of the service time can be achieved by considering T_{poll} . Finally, the dependence of the average service time on n , n_{tx} and T_{poll} is given by:

$$\overline{T_{sv}} = \frac{n}{n_{tx}} \cdot T_{poll} \quad (6.47)$$

The number of nodes per slot that effectively transmit the data packet is obtained by computing the following expected number:

$$n_{tx\_S} = \frac{E[S] \cdot P_{sF}}{CW_2^{max}} \quad (6.48)$$

$$n_{tx\_F} = \frac{E[S] \cdot P_{cF}}{CW_2^{max}} \quad (6.49)$$

where n_{tx_S} and n_{tx_F} are the number of nodes per slot that transmit a data packet and experienced a successful reception or the number of nodes transmitting a packet involved in a collision, respectively. The total number of nodes per slot, n_{tx} , is given by:

$$n_{tx} = n_{tx\_S} + n_{tx\_F} \quad (6.50)$$

The throughput $\overline{\vartheta_s}$ is defined as the network capability of processing successful packet transmissions. Regarding the proposed model, a packet is successfully transmitted if the node detects

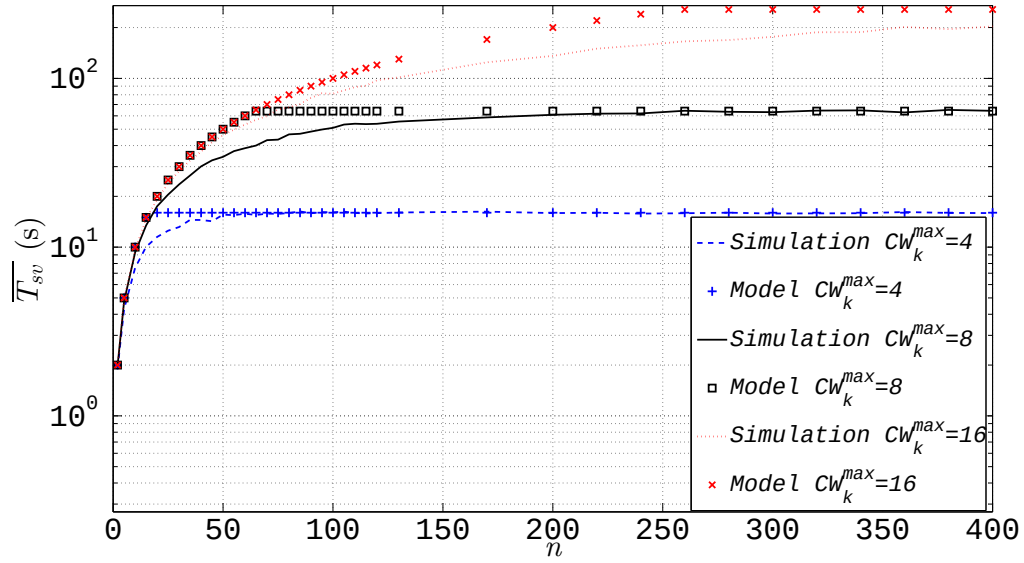


Figure 6.28: Simulation and analytical results for the service time for $CW_k^{max} = \{4; 8; 16\}$, $k \in \{1, 2\}$ in the saturated regime.

the medium idle during the contention window CW_1 and CW_2 . The packet transmission can either result into a successful reception or collision at the receiver node. The throughput is expressed by

$$\overline{\vartheta}_s = \frac{L_{data}}{\overline{T}_{sv}} \quad (6.51)$$

Note that the network throughput $\overline{\vartheta}_s$ is meaningful only when the WSN is under saturated conditions.

6.5.2 Simulation and Analytical Results Comparison

Figures 6.28 and 6.29 show the dependence of the average service time and throughput on the number of nodes with the contention window maximum sizes (varying from 4 up to 16 slots).

When the number of nodes is small, e.g., $n = 20$, there are some gaps between our analytical and simulation results for the average service time, $\overline{T}_{sv}$, shown in Figure 6.28. For instance, numerical results for the service time $\overline{T}_{sv}$ when $CW_k^{max} = 8, k \in \{1, 2\}$ are deviated from the simulation until it reaches a network size of 64 nodes. However, for network sizes that vary from 2 up to a maximum size of 20 nodes and larger than 70 nodes both numerical and simulation results are well matched for the service time. The reason for these deviations is the number of nodes that pass from CW_1 to CW_2 . The CW_1 collision probability is only meaningful when two or more nodes pass from CW_1 to CW_2 . If less than two nodes pass from CW_1 to CW_2 , these deviations are observed. They become more significant as the contention windows sizes increases.

Figure 6.29 presents the network throughput $\overline{\vartheta}_s$. Similarly to the average service time from Figure 6.28, the model matches the simulation results although some deviations are observed. It can be observed from the figures that the average service time increases, while the network throughput decreases significantly as the number of sensor nodes and the contention windows sizes increase. The average service time and throughput are bounded (both reach the satu-

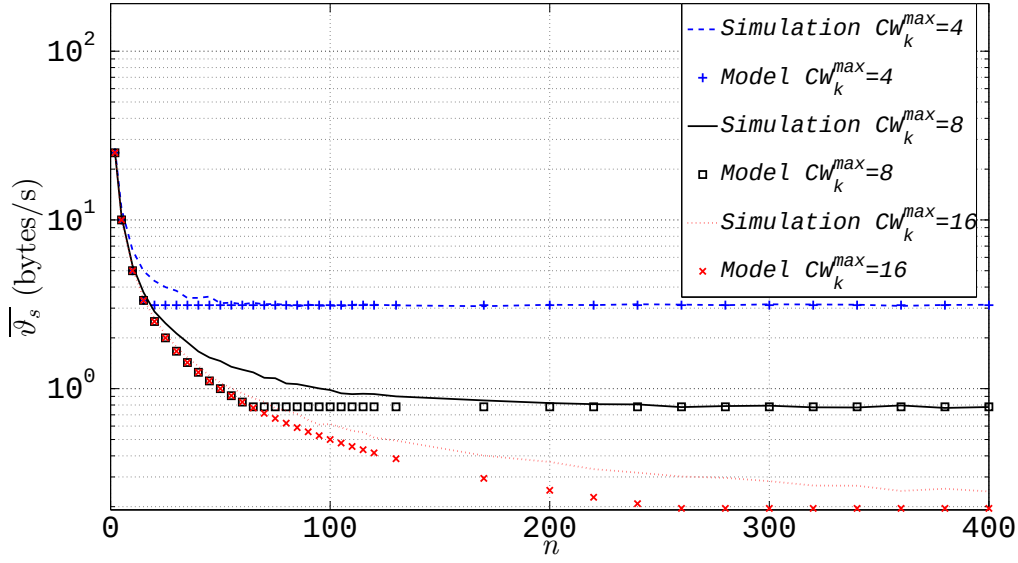


Figure 6.29: Simulation and analytical results for the throughput for $CW_k^{max} = \{4; 8; 16\}$, $k \in \{1, 2\}$ in the saturated regime.

ration) by an asymptotic value when the collision probability in the contention window CW_1 reaches the maximum value.

6.5.3 Summary and Conclusions

This Section focuses on the collision probability of a MAC protocol with a two-phase contention mechanism. Following the analytical study from Section 6.4 on the collision probability in the first contention window (CW_1) and in the second one (CW_2) along with the expected number of nodes that pass from CW_1 to CW_2 (under saturated and unsaturated traffic loads), the simulation results from this Section verify the analytical models (individual slot state analysis approach and combinatorics one). The collision probabilities of SCP two-phase contention mechanism are investigated whilst considering saturated and unsaturated traffic load regimes. We show that the CW_2 collision probability is directly related to the expected number of nodes that pass to CW_2 . For the expected number of nodes that pass from CW_1 to CW_2 , simulation and analytical results are well fitted. The results from the model under the unsaturated regime present some deviation relatively to the simulation results, although they follow them for larger number of nodes. For $CW_k^{max} = 8$, $k \in \{1, 2\}$, the CW_2 collision probability analytical curves are similar to the simulation ones, except for $n \leq 20$ and $n \leq 70$, for the saturated and unsaturated regimes, respectively. For $CW_k^{max} = 16$, $k \in \{1, 2\}$, the analytical results match the simulation ones, except for $n \leq 40$ in the saturated regime. In the unsaturated case, some deviation from the simulated results occurs for larger number of contending nodes. The analytical model underestimates the simulated collision probability in CW_2 , presenting a maximum deviation of approximately 5 % from the simulated value. Once again, the observed deviations are due to the rounding operations of the expected number of nodes that pass from CW_1 to CW_2 . From our analytical model for the collision probability in the two-phase contention window mechanism we derive the average MAC service time for a successful transmission and the achieved throughput. The average service time increases while the network throughput decreases significantly as the number of sensor nodes and the contention windows sizes increase. The average service

time and throughput are bounded by an asymptotic value when the collision probability in the contention window CW_1 reaches the maximum value.

6.6 Simulation of SCP in the Context of IEEE 802.15.4

6.6.1 IEEE 802.15.4 Compliant

The SCP has been first implemented by us in the OMNeT++ simulator [Var10], using the Mobility Framework initially from [REHD08]. Then, the SCP code has been ported to the new MiXiM Framework [KSW⁺08]. The MiXiM Framework supports CC1100 [CC107] and CC2420 [CC207] radio energy consumption models, as well as several propagation models. Moreover, we have extended it to work with AT86RF231 [AT809] radio transceiver. The latter is the best radio available in the market in terms of energy consumption. From all the radio transceivers the CC1100 is the only one that is non-compliant IEEE 802.15.4. We intend to compare the performance of SCP with IEEE 802.15.4 compliant and non-compliant transceivers. IEEE 802.15.4 is a double standard: PHY and MAC layers. By definition, if we program a board with our own MAC, it cannot be IEEE 802.15.4 compliant. The reason for using an IEEE 802.15.4 compliant radio is that hundreds of millions of 15.4 chips have been sold in the world and it is by the far the *de facto* standard for those low power networks. The key aspects of the IEEE 802.15.4 standard are the following: the transmitter output power can be tuned from approximately -30 dBm to +3 dBm on the majority of the radios; the sensitivity has to be < -85 dBm, but the sensitivity for some radios can go as low as -101 dBm; there are 16 different frequency channels ($2.405 \text{ GHz} + n \times 5 \text{ MHz}$), which are orthogonal (i.e., adjacent channels do not interfere); a radio chip consumes power when it is on (about the same power when transmitting, receiving or idle listening), and no power when the radio is off; it takes $192 \mu\text{s}$ for a radio chip to perform the transition from Transmission (TX) to Reception (RX) mode, and vice-versa; The maximum length of the IEEE 802.15.4 frame should be 127 Bytes. We consider an IEEE 802.15.4 non-beacon scheme in our simulations.

Our simulator considers single and multi-hop network topologies. The nodes may communicate only with reachable neighbour nodes. The deployment area defined in the configuration file for the single-hop scenario is $400 \times 400 \text{ m}^2$, while for the multi-hop scenario it is $800 \times 100 \text{ m}^2$. For each experiment, a set of six seeds is chosen for the random generator of SCP.

In our simulator protocol stack, each layer is connected with the higher and lower layers. There is an application module layer connected to the MAC and PHY layer modules. Besides these modules, a battery module and statistics battery module are included in order to simulate the network or node lifetime, while varying the capacity of the batteries. In the end of the simulation the statistics battery module presents the battery statistics collected during the simulation. Nodes are assumed static.

The typical values for the current consumption, data rate, and sensitivity of the radios are also defined in the simulation configuration file, as presented in Table 6.4. The sensor nodes battery voltage is 3.3 V. The following channel parameters are also defined in the MiXiM simulation Framework: *max_TXPower* corresponds to the maximum transmission power allowed in the channel (1.99 mW); *txPower* is the transmission power (1 mW), while *thermalNoise* is the electronic noise generated by the thermal agitation (-110 dBm). The Analogue Model Type parameter is the propagation model used in the channel (*SimplePathlossModel*), while *alpha* is the propagation exponent for the free-space path loss formula (i.e., 2). The *berLowerBound*

Table 6.4: Typical values for CC1100, CC2420 and AT86RF231 radios ($P_{tx}=1$ mW).

Symbol	Meaning	CC1100	CC2420	AT86RF231
I_{tx}	Current in transmitting	16.9 mA	17.4 mA	11.6 mA
$I_{rx}=I_{listen}$	Current in receiving/listening	16.9 mA	18.8 mA	12.3 mA
I_{poll}	Current in polling	16.4 mA	18.8 mA	12.3 mA
I_{sleep}	Current in sleep	0.02 mA	0.000021 mA	0.00002 mA
r_B	Bit rate	250 kbps	250 kbps	250 kbps
S_{min}	Sensitivity	-111 dBm	-94 dBm	-101 dBm
f_b	Carrier Frequency	868 MHz	2.4 GHz	2.4 GHz

parameter is the lower bound of the bit-error-rate (1×10^{-8}). Modulation type is the modulation that the transceiver works with (MSK for IEEE 802.15.4 non-compliant radio transceivers and OQPSK for IEEE 802.15.4 compliant ones). The *queueLength* parameter is the maximum number of packets waiting to be transmitted allowed in the queue (i.e., 50). In our simulations, the three radio models (from MiXiM) do not include the poll state [Var10]: when a node wakes-up and does not have data packets in its MAC queue, it polls the channel for 2 ms, while the power consumption is the same as in the receiving state.

6.6.2 Comparison between IEEE 802.15.4 Compliant and IEEE 802.15.4 Absence

Power Consumption without Piggyback (periodic traffic)

It is worthwhile to compare simulation and analytical results for the average power consumption for each node. When no piggybacking is considered, we define the “adapted” analytical model (lower and upper bounds) from the original SCP work [YSH06] and ran the simulator to extract the values.

The employed topology considers five nodes in star topology. In this simulations, the *sync slave* mode is enabled, the synchronization time is defined as $t_{sync} = 60$ ms and the inter arrival period is variable. Moreover the simulator also considers, t_{sync} , the synchronization period, which depends on the inter-arrival period (already defined by the authors from [YSH06]), T_{sync} . As the synchronization period increases the wake-up tone duration also increases. We consider for the maximum contention window size $CW_1^{max} = 8$ and $CW_2^{max} = 16$. For this experiment all five nodes from the network form in a single-hop configuration, where each node generates and broadcasts 50 data packets (with 50 Bytes each). Since the inter-arrival period varies between 50 and 300 s, the traffic load is considered to be light. Simulations are run five times for each of the six seeds, generating a total of thirty experiments. For each experiment the average power consumption of each node is obtained, as shown in Figure 6.30. The achieved 95 % confidence intervals are negligible.

Figures 6.30 and 6.31 presents a power consumption comparison between simulation and analytical results (lower and upper bound), as a function of the inter-arrival period for three different radio transceivers. The CC1100 is the one that presents the highest power consumption when is compared with the CC2420 and AT86RF231 ones.

The CC2420 transceiver consumes approximately 0.04 mW less than the CC1100 one, while AT86RF231 consumes around 0.08 mW less. This is due to the low power consumption that the AT86RF231 presents combined with the long times the node remains in sleep mode. Besides, the MSE is calculated with respect to the analytical lower bound curve, and a value of 5.1319×10^{-7}

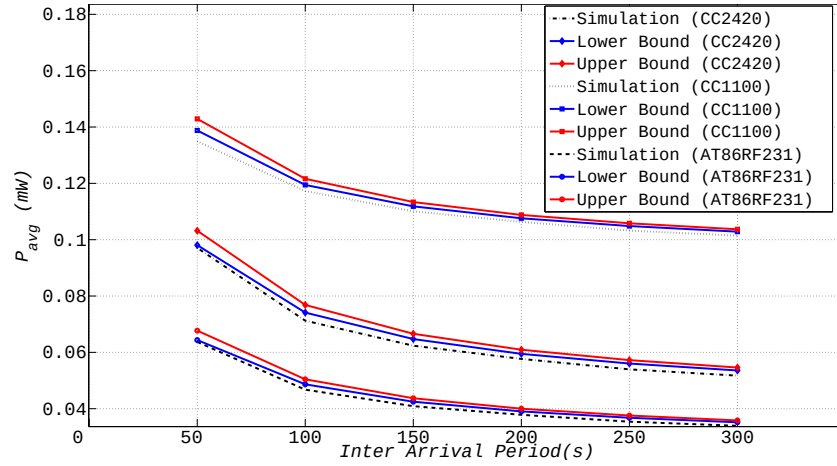


Figure 6.30: Lower/upper bound and simulation results with no piggyback for the power consumption per node of CC1100, CC2420 and AT86RF231.

mW for CC1100, a value of 1.4213×10^{-6} mW for CC2420 and a value of 6.3434×10^{-7} mW for AT86RF231 is obtained. This shows a high similarity between the simulations and analytical results.

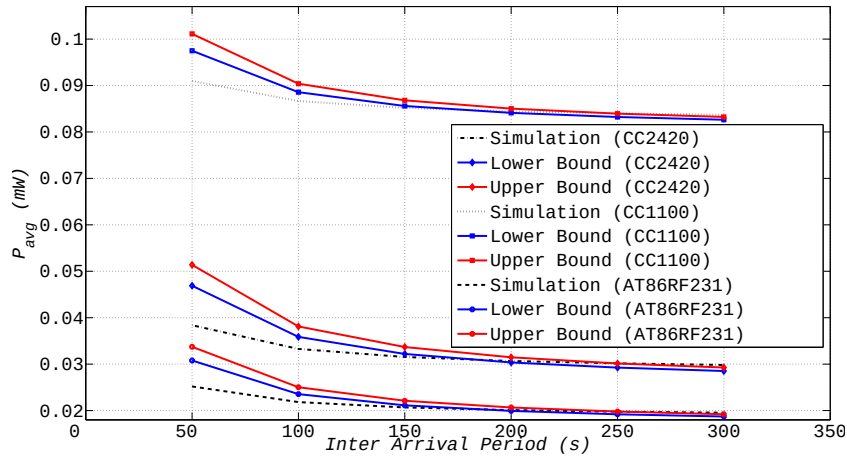


Figure 6.31: Lower/upper bound and simulation results with piggyback for the power consumption per node of CC1100, CC2420 and AT86RF231.

If the t_{sync} parameter is changed from 60 to 50 ms while maintaining the remaining parameters, the power consumption becomes less similar to the lower bound (in comparison with the previous one). From these results, one may conclude that the power consumption with the *sync slave* mode enabled presents better results when $t_{sync} = 60$ ms. However, for values of t_{sync} lower than 50 ms it was not possible to achieve stable results with the SCP simulations. Moreover, for values of t_{sync} higher than 60 ms, higher values for power consumption are achieved.

Power Consumption with Piggyback (periodic traffic)

The lower and upper bound for the “adapted” analytical model are also defined for the case when synchronization schedules are piggybacked, whilst maintaining the simulator topology. However, since all the exchanged traffic is of the broadcast type, all the SYNC packets can be suppressed and the schedule synchronization is performed by using the piggyback technique. Hence, the piggyback mode is enabled for this experiment. There is no need to define the values for the parameter t_{sync} , as the schedule information is already piggybacked into the

data packets, leading to a consequent decrease of node energy consumption. For this set of simulations, the wake-up tone duration is always equal to 2 ms. The only parameter that varies is $T_{data} \in \{50; 100; 150; 200; 250; 300\}$.

The dependence of the average power consumption of each node on the inter-arrival period is shown in Figures 6.30 and 6.31, where the simulations and analytical results (upper and lower bounds) are also presented for comparison purposes. The achieved 95 % confidence intervals are negligible.

For $CW_1^{max} = 8$ and $CW_2^{max} = 16$, the obtained simulation results are similar to the lower bound curve defined by the analytical model until the inter-arrival period achieves 200 s. For an inter-arrival period higher than 200 s, the simulation results are similar to the upper bound curve and even superimposes the upper bound when it achieves 300 s. The MSE values obtained for this experiment with respect to the lower bound curve are equal to 7.9825×10^{-6} mW, 1.3524×10^{-5} mW and 5.8479×10^{-6} mW, for the CC1100, CC2420 and AT86RF231 transceivers, respectively.

By comparing the power consumptions with explicit SYNC packets and with piggyback synchronization, we observe that the piggyback technique is truly efficient, since the power consumption with piggybacking achieves lower values than the one with explicit SYNC packets. In this set of experiments the poll period is set to 5 s, which is more than enough for example for a healthcare monitoring application reporting sensors values. Therefore, in a healthcare application, if we use a sensor node with the AT86RF231 radio transceiver whilst enabling the piggyback synchronization, the node lifetime will increase significantly due to the low associated power consumption.

Throughput Performance with Heavy Traffic Load

In real world applications, WSNs do not have the capability to predict what type of traffic load is being exchanged with high accuracy. For example, in a healthcare scenario, the sensor nodes deliver the monitoring data from the vital signs of the patients at a lower data rate (in usual situations). However, when a patient presents anomalies in the vital signs the sensor node may deliver data at a higher rate, leading to the need for higher network throughput.

For this set of experiments, we have enabled the *Throughput* mode at the application layer, in order to test the network's response capability as the number of transmitting nodes increases. By varying the number of transmitting nodes the contention time of the network will increase, leading to an increase of the collision probability. Each node generates 20 packets (with 100 Bytes each). A five nodes in star topology is considered. In these experiences the nodes poll the channel each second. Besides varying the number of transmitting nodes, the CW_1 and CW_2 contention window sizes also vary.

The throughput is the ratio between the amount of data packets received with success by the destination node and the time taken to arrive at this node. By analysing Figure 6.32, all the results for the throughput (for all the three radio transceivers) match while the contention window sizes vary. The throughput is maximum (for all contending time configurations) when there is only one node transmitting, as expected, since there is no more nodes competing for the channel to send packets. When two nodes are competing for the channel, the throughput drops around 25 % of the maximum achievable throughput, because there is more than one node trying to transmit the data packet. As the number of transmitting nodes increases, the contending time will also increase, leading to a collision probability increase.

In terms of energy consumption when considering the IEEE 802.15.4 compliant radios (with

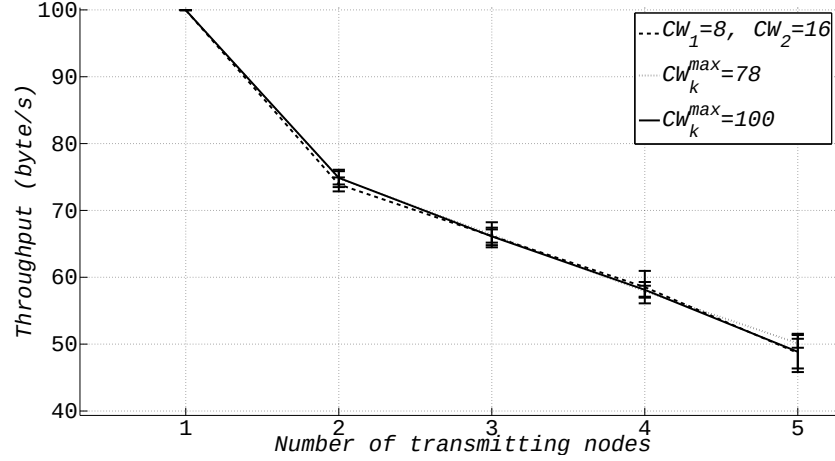


Figure 6.32: SCP throughput in function of the number of transmitting nodes and maximum contention windows sizes, $k \in \{1, 2\}$.

high duty cycles) the CC2420 energy consumption is higher than the CC1100 one, because the CC2420 achieves lower power consumption when the radio transceiver remains more time in sleep mode. Since the *Throughput* mode enables the node to wakeup every second to poll the channel, the energy consumption will increase when compared with the CC1100. The AT86RF231 radio transceiver is the one that presents the lowest power consumption (from all the three radio transceivers), mainly due to the lowest values of the power consumptions it achieves whatever the operating mode is.

Node energy consumption for Linear Chain (multi-hop)

By considering experiences with multi-hop topology in a linear chain, we intend to evaluate the SCP energy and latency performance. We enabled the *multi_hop* mode, where only the application layer from node 1 generates data packets to be sent to the other nodes. Node n receives data packets and answers with ACK packets when a data packet is received correctly, as presented in Figure 5.7. The wake-up tone duration is always set to be equal to 2 ms, whilst each node polls every second. In our topology, we have deployed $n - 2$ forwarders nodes, one sink node, and one source node. For the multi-hop evaluation the acknowledgement mode may be enabled/disabled.

In multi-hop networks, there is no optimal working point and network performance depends on what application the network supports. The topology used in this set of experiences is the one presented in Figure 5.7, with a network composed by a 9-hop linear topology with ten nodes (each one separated by 50 m from each other).

The source node generates 20 packets (each with 50 Bytes), with an inter-arrival period that varies between 0 and 10 s. Nodes will rebroadcast the data packets along the linear chain until the packet reaches the most distant node from the chain. Considering an inter-arrival time equal to zero means the application layer generates data packets and sends it to the lower layers the fastest way possible, as previously explained in the *Throughput* mode.

For a contention window sizes configuration of $CW_1^{max} = CW_2^{max} = 208$, this combination is the one that presents the highest energy consumption per node for all the three radio transceivers, Figure 6.33, due to the maximum contention time nodes use to avoid the packets collisions. Comparing the energy consumptions between the three radio transceivers, the one that presents the lowest mean energy consumption is the AT86RF231 one. The CC2420 radio transceiver presents energy consumptions similar to the CC1100 radio transceiver. The energy consump-

tions are lower when comparing with the energy consumptions for multi-hop experiments in the original paper [YSH06].

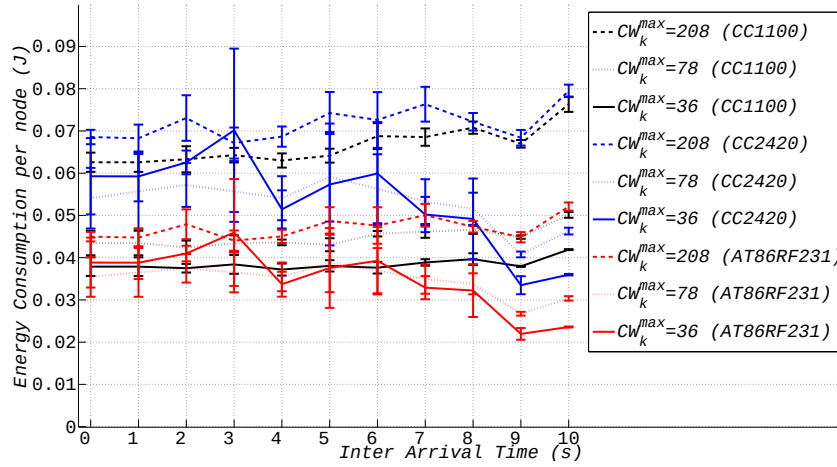


Figure 6.33: Average energy consumption in function of the inter-arrival time and different contention windows sizes for the multi-hop experiments, $k \in \{1, 2\}$.

For all the configurations the energy consumption behaviour is approximately stable as the inter-arrival time is increasing.

Node latency (multi-hop)

This section addresses the SCP latency over a 9-hop network. We alternate the polling period between 0.15 s and 1s, enable or disable the *acknowledgement* mode, and set the contention windows maximum sizes to $CW_1^{max} = CW_2^{max} = 16$ slots. When the inter-arrival time is equal or higher than 1 s (light traffic) it is expected that only one packet is sent through one hop, during one polling interval. When the polling period is changed to 0.15 s we expect that the latency decreases significantly, since the node will wake-up almost seven times in one second, and will schedule and send more data packets in less time.

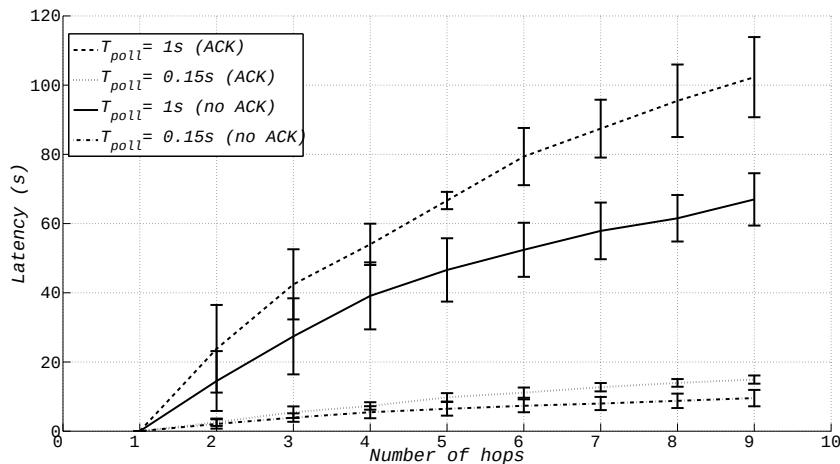


Figure 6.34: Mean packet latency over 9 hops in function of number of hops, for $CW_1^{max} = CW_2^{max} = 16$, while enabling/disabling ACK packets feature.

Regarding Figure 6.34, we may conclude that the latency curve when SCP polls each second (with the ACK packets feature enabled) is the one that presents the highest delay, due to the data packets retransmissions. When the polling period is set to 0.15 s, the maximum data packet latency is less than 20 s, but the energy consumption increases due to the number of

times the node wakes-up. The other two latency curves are related with the same experiments, but the ACK packets feature is disabled. With the ACK packets feature disabled for all three radio transceivers, we observe that the maximum data packet latency is less than 70 s (at the end of the linear chain), when polling each second. Moreover, when polling at each 0.15 s (with the ACK packets feature disabled), the latency is less than 10 s.

Node data packet success rate (multi-hop)

To observe if there is any tradeoff when the ACK packets feature is enabled or disabled, we have plotted the Data Packet Success Rate (DPSR) for all four configurations described previously. Figure 6.35 shows that, with the ACK feature enabled for both polling periods, there is around 100 % packet delivery success for all the three radio transceivers. When the ACK feature is disabled for both polling periods, the packet delivery in both experiments varies around 75 and 89 % for all the considered radio transceivers. Regarding these results, enabling ACK packets feature will result into an increase of data packet delivery. However, the tradeoff is the increase of the latency and energy consumption.

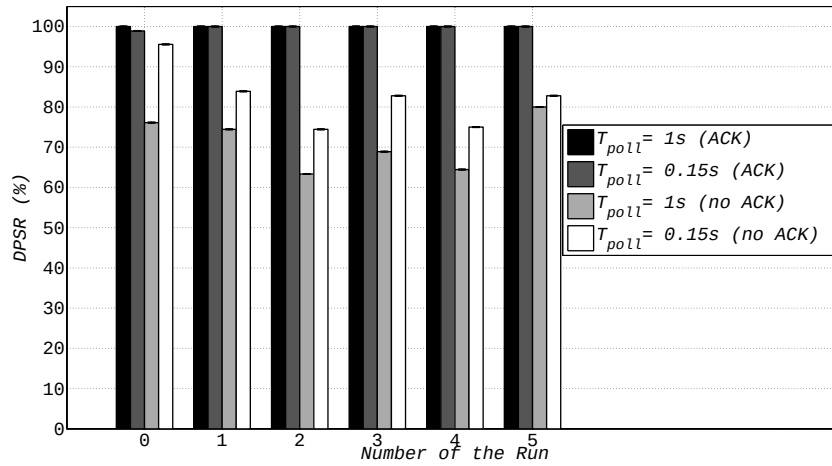


Figure 6.35: DPSR in function of the simulator run over 9 hops, for $CW_1^{max} = CW_2^{max} = 16$, while enabling/disabling the ACK feature.

6.6.3 Summary and Conclusions

In this Section, we provide a detailed analysis of the mechanism used in SCP, learned from our own experience while implementing the SCP protocol in the MiXiM Framework. Our results help to clarify some missing aspects in the original SCP protocol description, as well as providing an evaluation of performance metrics (for single and multi-hop topology) by means of simulation. By comparing the power consumptions in the presence and absence of a fixed wake-up tone duration, the energy savings obtained with a fixed wake-up tone duration are adequate (more or less 0.005 mW). The use of IEEE 802.15.4 compliant radio transceivers leads to a clear decrease in the energy consumption in the presence and absence of piggybacking. Considering a multi-hop linear chain of sensor nodes, the SCP energy consumption is stable as the inter-arrival time varies. However, only the AT86RF231 transceiver presents lower mean energy consumption compared with the radio transceiver that does not complies with the IEEE 802.15.4 standard. Besides, the values of the achieved throughput are similar for both types of transceiver. In terms of delay, all the three radio transceivers present the same data packet latency, since the transmission data rate is the same and the specific time parameters of all these radio

transceivers are approximately the same. Considering a healthcare application where the nodes report periodically to a sink node the values from the sensors, the SCP can be selected has the MAC protocol that can deliver data efficiently to the sink with low power consumption cost. However, some tradeoff exists when choosing the reporting period of the node. The latency, DPSR and energy consumption (considering a linear chain of sensor nodes in the Hospital) should be well balanced in order to fulfil the minimum requirements for the application.

6.7 Final Remarks

This chapter addressed four main issues: i) simulation of SCP-MAC in single-hop and multi-hop scenarios, ii) the proposal of a stochastic model for the collision probability, iii) the application of the model to derive the average MAC service time for a successful transmission as well as the achieved throughput, and iv) the comparison of the performance metrics of the SCP while considering an IEEE 802.15.4 compliant and IEEE 802.15.4 agnostic physical layer.

The SCP performance evaluation, which was implemented in the simulator, included the analysis of different performance metrics (in single-hop and multi-hop scenarios), such as power consumption (with and with no Piggyback), energy consumption and throughput, considering heavy and light periodic traffic patterns. It has been shown in Section 6.1 the adequacy between the model(s) and simulation results. Besides, the use of piggybacking technique has led to a gain of 10-30 % in the power consumption compared to explicit SYNC packets (piggybacking is not enabled). In addition, has also been investigated how some values of the parameters from SCP may cause changes in the performance. By setting the duration of the wake-up tone to a fixed value of 2 ms (minimum duration of the wake-up tone in SCP) an effective decrease of the energy consumption is achieved.

The comparison between different CW sizes has shown that, for a $CW_1^{max} = CW_2^{max} = 78$ and a $CW_1^{max} = CW_2^{max} = 100$ configurations, the achieved throughput are higher and more stable (80 B/s) than with $CW_1^{max} = CW_2^{max} = 16$ slots. It can also be concluded that the node that employs a larger maximum contention windows size presents a shorter lifetime.

A stochastic model for the collision probability in the collision avoidance mechanism with two contention windows from the SCP protocol has been proposed, whilst considering the saturated and unsaturated regimes. Results have shown that the CW_2 collision probability is directly related to the expected number of nodes that pass to CW_2 . It has also been shown that, for the expected number of nodes that pass from CW_1 to CW_2 , simulation and analytical results fit well. The use of IEEE 802.15.4 compliant radio transceivers leads to a clear decrease in the energy consumption in the presence and absence of piggybacking. In terms of delay, all the three radio transceivers present the same data packet latency, since the transmission data rate is the same and the specific time parameters of all these radio transceivers are approximately the same.

Chapter 7

Frame Capture Effect and Reliability Based Decider

The contributions from this chapter are twofold. Firstly, a new physical layer packet reception decision algorithm based on a reliability concept is proposed. Secondly, the implementation of the frame capture effect feature in the IEEE 802.15.4 compliant physical layer of the MiXiM simulation framework is addressed. The chapter is composed by seven sections. In Section 7.1 after defining the frame capture concept, is given, the main reasons for it to occur are described as well as its fundamental work principles. Section 7.2 presents the different frame capture scenarios (different frame overlapping situations) considered in this work. Section 7.3 tackles the potential impact of the frame capture effect on the MAC protocols. The way how the frame capture is implemented in the MiXiM simulation framework is discussed in Section 7.4. The presence and consideration of the frame capture effect in other simulators is also discussed. The decisions made on frames that arrive simultaneously at the physical layer and corresponding reasons are discussed, while presenting the details on IEEE 802.15.4 BER computation. Section 7.5 describes another novelty of the work from this thesis. It includes a formulation based on a reliability concept that utilizes the SNIR and size of the packet to guarantee the delivery, to the MAC layer, of a packet received at the PHY layer, with a certain reliability. This section ends with the justification of the frame capture decision thresholds considered in this work. Section 7.6 addresses the simulation scenario and metrics considered in the evaluation of the frame capture effect. Finally, Section 7.7 compares the results between the proposed enhanced reliability decision algorithm with frame capture and the default decider algorithm (for the simple MAC and SPC-MAC protocols), followed by some conclusions. Appendix E describes the environmental and path loss models implemented and considered in the MiXiM framework.

7.1 Definition of Frame Capture

The capture effect occurs at the physical layer, under some conditions, when two signal transmissions spatially and temporally overlap at a receiver. The simultaneous detection of two frames at a receiver is generally regarded as a collision. They will interfere with each other. As a consequence, the receiver is not able to decode either one of them. Although this is theoretically true, in the last years, the work from some researchers [LRLK08, FXHZ10] has shown that this assumption is not absolutely true. Under certain channel conditions and circumstances, the capture effect occurs when the strongest signal causes the other signals to be treated as noise (or interference) whilst being filtered out by the receiver. As a consequence, a packet is received even though a collision has occurred due to concurrent transmissions [LRLK08].

This phenomenon of being able to receive a frame (even in the presence of another interference frame) is called Frame Capture (FC). Sometimes, it is also named Physical Layer Capture (PLC), or even co-channel interference tolerance. This effect neglects the assumption of “*collision as failure*” in which packet collision leads to packet corruption. This assumption is commonly accepted in simulations [WWJ⁺05, SKA04], theoretical analysis [KT75], and collision avoidance

schemes [PCB00] .

The FC effect can be beneficial, since it has been exploited by many MAC and networking protocols to prevent packet collisions, increases network throughput, while decreasing delay. In theory, frame capture can provide additional gains through collision detection and the recovery of the strongest packet from collisions [WWJ⁺05].

7.1.1 Related Work

To the best of our knowledge, even though the capture effect has been mentioned and observed in a wide variety of radio transceivers, including IEEE 802.11, bluetooth radio and cellular systems, in the literature, the availability of simulators that support this effect and are IEEE 802.15.4 standard compliant is scarce. Several works have addressed the impact of FC on the performance of common networking protocols. In Aloha [Nam84] and 802.11 networks [HvS02, CL99, KL99], the capture effect has been used to increase throughput and decrease delay.

The authors from [LE06b] present a theoretical work in which the presence of FC leads to an optimal throughput and energy efficiency when all nodes transmit at maximum power. Other works have presented studies in which, depending on the type of modulation and decoding scheme, the signal strength difference required for FC to occur can be as large as 1-3 dB [Ash92], or as little as 0.17 dB [SC89].

Reference [WJCD00] presents the implied unfairness for ad-hoc networks, where closer nodes can “capture” the channel if their signal is sufficiently stronger. The authors from [CMR06] refer to FC as Physical Layer Capture, and conclude that this effect is larger at lower bit rates, by means of simulations in QualNet (to support their conclusions).

The authors from [LKL⁺07] performed the most complete real-world experiments, investigating the behaviour of FC in detail, while adding more information to the frame capture notion. These authors have discovered that, apart from the SNIR, the arrival time of the frames is also important, i.e., whether a frame can be captured or not. They have introduced the notion of different region, where the overlapping of frames occur. Even though this work was developed entirely for the IEEE 802.11a standard, it can be considered as a solid basis and be used to extract useful insights to guide the implementation of the FC in an IEEE 802.15.4 compliant physical layer.

In [FXHZ10], the authors have sought to determine the best way to use multiple receivers in a single-hop network cluster whilst comparing the advantages of receivers on multiple channels, with the enhancement in the capture effect when multiple receivers are on the same channel. The IEEE 802.11a work from [LKL⁺07] is considered by the authors while considering the Shuffle link-layer protocol [SCM⁺08]. This protocol [FXHZ10] has been proposed to reorder and schedule packet transmissions to take advantage of the Message-In-Message (MIM) capabilities of some wireless cards. Since, in general, the radio chips used in sensor networks do not have this capability, the authors consider two radio chips working in tandem, to duplicate the benefits of MIM packet reception. Furthermore, the authors from [DFEV05] show that, if multiple receivers are present, it is possible to combine corrupted versions of the packets for error correction purposes. Employing multiple receivers operating on the same frequency within the range of the transmitters originates two beneficial effects. First, the FC might prevent some packet losses when packet collisions are expected. Second, corrupted packets received at multiple receivers might have enough information to be successfully corrected and decoded.

In contrast to previous protocols, there are different works in the literature [MSM05, PEE⁺08, CLWY07] for modelling the 802.15.4 MAC protocol. However, the authors from [GBV10] state

that none of these models can be applied to query-based applications, where nodes have only one packet to be transmitted per query. These authors address the FC effect, in the beacon-enabled mode of the 802.15.4 MAC protocol, by means of mathematical analysis and experimentation. In contrast to the remaining works on 802.15.4 MAC modelling, their model allows for computing the Packet Success Probability (PSP) for a node in the presence of the FC effect.

7.1.2 Main Causes

Normally, in MAC protocols that employ a collision avoidance mechanism based on CSMA/CA, most of the collisions are avoided by using RTS/CTS control packets as well as the backoff counter. However, this only successfully works when unicast traffic is considered. If broadcast traffic is considered, the RTS/CTS mechanism cannot be used, since only one node must respond to the RTS packet. If several nodes respond to a received RTS packet, a collision will occur even before the data packet is being sent. In the context of the MAC protocols with no RTS/CTS scheme (broadcast traffic is considered), nodes are less aware of the surrounding traffic as well as of the transmissions of their neighbouring nodes. This leads to possible hidden terminals among the nodes.

Other MAC protocols, such as the SCP-MAC [YSH06], do not consider the traditional CSMA/CA avoidance mechanism. Rather, they consider a double contention window mechanism with a preamble between both contention windows, which is sent by the nodes that won the first contention window. The preamble sent by the node acts as a control packet that announces to other potential senders that a data packet transmission is going to occur after the second contention window. In this collision avoidance scheme, two types of collision may occur. First, preamble collisions occur when nodes choose the same time slot in the first contention window, to simultaneously perform carrier sense and initiate the transmission of the preamble. Second, data packet collisions occur when the nodes that won the first contention window gain access to the second contention window and start simultaneously transmitting the data packet in the second contention window. In this protocol, the data is only lost when data packet collisions occur. The occurrence of a preamble collision does not mean an effective data packet loss. Instead, only the preamble collides.

7.1.3 Work Principles for the Frame Capture

It is worthwhile to understand how the frame capture deals with two (or more) interfering signals at the hardware level. There are a lot of papers addressing the observed behaviour of the FC in different protocols. However, there is not a clear explanation on how the interfering signals are handled at the physical layer with frame capture implemented. Therefore, a clear description of the frame capture behaviour is in order, as it gives insights on how to implement the FC effect in a simulation framework.

Frame capture can occur in different overlapping scenarios. There are many variables that may influence the receiver behaviour and therefore the possible occurrence of a collision. Besides, there are certain thresholds involved in the decisions on which frame should the node receive when frame capture is enabled. These thresholds will be explained ahead.

If two or more frames are being transmitted “simultaneously” or are overlapping each other, the following factors should then be taken into account:

- **Received Signal Strength Indicator (RSSI)** - One of the two signals has to be sufficiently stronger than the other one in order the receiver to be able to decode it, even if a weaker

interfering signal is present. When the RSSI from both signals are equal, the decision on the correct decoding of one of the frames depends on the radio transceiver chipset hardware. Moreover, if one of the two interfering frames interferes with the preamble of the other ones, the required difference in RSSI is higher, because the preamble section of the packet is responsible for the correct receiver “lock” onto one of the signals;

- **Frame Time Arrival** - The time interval between the arrivals of two (or more) interfering frames is very important. Depending on the time of arrival of the interfering signal the beginning of the overlapping region will correspond to different sections of the frame. The overlapping can occur in three different sections of the frame: i) preamble field, ii) sync field, or iii) data field. With the FC enabled all these sections are distinguished, in Section 7.2, into different scenarios of overlapping with different decision thresholds to accept or not the frames;
- **Chipset Manufacturer** - Depending on the frame time arrival and depending on the chipset manufacturer, different conditions should be met in order the frame capture to work. In some chipsets, the frame capture only occurs if the second signal is strongest and arrives before or during the first frame’s preamble. The CC2420 [CC207, GBV10] can capture the stronger frame even after the reception of the weaker frame’s preamble. This means that there is independence between the time arrival of the frames. In the context of the frame capture effect, different overlapping regions (corresponding to different overlapping sections among the frames) are considered and further explained. These regions are numbered from 1 to 5.

As the interfering signals overlap the desired signal, the so called noise, I , is given by the sum of interfering carrier powers. If the useful carrier power from the desired packet, C , is sufficiently larger than I , then the desired signal is successfully decoded with large probability of success. This probability can be denoted as Conditional Frame Capture Probability (CFCP), which gives the probability that a packet is successfully decoded for a certain value of the carrier-to-noise ratio, C/I . The behaviour of the CFCP versus the C/I normally shows a step-wise behaviour. It takes values close to one, if C/I is higher than a given value. The authors from [GBV10] denote this value as protection ratio whilst defining it as the minimum C/I that ensures the correct reception of a packet.

In this work, the intention is to develop a PAN composed by multiple nodes that move randomly and operate with a simple MAC protocol that does not include any kind of carrier sense or collision avoidance mechanism. The objective is to study the worst case situations, when nodes transmit overlapping packets. Different overlapping regions are considered with the intention of developing a more robust physical layer with frame capture capabilities that is able to answer to different cases of overlapping frames. In such regions, the characteristics of frame capture effect in IEEE 802.15.4, which uses an OQPSK modulation format with DSSS, is going to be investigated and implemented in the MiXiM [Var10] simulation framework.

7.2 Frame Capture Scenarios

Based in the literature [LKL⁺07, CMR06, GBV10] and the experience acquired during the implementation of the frame capture effect in the MiXiM framework simulator [FXHZ10, LKL⁺07], two sets of interference regions can be defined. The former considers the relevant scenarios in which a maximum of two frames (the interfering and the desired ones) reach almost

Table 7.1: Collision ratio in each collision region (example for the CC1100 transceiver, extracted from [FXHZ10]), with $\delta_{preamble} = 32$ bits, $\delta_{sync} = 32$ bits, $\delta_{data} = 16$ bits, and $\delta = 80$ bits.

Collision Region	% of Collisions
Region 1	$100 \times \frac{\delta_{data}}{2\delta} = 10$
Region 2	$100 \times \frac{\delta_{sync}}{2\delta} = 20$
Region 3	$100 \times \frac{\delta_{preamble} + \delta_{data}}{2\delta} = 30$
Region 4	$100 \times \frac{\delta_{sync}}{2\delta} = 20$
Region 5	$100 \times \frac{\delta_{preamble}}{2\delta} = 20$

simultaneously the receiver. The latter addresses the cases with more than one interfering frame overlapping the desired signal whilst considering the same regions. One assumes that the strongest frame is always the desired one, since the content of the frames cannot be used to distinguish them. Receiving the strongest frame is a good decision in these cases because a strong SNIR corresponds to a low BER which, in turn, leads to a higher CFCP. Hence, it is reasonable to assume that the objective of a node with the frame capture feature enabled is to receive the strongest frame.

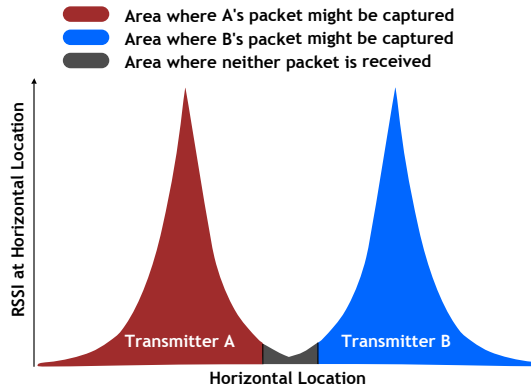


Figure 7.1: Signal strength and reception for two signals transmitted simultaneously (adapted from [FXHZ10]).

The authors from [GBV10] present an extension of the work from [WWJ⁺05] where they continue the initial work of the characterization of the capture effect with the CC1100 transceiver whilst expanding the analysis in order to include a general model to predict frame capture gains. The authors from [GBV10] illustrate the frame capture feature through Figure 7.1. Also Table 7.1 gives an overview of the percentage of collisions that occur in each region, depending on the sizes of the different CC1100 radio packet fields for the packets.

Since this thesis considers the CC2420 radio transceiver, for the sake of simplicity, only three main sections are considered: a preamble, a sync word, and a data field. Depending on the section of the frame that suffers collision, the Packet Success Rate (PSR) differs. Considering this packet format there are five possible collision scenarios, although two main sets of scenarios are addressed more ahead: one with only one interfering frame and another which accounts for more than one interfering frame. The PSR given in Table 7.1 for each region depends upon the duration of the corresponding sections of the packet, $\delta_{preamble}$, δ_{sync} , δ_{data} , and δ (the total duration of the packet).

Table 7.2, extracted from [LKL⁺07], shows the different frame capture regions with different timing and SIR situations for the Atheros chipsets. These experiments were performed for IEEE

802.11a compliant systems. Δt is the difference between the arrival times (in μs), $L_{preamble}$ is the length of the frame preamble, and the SNIR is given by $RSSI_1 - RSSI_2$ (in dB) as shown in Table 7.2. The $RSSI_1$, and $RSSI_2$ are the RSSI values for the frame 1 and 2, respectively. All the presented scenarios comply with the following condition: $RSSI_1 > RSSI_2$. The receiver “locks” onto a frame if it has received the respective preamble and it is currently in the phase of demodulation and reception of that frame. From this point forward, the receiver considers all the remaining frames in the medium as noise and ignores the interference. Even though Table 7.2 is targeted to the IEEE 802.11a standard, insights can be extracted from this table. The values of SIR proposed for the IEEE 802.11a frame capture feature are going to be considered for the frame capture feature implementation in the MiXiM framework as a starting point, but considering an IEEE 802.15.4 compliant physical layer. Table 7.2 shows that the strongest frame can always be captured. When an interfering frame overlaps the desired signal, if the SIR of the strongest frame is high enough then the receiver is also able of capturing the strongest frame. Since the preamble of the packet is a very important section of the packet when the receiver is in the “lock-on” procedure, the required SIR is higher if $\Delta t < L_{preamble}$. If the receiver is locked onto the weakest frame, the procedure of ignoring this weakest signal (and start receiving the strongest frame) is easy. If the receiver has the capability to receive a signal it means that it is able of suppressing it [SCM⁺08].

The authors from [LKL⁺07] performed experimental work on IEEE 802.11a to obtain the different regions from Table 7.2. In their experiments a testbed was created composed by a receiver, two senders (one normal sender and an interferer) who cannot hear each other. Besides, two extra receivers are considered to monitor the two senders while getting exact timings from the sent frames. Collisions have been induced at the receiver. Three cases can be clearly distinguished:

- Sender First (SF) capture - the strongest frame arrives first (Regions 1 and 2 in Table 7.2);
- Sender Last, Interferer Clear (SLC) capture - the strongest frame arrives second while the receiver is decoding the weaker frame (Regions 3 and 4 in Table 7.2);
- Sender Last, Interferer Garbled (SLG) capture - the strongest frame arrives second while the receiver is still not decoding the weakest frame (Region 5 in Table 7.2).

In the classification of these regions, a distinction is made between the nodes. The sender is the node transmitting the desired frame while the other nodes are named interferers. In [LKL⁺07], it is mentioned that when frame capture effect is enabled the probability of success depends on the data rate and on the signal strength of the strongest frame. However, in the SF case, at a data rate of 6 Mbps almost all the frames can be captured even though the value of the SIR is around 0 dB (both frames present the same RSSI). For higher data rates the required SIR increases. For IEEE 802.15.4, the data rates accounted for are considered low compared to the ones from [LKL⁺07] (6Mbps). Therefore, for each scenario, the required SIR values are lower than the ones considered for IEEE 802.11a in the work [LKL⁺07]. As aforementioned, the work from [FXHZ10] is going to be used as the basis to implement the frame capture feature in the MiXiM framework [WSKW09] from the OMNeT++ simulator [Var10]. In this work, the authors made experiments with the CC1100 radio transceiver, which is similar to the one used in our simulations (i.e., CC2420). However, the former one is not IEEE 802.15.4 compliant and has a maximum bit rate lower than one from CC2420. Moreover, the modulation schemes are different for each one of the radios. Hence, even though the radio transceivers are not the same, the

Table 7.2: Frame Capture regions (data rate of 6 Mbps) [LKL⁺07].

Timing relation	Frame 1 is captured if	Frame which arrives first
1. $\Delta t > L_{preamble}$	$SIR > \sim 0$ dB	1
2. $\Delta t < L_{preamble}$	$SIR > \sim 12$ dB	1
3. $\Delta t < L_{preamble}$	$SIR > \sim 12$ dB	2
4. $\Delta t > L_{preamble}$ receiver locked onto frame 2	$SIR > \sim 10$ dB	2
5. $\Delta t > L_{preamble}$ receiver not locked onto frame 2	Frame 1 might be captured, $SIR \leq 10$ dB Probability increases linearly as SIR increases	2

insights that can be extracted from the work performed in [FXHZ10] have been considered to implement the frame capture feature in our simulator, considering the CC2420 radio transceiver. In [FXHZ10], the authors evaluated the collision behaviour considering five different regions (or scenarios) of packet interference with a packet composed by three sections. Figure 7.2 illustrates these frame capture scenarios, whilst considering a maximum of one interfering frame for different Time of Arrivals (ToA) (time instant when the receivers initiates the reception of the packet). The time intervals φ_1 and φ_2 presented in Figure 7.2 are given in seconds and are defined as $\varphi_1=0.01$ s and $\varphi_2=0.001$ s. These time intervals are considered in the validation of the frame capture effect feature in the OMNeT++ MiXiM framework and allow for verifying the overlap within specific sections of the desired packet. From the analysis of these overlapping sections the receiver signal falls into one of the following three cases: the receiver i) receives the first received signal, ii) discards the first signal and receives the second signal, or iii) discards all packets due to excessive interference.

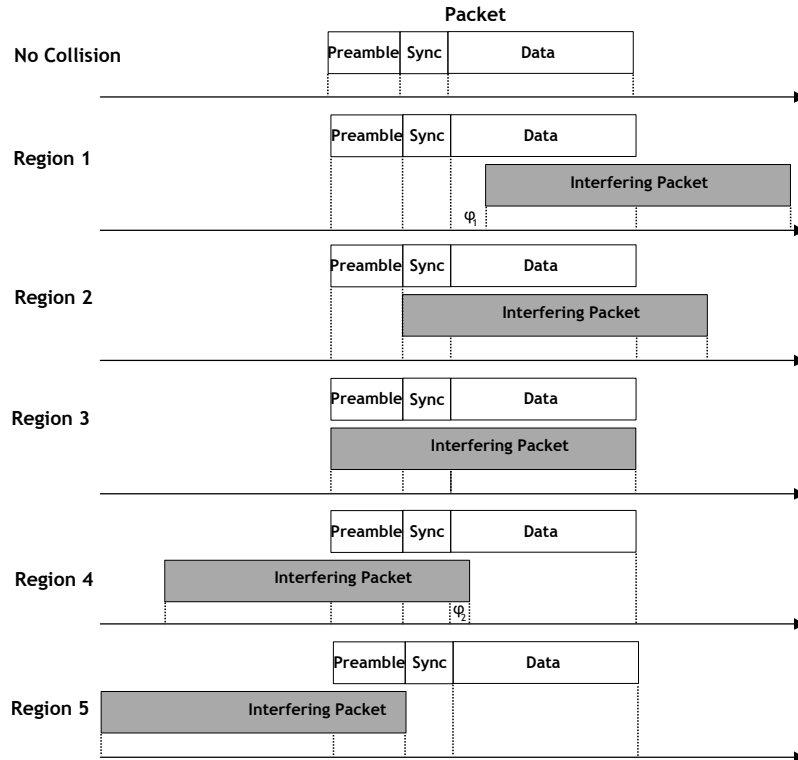


Figure 7.2: Frame capture sections with one interfering frame (interference regions 1-5 are defined by the overlapping between the two frames).

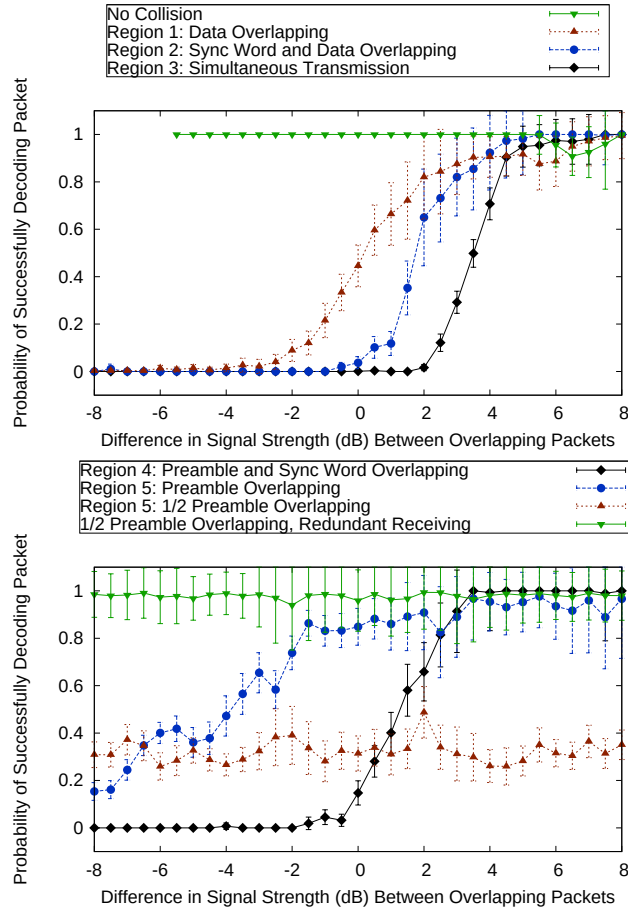


Figure 7.3: The packet reception rates for (a) packets in collision regions 1-3, and (b) packets in collision regions 4-5 (b). The error bars define the estimated 95 % confidence intervals. (extracted from [FXHZ10])

Prior to the the implementation of the FC effect in the MiXiM framework, it was worthwhile to analyze the results obtained by the authors from [FXHZ10]. In the experimental procedure considered in [FXHZ10], two radio transmitters were synchronized with a cable connection, while two transmitters are inducing packet collisions in the different collision regions. In this experimental procedure, the Minimum-Shift Keying (MSK) modulation at 902.1 MHz has been considered, with a 32 bit preamble length, 32 bit sync word length, and 16 bits of data. The differences in RSSI were measured by having each transmitter transmitting a single packet without collision before each collision. The transmission power of one transmitter was varied over time to fill out all the points on the curves, from Figure 7.3. Figure 7.3 shows the probability of successfully decoding the packet under different collision conditions and is divided into two different charts. Figure 7.3(a) shows the probability of successfully decoding the packet when interference starts after the packet begins while Figure 7.3(b) shows the reception rates when interference is at the beginning of the packet transmission. The curve from Figure 7.3(a) shows packet losses during collision region 1, when just the data segment suffers from interference, as well as the effect when exists bit errors during decoding. The curve showing packet loss rates during collision region 2, with the sync word and data overlapping, shows that packet reception begins before the desired packet has a signal stronger than the interfering one. This happens possibly because the radio transceiver locks onto the first signal it detects and thereby misses the strongest packet. The weakest packet presents a higher BER, and will be discarded (due to bit errors), in most cases. The collision region 3 is characterized by simultaneous packet transmission. The successful packet decoding begins to occur when the desired packet is at

about the same RSSI as the interfering packet. Figure 7.3(b) shows the packet reception rates when the interfering packet (with the weakest RSSI) is sent first while the desired packet is only transmitted afterwards, ending the transmission on a clear channel. To achieve a successful packet reception, the sync word must be correctly detected. When the preamble and sync word overlap with the interfering packet (collision region 4), it goes above a 0 % chance of reception when the relative packet signal strength is higher than 0 dB. This happens because, for the considered packet size in [FXHZ10], this packet can draw out the sync word of the previous packet and force the radio transceiver to receive this one instead. For the collision region 5, with just the preamble in collision, slightly different packet reception rates are observed. If the entire preamble is interfered with, packet reception depends on the capability of drawing out the sync word from the preamble of the previous packet and depends also on the packet's RSSI. In Figure 7.3(b) for the curves for the half of the preamble interference scenarios the probability of successfully decoding a packet does not vary as the RSSI varies. The authors from [FXHZ10] state that these losses disappear with redundant receiving (two radio transceivers working in tandem). Since the preamble is not decoded it cannot be corrupted, which means that interference during most of the preamble has little adverse effects upon the packet.

Although the half preamble scenarios are discussed in [FXHZ10], they are not considered in our implementation of the frame capture effect in the MiXiM framework.

Besides the frame capture effect scenarios presented in Figure 7.2 (with only one interferer), the physical layer implemented in the MiXiM framework accounts for similar overlapping scenarios when considering more than one interfering packet. Figure 7.4 presents these frame capture effect scenarios whilst considering more than one interfering packet. Interfering packets numbered from 2 to n are simultaneously transmitted. This way, the physical layer presents a more robust behaviour if a higher number of interfering packets are transmitted.

The time intervals φ_1 , φ_2 and φ_3 presented in Figure 7.4 are given in seconds and are defined as $\varphi_1=0.01$ s, $\varphi_2=0.001$ s and $\varphi_3=0.01$ s. Table 7.3 presents the ToA. Since with more than one interferer regions 4 and 5 are different in the sense how the interfering signals overlap the desired packet, the notion of Time of Ending (ToE) has to be introduced. The ToE is defined as the time instant when a packet ends. For regions 1, 2 and 3 the first packet to arrive at the receiver is the desired one, while in regions 4 and 5 the desired signal arrives after the interfering signal. For all the regions is assumed the time instant when the desired signal is transmitted as a time reference to initiate the transmission of the interfering signals.

The different time instants, ToA_i , $i \in \{1, 2, 3, 4, 5\}$, considered in the evaluation of the frame capture effect collision scenario in the simulator presented in Table 7.3. For example, for region 1 if the desired signal starts at $t_1 = 1.000$ s, then the first interfering packet starts at $t_{start1} = t_1 + ToA_{1a}$, and the second interfering signal starts at $t_{start2} = t_1 + ToA_{1b}$. At the region 4, if the desired signal starts at $t_2 = 1.011$ s, then the first interfering packet must start before the desired signal and end at $t_{end1} = t_2 + ToE_4$, while the second interfering signal starts at $t_{start2} = t_1 + ToA_4$. The region illustrated in Figure 7.5 may happen when the ToAs are not induced. This scenario leads to a strange behaviour at the physical layer. For example, if the first signal to arrive at the receiver is an interfering packet followed by the desired signal arrival and, meanwhile, other interfering signal arrives during the data field of the desired signal a odd behaviour occurs. In this interference region, if the first interfering signal finishes at the time instant of the end of the preamble field, when the receiver considers all the signals present in the channel to compute the different SNRs it does not accounts for the first interfering signal. This happens due to the way how the MiXiM handles the different signals in the channel. When

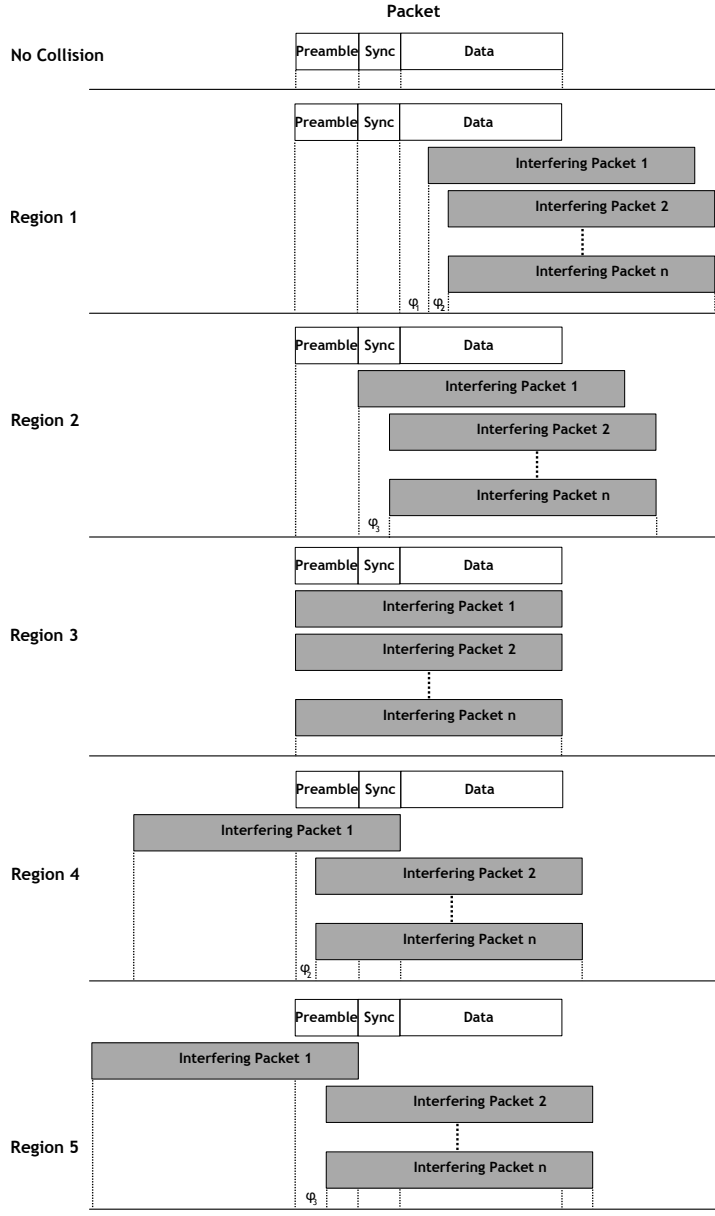


Figure 7.4: Frame capture scenarios with more than one interfering frame for five different overlapping regions.

Table 7.3: Time of arrival (ToA) and time of ending (ToE) of the interfering signals.

Collision Region	1 st interfering packet	2 nd or n th interfering packet
Region 1	$ToA_{1a} = t_{preamble} + t_{sync} + \varphi_1$	$ToA_{1b} = t_{preamble} + t_{sync} + \varphi_1 + \varphi_2$
Region 2	$ToA_{2a} = t_{preamble} + \varphi_1$	$ToA_{2b} = t_{preamble} + \varphi_1 + \varphi_3$
Region 3	Interfering packets are sent at the same time as the desired signal $ToA_{3a} = ToA_{packet}$	Interfering packets are sent at the same time as the desired signal $ToA_{3b} = ToA_{packet}$
Region 4	$ToE_4 = t_{preamble} + t_{sync}$	$ToA_4 = \varphi_2$
Region 5	$ToE_5 = t_{preamble}$	$ToA_5 = \varphi_3$

it checks for the active signals in the channel it only considers the ones that have not ended yet. Therefore, in this example, since the first interfering has already ended it is not taken into account in the computation of the different SNR intervals in the channel. It is assumed that the first interfering signal did not exist and the only interfering signals that exist in the channel

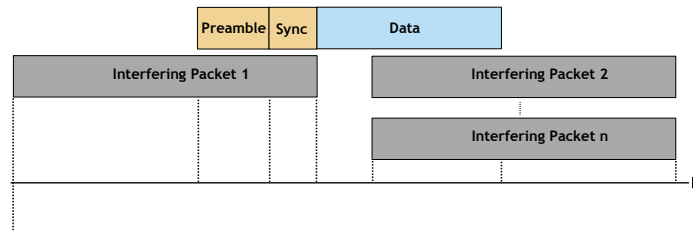


Figure 7.5: Interference region that may happen when times of arrival are not induced.

are the ones that arrived during the data field of the desired signal.

7.3 Potential Impact on the Performance of MAC Protocols

In MAC protocols designed for WSNs, the impact of the frame capture effect is more meaningful if broadcast rather than unicast traffic is considered. In unicast transmissions, it is common to use RTS/CTS and ACK control packets that almost avoids collisions in MAC protocols (excluding the cases of exposed and hidden terminal that can still lead to collisions). In broadcast transmissions, however, packets are not transmitted using the RTS/CTS mechanism. Besides, no acknowledgement is sent after reception.

Reference [WWJ⁺05] is one of the first works that have exploited the advantages of a system that is able to capture frames even when overlapping occurs. In this work, the impact of being able to detect or recover from a collision with frame capture is high. In TDMA mediation schemes, such as Flexible Power Scheduling (FPS) [HDB04], the receiver or parent node is the one responsible by the scheduling of the transmissions. A parent notifies which slots are available to receive data. All transmitters that intend to gain access to a particular slot must contend to reserve it. If the transmitter receives an ACK the slot is assigned to it and the remaining nodes will have to wait for the next round of slot assignments (to contend again). With the frame capture effect feature, this TDMA based scheme must be able to reduce the time a transmitter takes to have a slot assigned by the parent. If the parent can recover the ID of the losing node, it can send an ACK to the node that won a particular slot and a second message to the node that lost the pairing with the parent, to indicate that it must use a different available slot. With this improvement, the losing node is able to associate itself with the parent in a single try. Nevertheless, even if the transmitter associates itself with a parent it can regularly lose packets (due to collisions from neighbouring cells) and may be forced to use a different slot. By employing the FC effect feature, the parent can differentiate between collisions and normal packet losses. Then, it can send an ACK to the transmitter when the packet is received successfully, a NACK when the packet collides and nothing if no packet is received. If the transmitter receives many NACKs, it knows that a nearby cell is interfering and it must try a different slot. If it receives neither ACKs nor NACKs, it can infer that it has an unreliable link with this parent and no slot will be reliable for communication. The solution is to try and associate with a different parent. This way, the the transmitter knows what behaviour the nearby nodes have (in terms of choice of slots). With this technique, collision detection information is provided to the receiver where it is required, in both of applications described above. The ability to differentiate between packet losses and collisions and to identify nodes that caused the collision improves both applications at no extra cost. This information can be used for many other existing protocols.

The authors from [FXHZ10] also propose some recommendations for capture-aware MAC pro-

protocols in WSNs. The convergecast system used in their experiment can be applied to perform tracking and localization passive mobility detection, intrusion detection, and radio interferometry systems. This is only possible due to the characteristics of the latter systems, which do not need a 100 % packet success rate, yet they do require frequent and regular transmissions. Moreover, if time division MAC protocols employ the capture-aware features in PHY layer, although the nodes still use channel sensing the frame capture gives a new capability. The transmitter is capable of deciding when to transmit depending upon the interference. It transmits if the probability of correctly receiving its packet is high enough.

It has been shown by the authors from [AZM10] that throughput can increase up to 430 % for the worst performing implementation of the FC effect. In [AZM10], only infrastructured wireless networks have been simulated. The authors from [FXHZ10] have shown that the MAC protocol with the frame capture feature is able to significantly reduce packet collisions. An increase in fairness is also achieved when compared to a multi-channel approach. Those authors have also obtained a decrease of packet losses by about 7.1 %. Other authors, e.g., authors from [GBV10], have shown that frame capture implemented in a IEEE 802.15.4 compliant physical layer and with the beacon-enabled mode of IEEE 802.15.4 CSMA/CA MAC protocol, a maximum of 20 % gain achieved in packet delivery success. Therefore, the frame capture effect will also certainly be very beneficial in terms of throughput and packet delivery ratio to the MAC layer whilst allowing to infer the number of neighbouring nodes when this feature is implemented in the MiXiM framework [KSW⁺08] of OMNeT++. These possible outcome are shared for both unicast and broadcast traffic scenarios.

7.4 Implementation of the Frame Capture Effect

7.4.1 Frame Capture Effect in Simulators

The frame capture effect behaviour has been fairly documented for IEEE 802.11a and IEEE 802.11p wireless communication systems. However, it is not a common feature in many wireless network simulators yet, namely WSN simulators. There are some simulators that try and simulate this effect, such as the ones for infrastructured networks (not for mobile or ad-hoc ones), or it is implemented in a way that does not reflect all possible scenarios identified by the authors from [LKL⁺07]. Some authors implemented all the scenarios from [LKL⁺07]. However, in the current work, the intention is to implement the various scenarios presented in Figures 7.3 and 7.4. QualNet and ns-2 [KVSA04] have the frame capture feature implemented on them. However, the latter is intended only for the IEEE 802.11 standard, while the former one is only available commercially. Besides the aforementioned simulators, the Yet Another Network Simulator (YANS) [LH06] also has the frame capture effect capability, but only for IEEE 802.11 wireless communications systems.

Since OMNeT++ is the elected simulator and there is no frame capture feature available in it, this work also aimed at expanding the MiXiM framework [KSW⁺08] in order to support the frame capture feature with the modulation schemes of the IEEE 802.15.4 standard.

In light of these facts, there is a lack of availability of simulators dedicated to WSNs with the frame capture feature implemented in them. The majority of the simulators does not include this feature or it only covers some frame capture effect scenarios. Most of the simulators present fairly accurate methods for BER computation, although they only consider Additive White Gaussian Noise (AWGN) channels. In this work the objective is to implement the frame

capture effect within the physical layer of the MiXiM/OMNeT++ framework. Moreover, unlike some mentioned simulators, the MiXiM framework allows for choosing a different channel model (besides the AWGN model), such as the Rayleigh channel model. The implemented frame capture regions cover almost all the possible scenarios with overlapping frames.

7.4.2 Physical Layer and Decision on Airframes

This section discusses the physical layer from the MiXiM framework. The following description applies to the current, unmodified implementation of MiXiM physical layer [KSW⁺08], without any modifications required to support the frame capture. The main objective of the physical layer in MiXiM is to send and receive frames, applying the channel effects, by modelling, collision detection and bit error computation. Details on the environment models and path loss models from MiXiM are found in Appendix E. Figure 7.6 presents the different classes that are handled by the physical layer. From all the physical layer classes presented in Figure 7.6 the *BasePhyLayer* is the most important one, as it delivers all the basic functions, such as message handling from the MAC layer, and is able to call other functions and classes. Other important class is the *AirFrame*, which holds the class for a *Signal* that is exchanged throughout the input and output gates within the simulator. Various information attributes can be stored in the *AirFrame* class, such as the start time (time instant when the transmission started), end time (time instant that corresponds to the end of the signal), or the ID from the node that has sent the *AirFrame*.

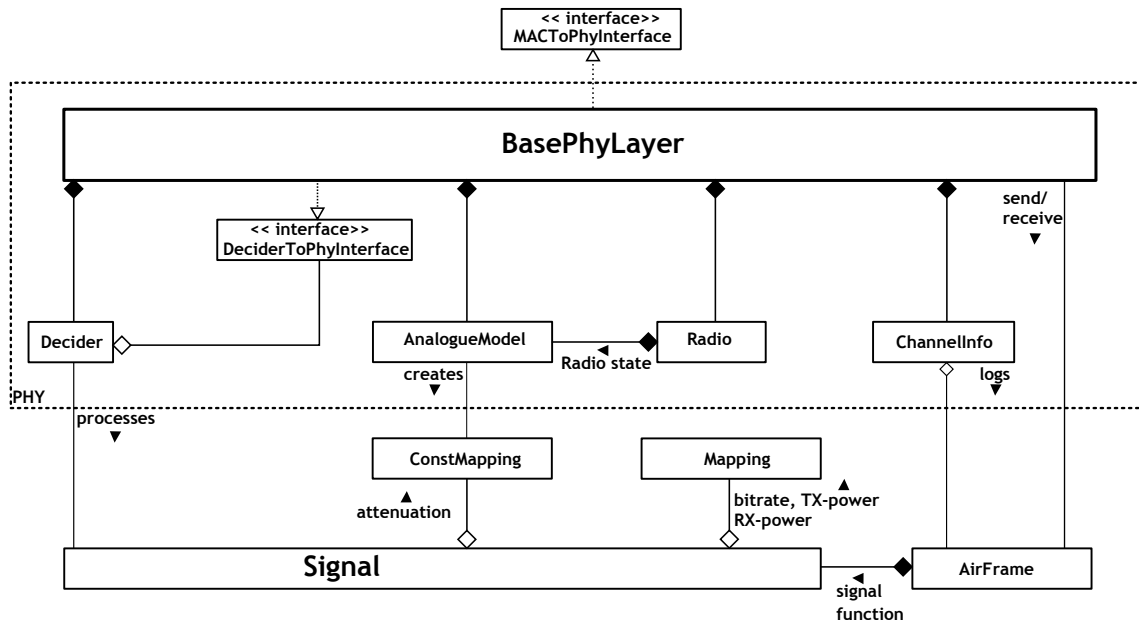


Figure 7.6: MiXiM physical layer diagram (extracted from [WSKW09], Figure 2).

The *ChannelInfo* module is responsible for managing the *AirFrames* specific to the node on the channel. This module knows, at any moment, which *Airframes* are currently being transmitted and which ones have already ended their transmission. It utilizes its active and inactive flags to mark the *AirFrames*, functionality that is further explored ahead.

As soon as an *AirFrame* arrives at the receiver, its encapsulated signal occupies the medium for a given time and is added to the *ChannelInfo* object and is considered as active until it ends. The *ChannelInfo* object keeps a record of all the information regarding the *AirFrames* that are currently being received, as well as the *AirFrames* that are currently interfering with

an ongoing frame reception. Besides, it also stores information on *AirFrames* that might have already ended but interfered with (some part of) an *AirFrame* that is currently being received. Once the *AirFrame* ends, it becomes inactive for the *ChannelInfo* object but it is still kept as an interfering *AirFrame* until there is no more active *AirFrame* overlapping with it in time. The *AirFrames* must be kept in order to allow calculation of the SNIR of a specific *AirFrame* (the desired one) while all other *AirFrames* on the channel are considered as interference. The *ChannelInfo* is able to supply to the Decoder module all the different intervals of SNIR, depending on the different overlapping *Airframes* that coexist in the channel.

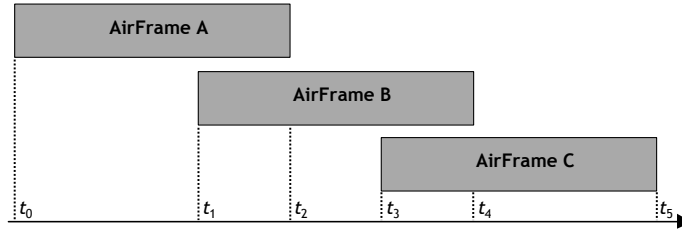


Figure 7.7: *AirFrames* on the shared channel (adapted from [WSKW09]).

Considering the example from Figure 7.7, where the *Airframes* A, B and C start one after another, the following events are observed at the following time instants:

- t_0 : A starts and is active;
- t_1 : B starts and is active;
- t_2 : A finishes and becomes inactive, but is not yet deleted from the *ChannelInfo* due to the overlapping with B, which is active;
- t_3 : C starts and is active;
- t_4 : B finishes and becomes inactive but is not yet deleted from the *ChannelInfo* due to the overlapping with C, which is active. A is deleted since it does not overlaps with any active *AirFrame*;
- t_5 : C finishes and is deleted from the *ChannelInfo* since there is no active *AirFrames*. B is deleted since C is inactive.

In the example from Figure 7.7 the intention is to receive the *AirFrame* B to be evaluated by the *Decider*. To calculate the SNIR properly, the *AirFrame* B as well as the interfering *AirFrames* A and C have to be taken into account and handled by the *Decider* module. Since the *Decider* module decides whether a signal should be received or not, the *ChannelInfo* does not delete an *AirFrame* as long as there is another active one overlapping in time. In the example from Figure 7.7 A is not deleted as long as B is active.

As mentioned at the end of Section 7.2, due to this procedure, the *AirFrames* are kept and deleted in the *ChannelInfo* object and may cause the interference region presented in Figure 7.5. This may happen because of the time instant when the desired *AirFrame* is evaluated. As in the example from Figure 7.7 if the objective is to receive the *AirFrame* B and since the *Decider* only decides whether the *AirFrame* B is successfully received or not at time t_4 , the *ChannelInfo* only classifies *AirFrame* C as the only interfering *AirFrame* present in the channel. Yet, the *AirFrame* A is considered as if it has never arrived at the channel.

Every *AirFrame* has an encapsulated physical *Signal* (sent over the wireless medium). The *Signal* is created at the MAC layer and is affected by the channel effects of the receiver, called

AnalogueModels. These models influence the signal according to the wireless environment where it is transmitted. They create *Filters* (or *Mappings*), which are applied to the *Signal*, simulating the path loss of a real signal. Different types of *AnalogueModels* can be chosen in the MiXiM framework:

- *SimplePathLossModel* - This is a simple implementation that adds a path loss filter to the signal. It models the Friis equation for various path loss exponents;
- *LogNormalShadowing* - It is a model that describes shadowing using a log-normal distribution;
- *JakesFading* - This is an implementation of the Rayleigh fading model based on summing sinusoids;
- *Indoor and Outdoor IEEE 802.15.4* - These are two models described in the IEEE 802.15.4 standard for indoor and outdoor scenarios.

The *Decider* is the module responsible for the evaluation whether the *AirFrame* is received or not. It evaluates the received *Signals* whilst calculating the BER, which includes the distinction between the ones that are assumed as interference and the ones that are assumed as the desired signal. Another task of the *Decider* is the evaluation of the channel, i.e., it performs carrier sensing and reports the channel state to the MAC layer. Each *AirFrame* is handled several times by the *processSignal()* method of the receiver *Decider*, as illustrated in Figure 7.6. The number of times it is processed depends upon the implementation of the *Decider*.

The *Decider* work flow is the following one:

- At the time of the reception of the first bit of an *AirFrame*, the *Decider* has to determine at which point in time it can decide whether the packet should be treated as noise or not, and return this time-point decision to the physical layer. Normally, the time to determine whether to receive an *AirFrame* or treat it as interference is performed immediately after the physical layer preamble is completely received and after receiving the last bit of the packet. Nevertheless, the *Decider* can make the decision at anytime;
- Then, the next time the *Decider* receives the *Signal* to process it, it has to decide whether the *AirFrame* should be considered as interference or it is the desired signal to be received. This evaluation is performed by evaluating the *SNIR-Mapping* at the current time instant (end of the preamble or/and end of the packet). To achieve this goal, it requests from the *ChannelInfo* object all the overhearing signals within this time interval. The *Decider* computes the RSSI of the desired signal in that time interval and obtains the SNIR by dividing the received power of the desired *AirFrame* signal by the interference mapping for the same time interval. The *Decider* has a special feature that allows for signalling the *AirFrames* as interference with a flag that indicates to the physical layer the intention of not receiving this *AirFrame* again for processing. Otherwise, if the intention is to receive correctly the *AirFrame*, then the *Decider* returns the end of the signal to the physical layer as the next point in time it wants to process the *Signal*;
- After completely receiving the *AirFrame*, the *Decider* has to compute the BER for the desired signal. To achieve this goal, it has to create a *SNIR-Mapping* but this time, for the entire *Signal* duration. It considers all the overlapping intervals from the interfering *AirFrames* with the desired *AirFrame* signal;

- In the simplest case, the SNIR is checked against a given threshold and the *AirFrame* is considered lost if the threshold is exceeded. Another option is to determine the BER based on bit error curves. The latter option is the one considered in the frame capture effect implementation, with some modifications;
- After the *Decider* determines that the *AirFrame* is correctly decoded, the packet is encapsulated and sent to the MAC layer together with a *DeciderResult*. The *DeciderResult* contains the evaluation data for the MAC packet (packet lost/correctly received, number of bit-errors, etc). Otherwise, the packet is encapsulated and sent by the internal control channel to the MAC layer with a flag signalling bit errors in the received packet. The encapsulated packet sent by the control channel is only meant to indicate at MAC layer level that a packet was received in the physical layer, but it was not possible to decode it properly [WSKW09].

The *Decider* is one of the most important parts we need to adapt in order to implement Frame Capture in the MiXiM framework. This is because the *Decider* processes every received frame. Within the Decider, the algorithm that checks the RSSI of new arriving frames compares it to the RSSI of other frames, and performs a capture decision if needed. Besides, it can discard a packet that was already lock onto the receiver whilst locking to a new one (stronger signal).

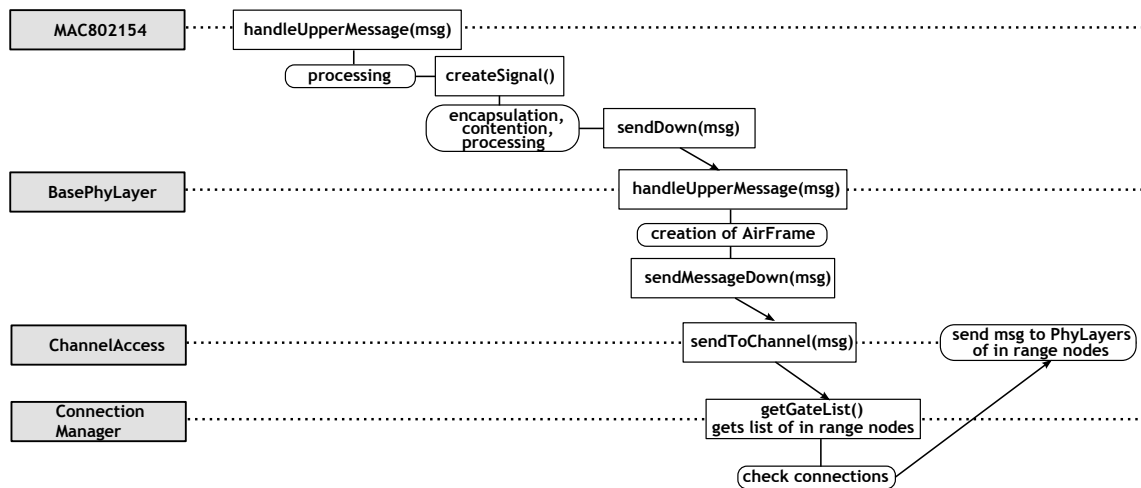


Figure 7.8: MiXiM physical layer TX flow diagram (adapted from [WSKW09]).

Figure 7.8 shows the flow diagram for the transmission events. The events take place as follows:

1. The application layer of the nodes generates a packet and sends it to the lower layer, until it reaches the MAC layer;
2. When the frame arrives to the IEEE 802.15.4 MAC layer, it performs the basic processing. It creates the *Signal* object with some control information, attaches this information to a *Mac802154Pkt* packet, which contains the data to be sent. Then, the *Signal* is encapsulated and sent to the lower layer (physical layer);
3. As soon as the physical layer (*BasePhyLayer*) receives this packet it creates an *AirFrame* object, which is the physical representation of the frame, and contains the *Signal* and the data. Note that the data is not included into the *Signal*. The *Signal* only carries the control information, such as bit rate, transmitter power, and time duration of the frame. The *Signal* is contained within the *AirFrame*;

4. The *ChannelAccess* class obtains from the *ConnectionManager* a list of nodes connected to intended node, which is obtained from a verification based on the locations of other nodes and objects. The *ChannelAccess* delivers the *AirFrame* to the input gates of the physical layers of the reachable nodes. Propagation delay can also be simulated. In this case, OMNeT++ runs a self-timer that adds a delay to the *AirFrame* delivery at the input gate.

The events involved in the reception are represented in Figure 7.9 as follows:

1. As soon as an *AirFrame* arrives at an input gate it is handled by the *BasePhyLayer* module, which, in turn, calls the *handleAirFrame()* method. The *AirFrame* has three possible states (NEW, EXPECT_HEADER and EXPECT_END). The *AirFrame* is passed on to another method depending on which state it currently is. As mentioned earlier, the *AirFrame* can be processed multiple times, so that the receiver does not have to decide in a unique decision what to do with the frame;
2. When the *AirFrame* is handled by the *BasePhyLayer* the first time, it is added it to the *ChannelInfo* information while an attenuation is applied to the *Signal* defined by the chosen *AnalogueModel*. Then, the *AirFrame* is passed to the *Decider*. If the *AirFrame* comes back to the *BasePhyLayer* for the second time, it is passed to the *Decider* immediately, without passing by the previous steps;
3. The *Decider* checks if the *AirFrame* has been treated or not in a earlier stage. The current *Decider* implementation has three main moments when it expects to see the *AirFrame* and the *Signal* in it: i) when the frame arrives, ii) when preamble ends, and iii) when it ends receiving the *AirFrame*. This behaviour must be expanded in order to enable the frame capture feature during and after preamble reception, and at the end of the receiving of the *AirFrame*;
4. To achieve this goal, the current MiXiM implementation of IEEE 802.15.4 has three methods: *processNewSignal()*, *processSignalHeader()* and *processSignalEnd()*;
5. To begin with, the *Decider* verifies if there are collisions and checks whether the RSSI of the signal is strong enough to be received. Then, it returns the next handling time from the simulation when it intends to receive the frame for a second evaluation. If this time is lower than zero, the frame can be discarded immediately. Otherwise, if this time is different from zero, it means that *BasePhyLayer* and *Decider* evaluate the frame again later;
6. The current implementation returns the *Signal* preamble end time instant (the time when the reception of the preamble has been completed) as the time it intends to evaluate the frame again. The method that returns this time is called *processNewSignal()*;
7. When the *processSignalHeader()* method is called, it checks if the preamble has a sufficiently large RSSI value (against the instantaneous interference), in order the receiver is able to lock on to the frame (i.e., synchronize the frame within the receiver). If the receiver decides to lock on to the frame, the *processSignalHeader()* returns the next handling time as the next time it intends to evaluate the frame again. In this case, the frame is going to be handled at the end of the *AirFrame* reception. Otherwise, if the frame is not synchronized the method returns zero as the next handling time instant, which causes to directly discard the current frame;

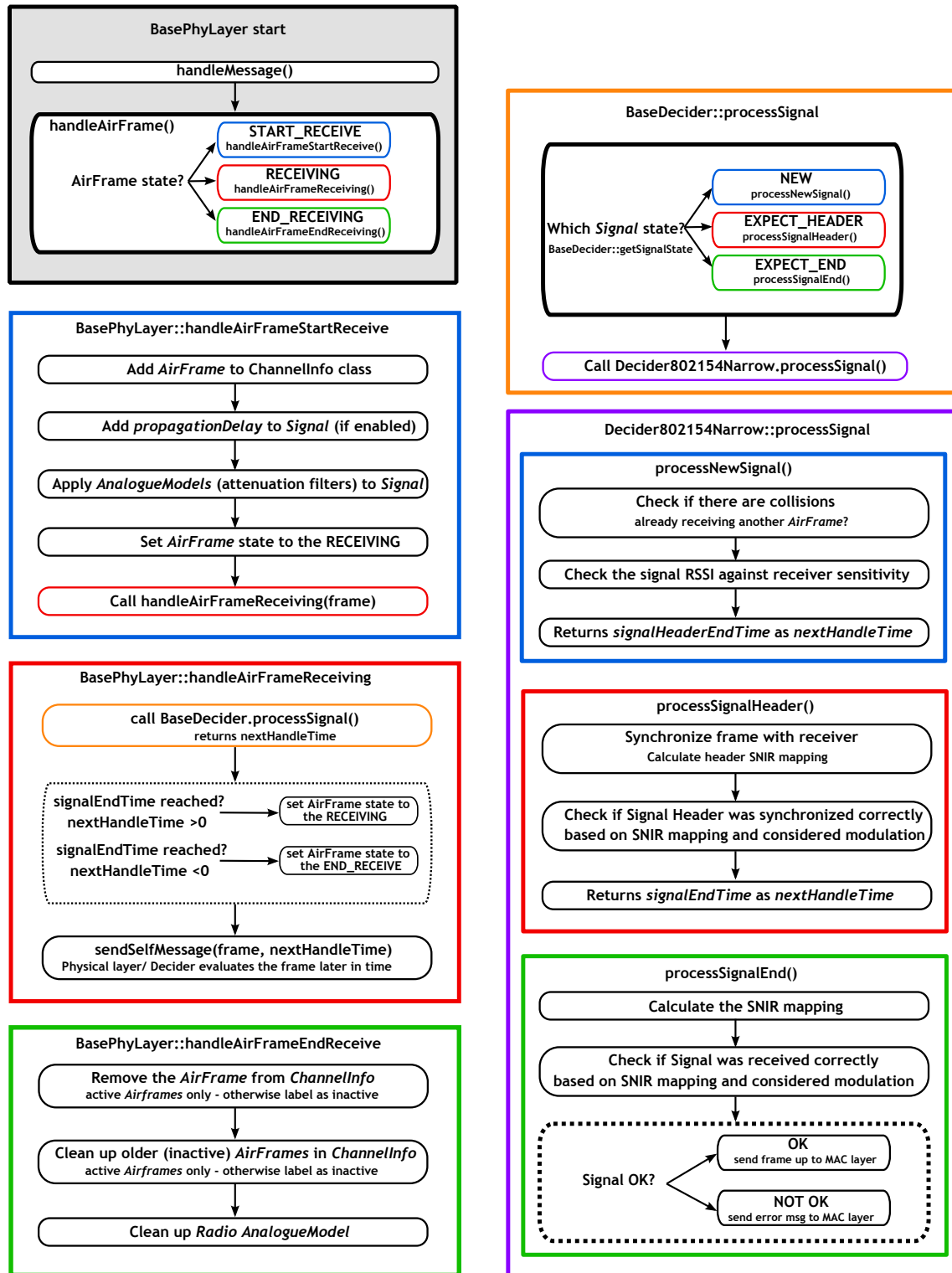


Figure 7.9: Flow diagram for the MiXiM reception layer. The colours from the blocks show the functionality called at each phase.

- At a later point in time, when `processSignalEnd()` is called, it evaluates definitely if the frame has been received correctly or not. It calculates the *SNIR mapping* based on the *AirFrames* registered in *ChannelInfo* class (through *BasePhyLayer*), the RSSI of the *Signal*, and decides based on the SNIR (during the frame reception) if the frame may be received correctly or may contain errors. This phase is going to be further developed ahead,

because some modifications have to be made to account the frame capture feature in MiXiM;

9. If the *AirFrame* has been decoded correctly, the *Decider* encapsulates the *AirFrame* and passes it to the MAC layer. Otherwise, it encapsulates the *AirFrame*, adds a flag that marks bit errors in the *AirFrame* and sends it throughout the control channel to the MAC layer.

7.4.3 IEEE 802.15.4 BER Calculation

In the default Decider implementation, the computation of the bit error rate is based on the IEEE 802.15.4 physical layer [IEE06]. The effect of the interfering signal on the desired signal is assumed to be similar to AWGN at 2.4 GHz. The 2.4 GHz PHY specified for this standard uses a quasi-orthogonal modulation scheme, where each symbol is represented by one of 16 nearly orthogonal PN sequences (OQPSK-16). This is a power-efficient modulation method that achieves low SNR and Signal-to-Interference Ratio (SIR) requirements at the expense of a signal bandwidth that is significantly larger than the symbol rate.

The BER is calculated by Equation 7.1.

$$BER = \frac{8}{15} \times \frac{1}{16} \times \sum_{k=2}^{16} -1^k \binom{16}{k} e^{(20 \times SNIR \times (\frac{1}{k} - 1))} \quad (7.1)$$

In Equation 7.2, PSR is the packet success rate, which is the probability that the frame has no errors, while $nBits$ is the length of the frame (in bits).

$$PSR = (1 - BER)^{(nBits-1)} \quad (7.2)$$

Equation 7.3, allows for computing the Packet Error Rate (PER) for the entire packet:

$$PER = (1 - PSR) \quad (7.3)$$

Figure 7.10 shows the bit error rate as a function of SNIR for the IEEE802.15.4 link layer, as calculated by the MiXiM framework simulator. In the simulator it is assumed that the values of SNIR which correspond to values of BER lower than 1×10^{-8} are assumed to be always 1×10^{-8} . The curves for the packet error rate from Figure 7.11 are the numerical solution of Equation 7.3. Different values are considered for SNIR and the packet length, namely 64 and 336 bits. It is observed that, as the value of the SNIR increases the power of the signal becomes higher than the power of the noise while the PER decreases, as expected. For larger packet lengths the PER values are always higher.

In the previous implementation of the *Decider* with the IEEE 802.15.4 standard, when the end of the *AirFrame* reception is attained the *Decider* evaluates definitely if the frame has been correctly received or not. Figure 7.12 shows a scenario with one interfering node. It considers frames F_0 and F_1 and shows the procedure for *SNIR Mapping* employed in the physical layer of MiXiM.

For demonstration purposes of this procedure it is considered that packet length is 400 bits, $RSSI_{F_0} = 3.81997 \times 10^{-6} \text{mW}$ (-54.18 dBm) and $RSSI_{F_1} = 6.7339 \times 10^{-7} \text{mW}$ (-61.70 dBm). The

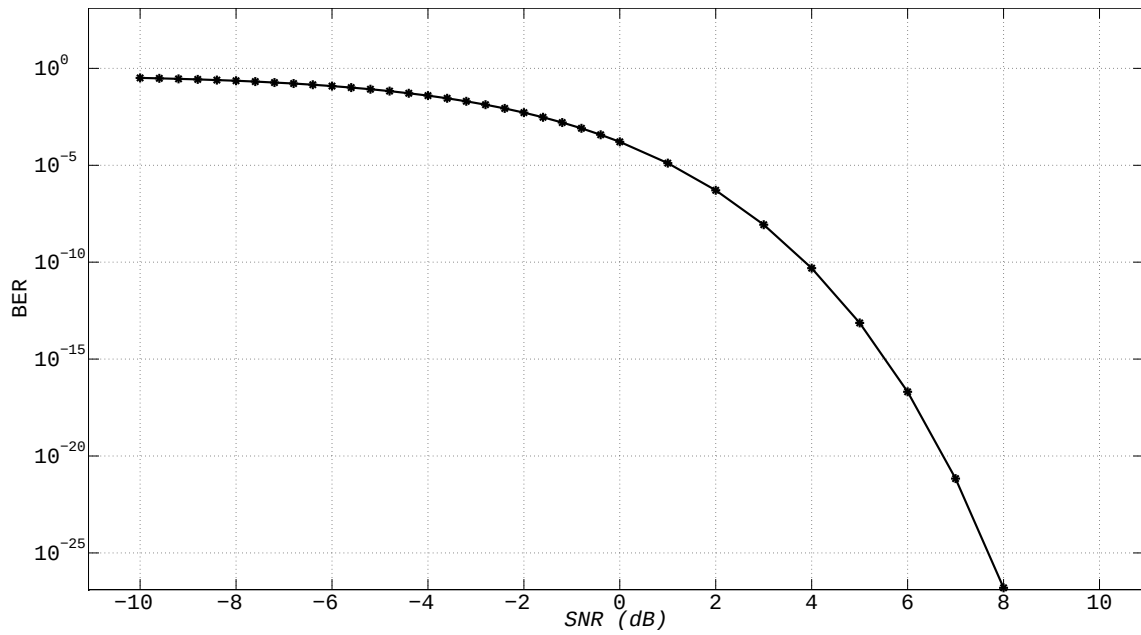


Figure 7.10: BER results for IEEE Std 802.15.4.

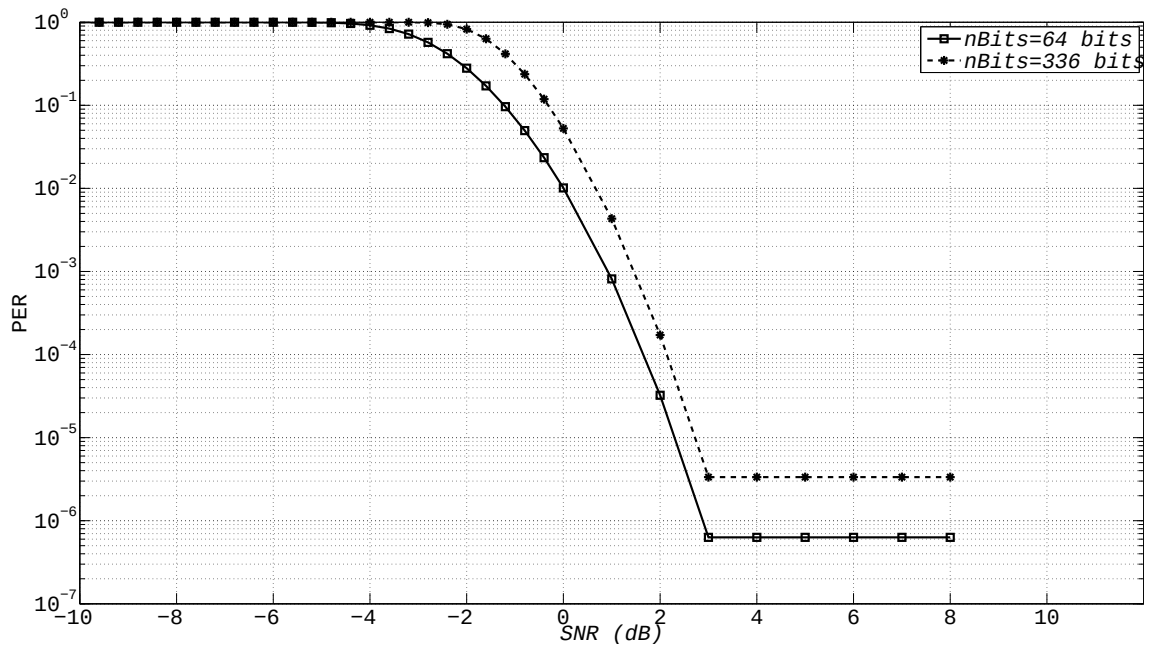


Figure 7.11: Results for PER for the IEEE Std 802.15.4 link layer and packets with 64 and 336 bits.

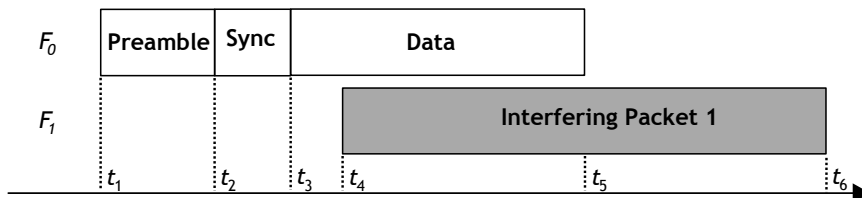


Figure 7.12: SNIR Mapping procedure in the IEEE 802.15.4 physical layer of MiXiM.

thermal noise is constant and is assumed to be $N_0 = -110$ dBm.

The receiver node computes the *SNIR Mapping* as follows:

1. The receiver gets the list of all *AirFrames* that were added to the *ChannelInfo* object, in

Table 7.4: RSSI, Noise and SNIR mappings in dBm.

Time Interval	Mapping		
	RSSI [dBm]	Noise [dBm]	SNR [dBm]
$[t_1; t_2[$	-54.18	-110	55.82
$[t_2; t_3[$	-54.18	-110	55.82
$[t_3; t_4[$	-54.18	-110	55.82
$[t_4; t_5[$	-54.18	-61.70	7.52
$[t_5; t_6]$	-54.18	-61.699	7.519

order to compute all the required mappings for the SNIR computation;

2. Depending on the overlapping of frames, different intervals can be identified as well as the mapping associated with each of the intervals. In the example from Figure 7.12 (with one interfering node) the receiver identifies five intervals when it gets the list of all *AirFrames*;
3. The receiver iterates all the five intervals from Table 7.4 and calculates the corresponding value for the BER for each interval and the given mappings, namely for the RSSI, noise and SNIR. These mappings are given in Table 7.4 for the considered example;
4. In each iteration (each interval) the receiver calls the *getBERFromSNR(snr)* method while calculating the PER for the corresponding SNIR with the matching number of bits that are being analyzed;
5. The value of the PER obtained in each iteration is compared with a uniformly generated random variable between zero and one. If the PER is lower than the random variable then this section of the packet is decoded without any error. Otherwise, if the value of the PER is higher than the random variable then this section of the packet is corrupted and causes immediate packet discard, without analyzing the remaining sections of the packet (if they exist). If there are more iterations to perform, the receiver repeats the BER calculation procedure for the next interval;
6. Basically the receiver verifies all the intervals of the packet with different SNIRs, calculating the values of BER and the corresponding values of the PER. As the algorithm moves from one iteration to another, if there is a value of PER higher than the random variable then the packet is immediately discarded.

Coding and error correction codes are not implemented in the simulator yet. The method for bit error rate calculation from the current *Decider* is going to be maintained. However, the way how the *Decider* evaluates if the section of the packet is received with success or not needs to be updated. The values of the PER against the uniformly distributed random variable (from the default *Decider*) does not meet the frame capture requirements. As a modification is needed aiming at meeting this requirements. The improvements in the simulator are going to be discussed ahead.

7.5 Reliability Concept and Decision Thresholds in FC

As described in Section 7.4.2, in the physical layer from the MiXiM simulator, each frame that arrives at the receiver is analyzed by the *Decider*. The *Decider* is responsible for the evaluation

of whether the frame is correctly decoded or not. To perform this evaluation, the *Decider* checks the channel, the frame's SNIR while iterating throughout the different sections of the frame, to check if there are any corrupted bits. If no corrupted bits are found then it sends the frame upwards to the MAC layer. The *Decider* is also responsible for the management of the current frame. The current frame is the one that the receiver is currently locked onto (i.e., synchronized).

The default *Decider* for the IEEE 802.15.4 standard has a form of frame capture already implemented. When a frame is received and the receiver locks on to it, if any other frame arrives during the frame's ongoing reception, the newest frame is ignored. However, this behaviour is only a part of what the frame capture feature is. It only capture frames that arrived first. As a consequence, this behaviour was upgraded to also account for the other frames that arrive during the preamble of the first frame, as described in frame capture scenarios from Section 7.2. The upgraded *Decider* needs to make a decision about which frame the receiver should lock onto, based on the current frame and the SNIR of the new frame. This *Decider* is going to decide between the first two received frames while the remaining ones are considered as interfering frames. This decision is easily explained by considering a scenario with several frames that are sent sequentially and temporarily separated from each other, with the newest frame signal strength always increasing, in such a way that the *Decider* would be continuously changing the frame that decides to lock onto. Limiting the behaviour of the *Decider* to evaluate only the first two received frames decreases the time needed to receive the frame with strongest signal. The additional behaviour required to achieve the frame capture is given below. The reception behaviour that needs to be implemented is given as follows:

- If a new frame arrives, the *Decider* temporarily stores the frame and makes no decisions about receiving it or not. It waits until the preamble of the frame has been completely received;
- After receiving the preamble, the *Decider* tries to lock onto the frame;
- Three procedures are performed by the *Decider* before enabling the frame capture feature. First, it checks which one of the frames has the highest signal (if more than one frame is received). The one with the strongest signal is the current frame while the other one is the interfering frame. Then, based on the frame classification according to the signal strength it decides on which collision scenario it corresponds to. Finally, according to the chosen collision scenario, it chooses which capture decision threshold is going to be used as the comparison threshold;
- The different collision scenarios and the corresponding frame capture decision threshold are as follows:
 - If there is no other frame being received in specific time instant and there was no interference during the reception of the preamble, the normal reception threshold is used (collision scenario 0, as in the default *Decider*). In this scenario since there is only one single frame, it is assumed as the current frame;
 - If the receiver is currently receiving another frame and it receives a new frame during the data field, the “locked” capture threshold is considered (-0.3 dB). This scenario corresponds to either the collision scenario 1 or collision scenario 4, depending on which frame has arrived first. If the strongest frame arrives first (and

only then a weaker frame arrives), the *Decider* assumes the collision scenario 1. Otherwise, if the strongest frame arrives later than the weakest frame the *Decider* assumes the collision scenario 4;

- If there is no other frame being received in that time instant but there was interference during the preamble, the “garbled” capture decision threshold is used (0 dB). This scenario corresponds to either the collision scenario 2 or collision scenario 5, depending on which frame arrived first. If the strongest frame arrives first (and only then a weaker frame arrives), the *Decider* assumes the collision scenario 2. Otherwise, if the strongest frame arrives later than the weakest frame the *Decider* assumes the collision scenario 5. On the one hand, in the collision scenario 2 a frame (the interfering one) begins in the end of the preamble reception. On the other hand, in the collision scenario 5, the interfering frame ends exactly during the preamble of the current frame (the strongest signal);
 - If two frames arrive “simultaneously” the receiver assumes that the frame with the strongest signal is the current frame whilst considering the other frame as the interfering one. This scenario corresponds to the collision scenario 3, in which the “simultaneous” capture threshold is considered (0 dB). This threshold is the same as the “garbled” capture decision threshold since this OQPSK-16 modulation scheme considered in MiXiM is tolerant relatively to interference with frames in overlapping scenarios;
 - If the first two frames have the same signal strength the simulator assumes that a true collision has occurred. However, in [GBV10], the authors claim that a packet has 99.9 % of probability of correctly being received if the frame capture feature is implemented in the physical layer. Therefore, in our upgraded version of the *Decider* there is the option of assuming that even with frames that present the same signal strength, one of the frames can be captured;
- The aforementioned considerations are based on the collision scenarios presented in Figure 7.2. However, this upgraded *Decider* has the capability of receiving more than two frames and decide on which frame is going to be captured. The *Decider* either assumes that beyond the second received frame it considers those frames as interference and adds all these frames to the noise mapping. Therefore, the new *Decider* also accounts for collision scenarios like the ones presented in Figure 7.3. This is a complex part of the new *Decider*, because the mappings (RSSI, Noise and SNR) must be performed in a different way than in the default *Decider*.
 - Then, if in some of these scenarios the receiver identifies the need to use frame capture, it has to unlock from the weakest signal and lock onto the strongest signal if the SNIR exceeds the corresponding frame capture decision threshold. If the SNIR is not high enough the frame is discarded (and seen as interference for the remaining duration of the frame);
 - If the *Decider* employs frame capture it requests to verify the frame again after receiving the preamble as well as after the full packet reception is complete. During the reception of the different parts of the packet, the *Decider* evaluates if any of the collision scenarios is adequate. If the *Decider* verifies that it needs to discard a frame and accepts a new one (with a stronger signal) it has to invert the roles, in order to receive the strongest signal;

- When the intended frame is received completely, the SNIR of the frame is computed as usual (dividing the frame's signal strength by the cumulative signal strength of all the interfering signals plus the thermal noise). Then for the corresponding SNIRs and lengths of the packet's sections, the BER equations are applied to calculate the frame error probability. These equations for BER and PER allows for forecasting the probability of correcting receiving a frame. As discussed earlier, the procedure followed by the default *Decider* to perform the final decision of accepting the packet (or not) is based on the comparison of a random number with the obtained PER value. If the generated random number is lower than the value of the PER, the frame is received correctly, if the value of the PER is higher than the drawn number, the frame is considered lost.

Note that the latter aspect is already present in the current *Decider* implementation. However, it does not reflect the best way to decide whether a packet is received with success or not. After running the simulation with the default *Decider* implementation (with the different collision scenarios) and collecting sufficient data from the simulator some conclusions can be extracted concerning the distribution of the value of the values of the BER obtained for successful and corrupted packets.

7.5.1 Enhanced Reliability Decision Algorithm in the Decider

The default *Decider* implementation employs an algorithm, that enables to decide if the frame is correctly decoded or not. This algorithm performs the final decision of accepting the packet or not, based on the comparison of a number randomly generated with the value obtained for PER. If the drawn number is below the value of the PER, the frame is considered to be received correctly. However, if the value of the PER is higher than the drawn number, the frame is considered lost.

Some simulations have been performed considering that this algorithm is the one that facilitates to decide the reception of the frame. These simulations have been performed for the collision (frame capture) scenarios shown in Figure 7.2 and allows for extracting the number of packets received with success and the discarded packets along with the corresponding values of the BER and PER. After plotting the PER as a function of the SNIR for the successful and discarded packets, it is evident that, for the same PER (same BER and packet length) the packet may be either received with success or discarded. This occurs because of the randomly generated numbers, which acts like a “blind” decision algorithm. It does not take into account if the conditions are the same, i.e., equal value of BER and packet length may cause the packet to be discarded sometimes and other times to be accepted. Therefore, to maintain this decision algorithm jointly with the (previous) implementation of the frame capture effect would lead to unexpected results or even worse results than with the default *Decider* implementation.

To sort this issue out the *reliability decision algorithm* is added to the implementation of the *Decider*, even when the frame capture is not enabled (default *Decider* implementation).

The reliability is defined for some applications (e.g., data transfer) as the data integrity and the level of guarantee of all the information sent by the transmitter that is accurately received at the receiver. Traditionally, each layer of the communication stack addresses reliability at different levels, to fix errors that are not correctable, observable, or are too costly to correct at the lower layers. However, if each layer performs a different reliability evaluation, this often leads to an unreliable or inefficient communication environment. Therefore, a cross-layer design has been proposed by numerous research papers and adopted in some systems for the reliability, namely between the PHY and MAC layers [GGSK11].

The physical layer in a digital communication system is responsible for bit-level transmission/reception of signals between nodes and should guarantee a certain level of reliability. It has to ensure that the transmitted bits are reliably reconstructed at a target receiver. The reliability at the physical layer is characterized by metrics like the SNIR, BER, Symbol Error Rate (SER), PER, and outage probability.

Achievable delivery of packets for reliable communications that rely on the values of the BER for IEEE 802.15.4 may simply be used considering the alternating bit protocol over a Binary Symmetric Channel (BSC) channel. This reliability guarantees a dependency between the desired reliability and the values of the BER for a certain packet length [KW05].

Based on the equations for PSR and PER defined in Equations 7.2 and 7.3, the number of trials $i \in \mathbb{N}$ needed to successfully transmit the packet over the link can be approximated to a geometric random variable X with the following probability mass function:

$$Pr[X = i] = PSR(nBits) \cdot PER(nBits)^{(i-nBits)} \quad (7.4)$$

and the following cumulative distribution function [KW05]:

$$F(k) = Pr[X \leq i] = \sum_{i=1}^k Pr[X = i] = 1 - PER(nBits)^k, \quad k \in \mathbb{N} \quad (7.5)$$

If the aim is to guarantee a certain delivery probability $\delta \in (0, 1)$, the physical layer may define the minimum number of trials, k^* , to successfully send the packet to the receiver with a probability whose value is at least δ (N.B. δ is the reliability). The value of k^* is also directly proportional to the energy consumption, and is given by:

$$k^* = F^{-1}(\delta) = \min\{k \in \mathbb{N} : F(k) \leq \delta\} \quad (7.6)$$

Conceptually, k^* is the δ -quantile of the random variable X . After some manipulation, one obtains:

$$k^* = \left\lceil \frac{\log(1 - \delta)}{\log(PER(nBits))} \right\rceil \quad (7.7)$$

where the $\lceil x \rceil$ represents the ceiling function. The number of trials k^* is represented in Figure 7.13 as a function of the BER for packets lengths $nBits = 64$ and 336 bits. Two different values are considered for the reliability (δ), $\delta_1 = 0.9$ and $\delta_2 = 0.99$. The plot presented in Figure 7.13 does not consider the ceiling function from Equation 7.7.

Figure 7.13 shows that for relaxed reliability requirements (example for $\delta_1 = 0.9$) and moderate-to-high bit error rates, in the range $[10^{-5}, 10^{-4}]$, the system wastes significantly less energy than for $\delta_2 = 0.99$. With $\delta_1 = 0.9$ the number of trials k^* needed to correctly deliver a packet is higher for higher packet lengths, as the value of the BER increases. If the value of the reliability is augmented ($\delta_2 = 0.99$) the number of trials needed to correctly deliver a packet is always higher than for $\delta_1 = 0.9$, packet lengths of 64 and 336 bits, as shown in Figure 7.13. Below a BER of approximately 10^{-4} , for the considered packet lengths, the channel quality is already good enough to successfully transmit the packet at the first trial while guaranteeing the target

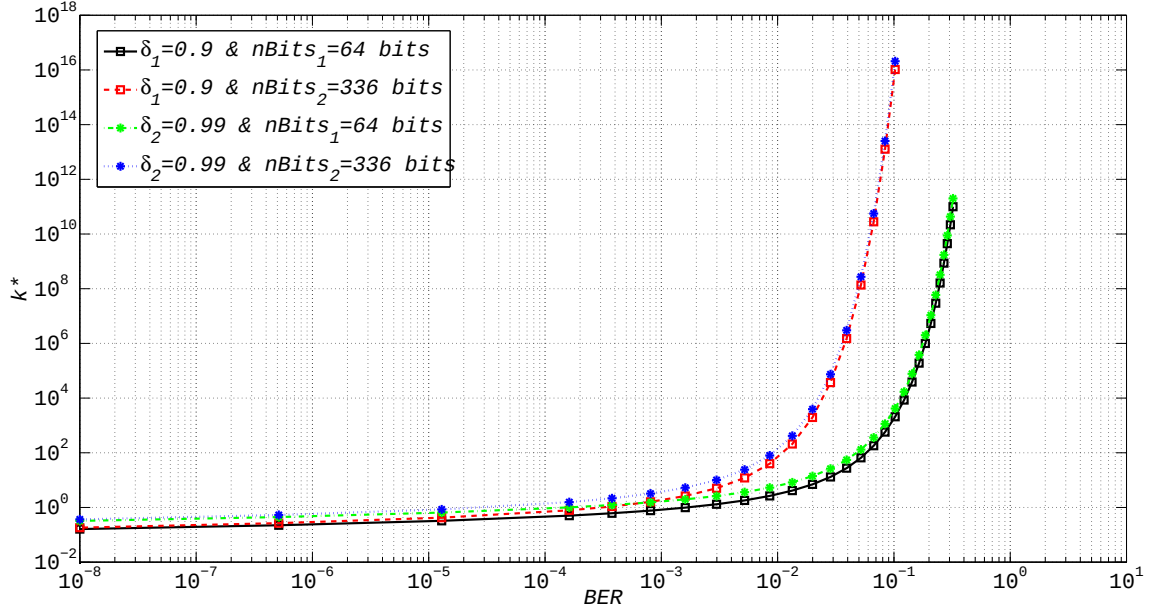


Figure 7.13: Minimum number of trials, k^* , needed to ensure that the packet reaches the receiver with a probability $\delta \in \{0.9; 0.99\}$, as a function of the BER for different packet lengths.

reliability bounds.

The proposed reliability concept [KW05] is included in the new implementation of the *Decider* in order to make a proper decision algorithm available, which establishes whether the packet is received with success or not. The algorithm was implemented in MiXiM by considering the two abovementioned values for the reliability, $\delta_1 = 0.9$ and $\delta_2 = 0.99$. The algorithm utilizes the Equation 7.7 to decide if the packet is received with success, which occurs if the condition $k^* \leq 1$ is verified. Otherwise, if $k^* > 1$, the packet is discarded. This means that in the new implementation of the *Decider* a packet is only successfully received at the first attempt.

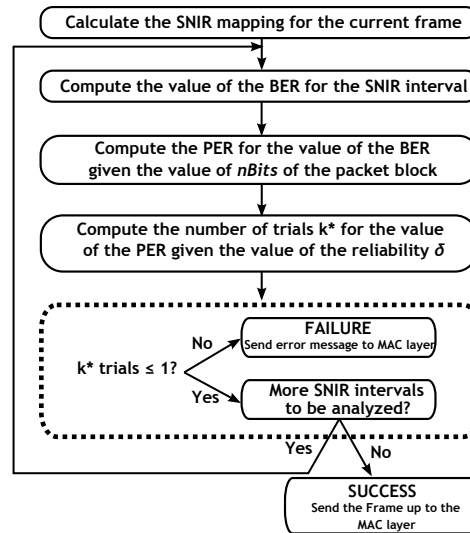


Figure 7.14: Reliability decision algorithm implemented in the MiXiM *Decider*.

The SNIR needed by most of the *Deciders* to evaluate if a signal was received correctly is calculated by dividing the received power of the signal to be evaluated (f_{RX_S}) by the receiving power of the interference, which is the summed up received power of every signal interfering ($f_{RX_{noise_{1..n}}}$) and thermal noise (i.e., -110 dBm) with the signal to be evaluated. Element-wise

operations on mappings are then needed to compute the value of the SNIR for a certain time interval: $F_{SNIR} = f_{RX_S} / \sum f_{RX_{noise_{1..n}}}$. The SNIR interval can be defined as the computation of the value of the SNIR for a certain time interval given by two time instants. Figure 7.7 presents five SNIR intervals. An example of a SNIR interval is the one defined between the time instants t_1 and t_2 . The mapping abstraction enables to compute the SNIR of a received packet at any interesting point in time, frequency and space, in a consistent manner.

The algorithm for the reliability decision implemented in the MiXiM framework is presented in Figure 7.14, and is as follows:

- When a frame is received in the *processSignalEnd()* method, the SNIR mapping is determined for the frame that is considered as the desired one. Depending on the number of frames that overlap different zones of the desired frame, a number of SNIR intervals is iterated by the algorithm. In each iteration, the algorithm checks whether that block, with a specific SNIR is corrupted or not;
- After determining the SNIR mapping (for all the SNIR intervals), the value of the BER is computed for this specific SNIR interval and with a given block length of *nBits*;
- Then, the algorithm computes the value of the PER for this specific BER and a given *nBits*;
- Based on the value of the PER value, block length and a certain reliability, δ , it computes the number of trials k^* needed to successfully decode this block of *nBits*;
- After that iteration, the algorithm checks whether the required number of trials, for a specific value of the PER, is lower or equal to one (i.e., $k^* \leq 1$). If so, the algorithm checks if there is more SNIR intervals to be analyzed. Otherwise, if the number of trials needed to decode the block of *nBits* successfully is higher than one, then the frame is immediately discarded and a message with the identifying error in the bits is sent by the control channel to the MAC layer;
- Finally, after ensuring that the number of trials is lower or equal to one, the algorithm checks if there is more SNIR intervals to be analyzed. If so, the algorithm repeats all the steps from the computation of BER value for a specific SNIR value. Otherwise, if there is no more SNIR intervals, the frame is decoded with success and it is sent up to the MAC layer.

Figure 7.15 presents a simplified representation of the overall behaviour of the *Decider* with the frame capture capability. The implementation was added in all the three functions of the *Decider* that process the frame at different points in time, during its reception. These functions are the *processNewSignal()*, *processSignalHeader()* and *processSignalEnd()* ones. The description of the enhanced *Decider* with frame capture capabilities has some parts that have been omitted, because they are the ones that have not been changed. Also note in the real implementation, various functions (such as the vectors used for the collection of the metrics) are implemented but their behaviour is not reflected in the diagram. Also, some modifications have been made at the function *getSignalState()* from the *BaseDecider* module. In the default *BaseDecider* module, the function *getSignalState()* is called each time the *Decider* receives a frame and needs to know if the frame is new or not in the new version of the *Decider*. This function was updated in order to handle two or more frames, so that the remaining ones are not considered as interfering frames anymore. The function presents the following procedures:

- It checks if the frame passed as an argument to the function for the first time;

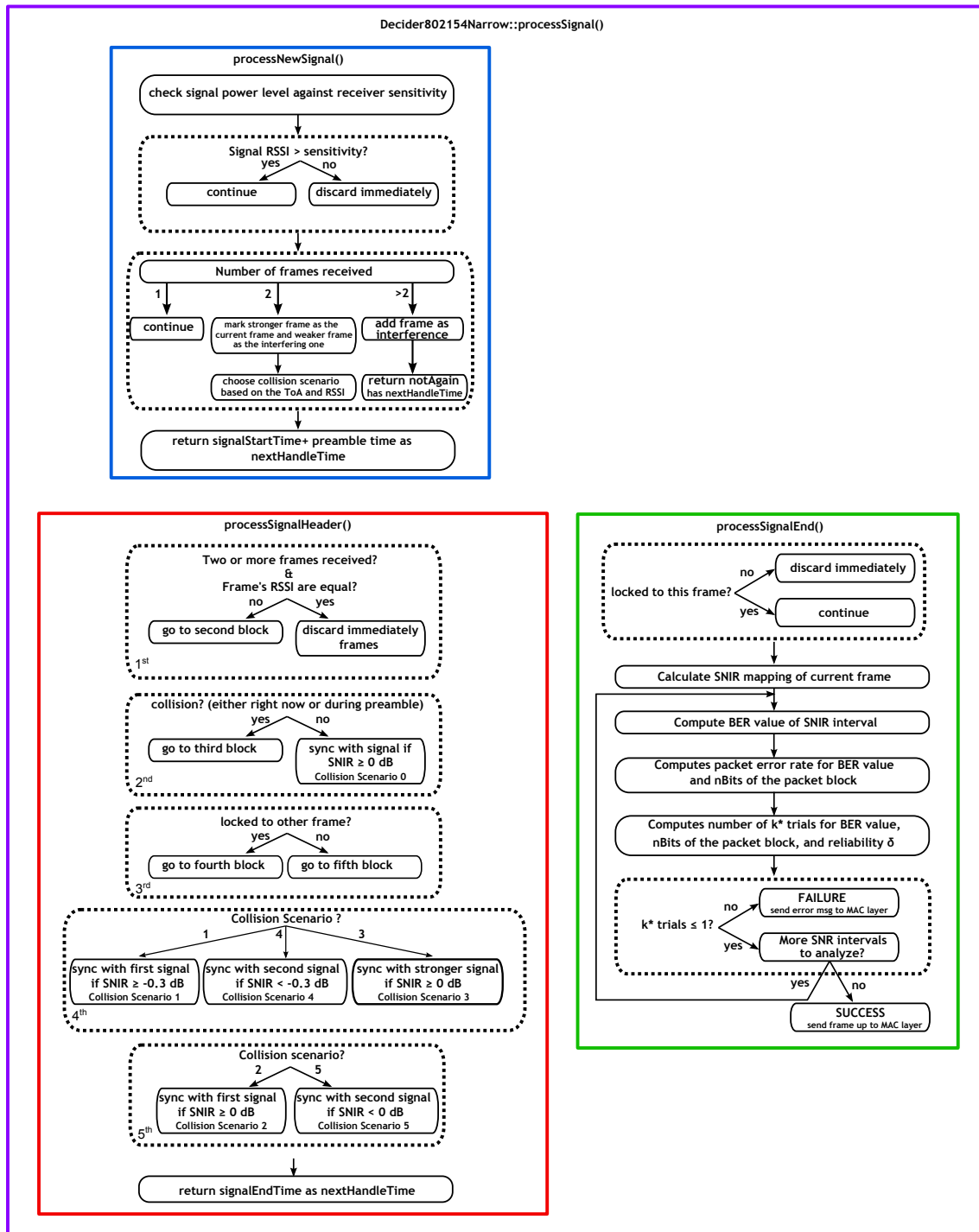


Figure 7.15: Upgraded MiXiM Decider - Modifications performed to enable Frame capture.

- If the frame is received for the first time it is accepted by the function. As a consequence, the function returns the *SignalState* as NEW to the *Decider*. This way, the *Decider* is able to know that this frame is being received for the first time. This is possible because each frame has an unique Identification (ID) during a simulation;
- If the frame is not received for the first time it arrives to the *BaseDecider* module, the method returns the *SignalState* to the *Decider*, and it can assume two values: EXPECT_HEADER or EXPECT_END.

7.5.2 Justification for the Frame Capture Decision Thresholds

From all the literature and research works it can be concluded that, depending on the current state of the receiver as well as the current state of the interference, there can be multiple SNIR capture decision thresholds in which a newly arriving frame must attain in order to enable the receiver to start decoding it. There are four relevant capture thresholds [FXHZ10, LRLK08]:

- The “*normal*” capture decision threshold - It is the required SNIR for a frame that experiences no interference, i.e., just thermal noise and noise from sources other than the IEEE 802.15.4 nodes also competing for the medium;
- The “*locked*” capture decision threshold - It is the required SNIR for a frame if the receiver is already locked to and receiving another frame;
- The “*garbled*” capture decision threshold - It is the required SNIR for a frame if the receiver is already experiencing interference from another frame but is not locked to this interference;
- The “*simultaneous*” capture decision threshold - It is the required SNIR for a frame if the receiver is experiencing interference from another frame but is neither locked to this frame nor to the interfering frame, since both frames have been received “simultaneously”.

These thresholds are based on simulation experiments and the observed behaviour from the work in [FXHZ10]. In the first simulations performed with the frame capture feature, the considered thresholds were the same as the ones applied to IEEE 802.11a in the work from the authors of [LRLK08]. In the second set of simulations, the frame capture thresholds were based on the behaviour observed from the curves of the Figure 7.3. In the second set of simulations the thresholds are lower than the ones from [LRLK08]. Then, based on the conducted simulations, it is possible to tune the thresholds in order to guarantee the maximum packet reception possible when considering one interfering frame. For the scenarios with more than one interfering frame, these thresholds have been maintained. Therefore, it should be kept in mind that these thresholds do not always guarantee the maximum successful packet reception in all the scenarios. Rather, the objective of the frame capture is to increase the data packet success rate.

7.6 Performance Evaluation

Two significant changes have been made to the simulator:

- The frame capture feature is implemented so that not all frames during a collision are necessarily lost;
- The *Decider* algorithm to determine whether the frame is received or not is modified aiming at ensuring a certain reliability for correctly decoding the frame.

Both improvements should be considered separately in the evaluation of the frame capture effect. In order to properly evaluate the frame capture feature with the new decision algorithm, a performance comparison must be performed between the *Decider* with the FC enabled and disabled for the considered collision scenarios.

The frame capture has certainly a significant effect on the throughput. If a frame is captured, a collision no longer necessarily means loss of capacity. Frame capture always occurs during a collision (i.e., the transceiver is able to capture a frame in favour of a weaker frame). Hence, any scenario where many collisions occur is interesting for analysis. Therefore, all the simulated scenarios induce collisions, to better evaluate the frame capture effect. The intention is to show by means of simulations that frame capture has a considerable impact on the performance of networks with broadcast traffic.

7.6.1 Simulation Scenario

In these simulations, the IEEE 802.15.4 outdoor channel model is considered. The channel model affects the network performance by means of the physical layer impairments, such as fast fading and shadowing. The node topology represents a tight cluster of dense deployed wireless nodes, which is a worst-case situation in terms of collisions. We assume that the sensor nodes have random positioning mobility. An example of node deployment is shown in Fig. 7.16. The reason for applying this type of mobility model to the nodes is the need to vary the RSSI from the receiver node. In the MiXiM framework, the RSSI of a frame sent by a node varies depending on the distance to the receiver node. In these collision scenarios, nodes are deployed using a 2D Poisson process on a $80 \times 80 \text{ m}^2$ area (i.e., x and y coordinates are randomly chosen with uniform distribution within $x, y \in [0, 80] \text{ m}$). The random positioning is repeated each 3 seconds. The number of contending nodes is kept constant during the simulations, in order to properly evaluate the effective data packet delivery. There is only one sink node while the remaining ones are sources (and send broadcast packets), as shown in Fig. 7.16.

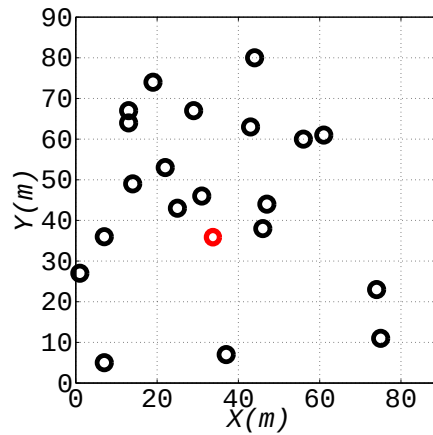


Figure 7.16: Example of a deployment scenario (the red circle is the sink node while the remaining ones are sources).

For each deployment with n contending nodes, a set of 6 seeds has been chosen for the random number generator (which has six degrees of freedom). Each simulation takes 100000 seconds of simulation time, corresponding to 19998 attempts of transmitting frames for each seed.

In this set of frame capture simulations, the Texas Instruments CC2420 low-power radio transceiver is considered with a transmission rate of 250 kbps, whose characteristics are available in the MiXiM [WSKW09, KSW⁺08]. Frames are periodically generated at the application layer with a certain frame time interval parameter (5 s). Each time the application layer generates a frame, it only transmits the frame after the node has chosen a new position in the simulation area. The considered frame length during the simulations is 50 Bytes (400 bits). The enhanced *Decider*

has a variable named “*frame_capture_feature*” that facilitates to enable or disable the frame capture feature in the simulator. Besides, the capture decision thresholds and the minimum number of trials (k_{min}^*) that guarantee a correct decoding of the frame can be easily modified by the user.

As it is usual in IEEE 802.15.4 the thermal noise is set to -110 dBm. The capture thresholds are implemented as described in Section 7.2. Radio switching times have been omitted, i.e., a receiving radio can switch between the sending and receiving mode instantly. The receiver sensitivity is set to -94 dBm, which is a typical value for the CC2420 radio transceiver [CC207]. The maximum transmission power of all nodes is 1 mW (-30 dBm).

7.6.2 Performance Metrics

During the simulations, the collection of the right metrics is essential to give insights regarding the performance of the network. OMNeT++ already has modules dedicated to the collection of metrics. From within any OMNeT++ module, the function *recordScalar(name, value)* can be called, storing a name-value pair. Apart from the general network performance metrics, the information on the capture events is also important. Therefore the following metrics have been recorded:

- Number of successful packets received by the sink;
- Number of packets discarded by the sink;
- Total number of packets received by the sink;
- Minimum BER observed for each successful packet received by the sink;
- Minimum BER observed for each packet discarded by the sink;
- Corresponding minimum SNIR for the minimum BER for each packet successfully received by the sink;
- Corresponding minimum SNIR for the minimum BER for each packet discarded by the sink;
- Corresponding minimum PER for minimum BER for each packet successfully received by the sink;
- Corresponding minimum PER for the minimum BER for each packet discarded by the sink;
- Value of the k^* for the minimum BER, for each packet successfully received by the sink;
- Value of the k^* for the minimum BER, for each packet discarded by the sink;

These capture metrics are considered for the verification of the implementation of the frame capture feature for WSNs in the MiXiM framework.

7.7 Results

This section discusses the results of all the simulations that have been performed to evaluate the performance of the frame capture effect. Note that the confidence interval is not visualized in any of the curves. The confidence intervals are not plotted to avoid confusion in the interpretation of the graphs. Therefore, the mean values of the 95 % confidence intervals are

Table 7.5: SNIR distribution for the MiXiM *Decider* default implementation for the different collision scenarios.

Collision Region	SNIR interval for the critical zone [dB]	SNIR interval for the success zone [dB]	SNIR interval for the failure zone [dB]
1	$[-2; 0]$	>0	<-2
2	$[-2; 0.5]$	>-0.5	<-2
3	-	≥ 0	<0
4	$[-3; 0]$	>0	<-3
5	$[-8; 0]$	>0	<-8

shown in the curves. These average curves have been calculated with six different random simulations. The six considered seeds are always the same and generate always the same positions for the nodes at each time they randomly choose their positions. Since the node placement is the same for all the scenarios, the SNIR relations are the same. Therefore, the comparison of the different metrics is possible, whilst considering different collision scenarios.

7.7.1 Previous Decider implementation

Before implementing the frame capture feature in the MiXiM framework, some evaluation of the previous *Decider* implementation was performed. The objective of this evaluation was to understand the behaviour of the current *Decider* when subjected to the different collision scenarios. The previous *Decider* does not account for the full frame capture feature, as mentioned earlier. All the presented histograms are normalized with respect to the total received packets (received with success and discarded). In this evaluation only one interfering frame was considered.

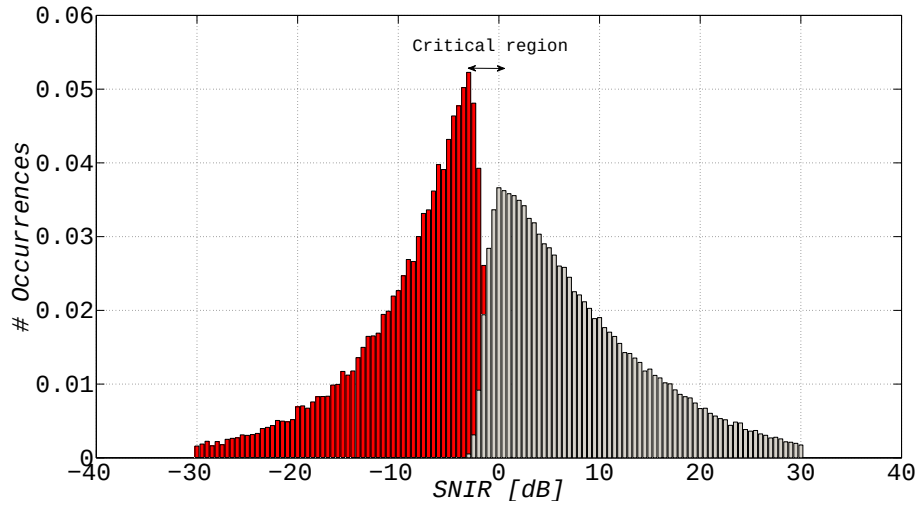


Figure 7.17: SNIR histogram distribution for the MiXiM *Decider* default implementation under Collision Scenario 1. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.

Figures 7.17 to 7.21 show the SNIR histogram distributions for the MiXiM *Decider* previous implementation under the five collision scenarios (1 to 5). The red bars refer to the packets that are received with failure, while the grey bars refer to the packets that are received with success. In the figures, is presented the SNIR turning point (to initiate always receiving the packets successfully) which differs depending on the Collision Scenario. The values of the SNIR turning point are summarized in Table 7.5. In the Figures 7.17 to 7.21 there are more packets received with errors than with success. With the default *Decider* implementation, there is a critical zone in which, for the same values of SNIR the packet is received either with no errors

or with errors. This critical zone varies depending on the collision scenario and is summarized in Table 7.5. In addition, in Table 7.5 is presented the SNIR intervals for the packets that are received with success and failure zones.

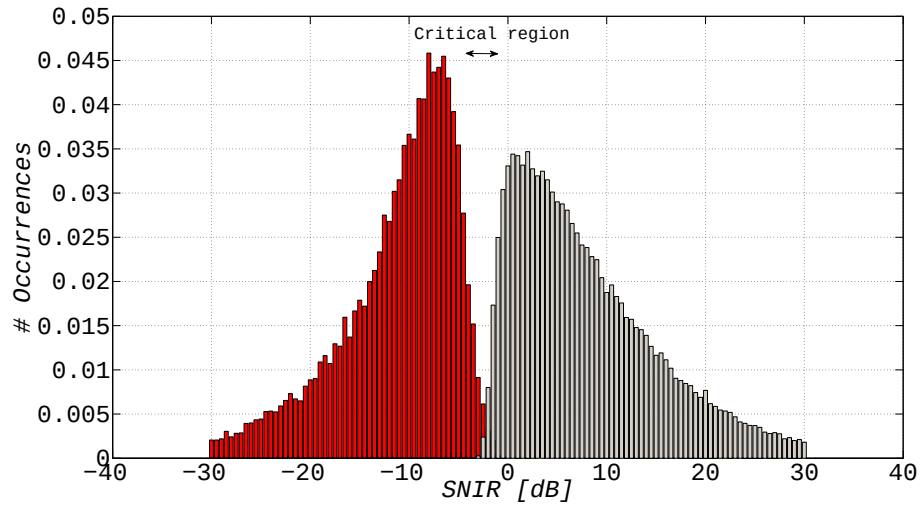


Figure 7.18: Normalized SNIR histogram distribution for the MiXiM *Decider* default implementation under Collision Scenario 2. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.

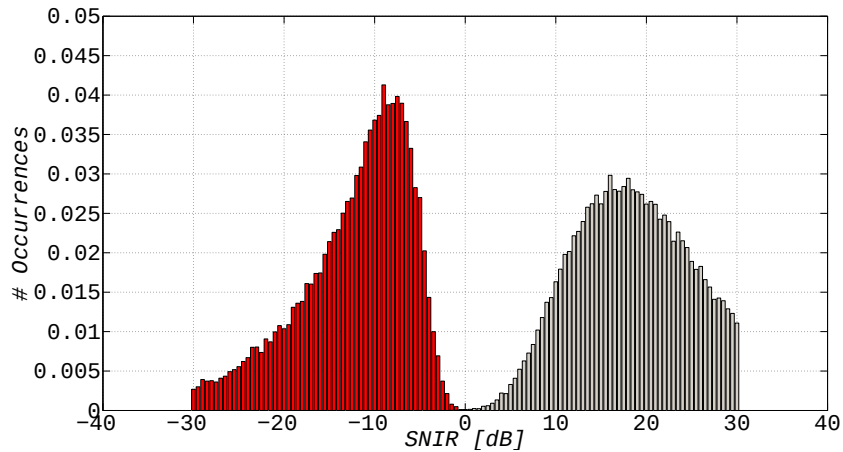


Figure 7.19: Normalized SNIR histogram distribution for the MiXiM *Decider* default implementation under Collision Scenario 3. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.

The existence of the critical zone is due to the random comparison that is performed in the default *Decider* implementation. It does not take into account the value of the SNIR. Apart from the value of the SNIR, the final decision on successfully decoding the packet depends on the comparison with a random number, which is not so effective.

The packet success rate on SNIR was also evaluated with the default *Decider* implementation for the different collision scenarios. The results from this evaluation of the PSR are presented in Figure 7.22. All the presented values correspond to mean values obtained from the six seeds considered in the simulations. It can be observed in Figure 7.22 that, in all the collision scenarios, the PSR achieves the maximum value for SNIRs values higher than about 0 dB. By comparing each of the collision scenarios, one considers that the Collision Scenario 3 (green line) is the one that presents a non-null PSR for a SNIR of about -2 dB. This happens because this scenario corresponds to the full packet overlapping case. Since there is more bits of the

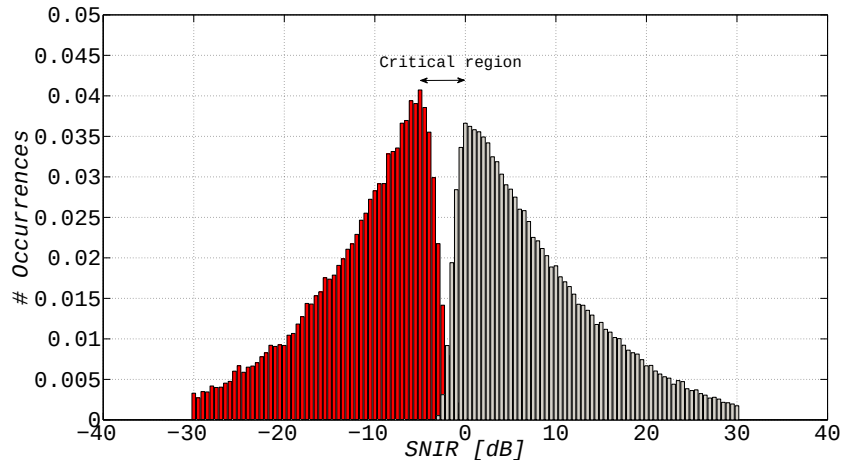


Figure 7.20: Normalized SNIR histogram distribution for the MiXiM *Decider* default implementation under Collision Scenario 4. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.

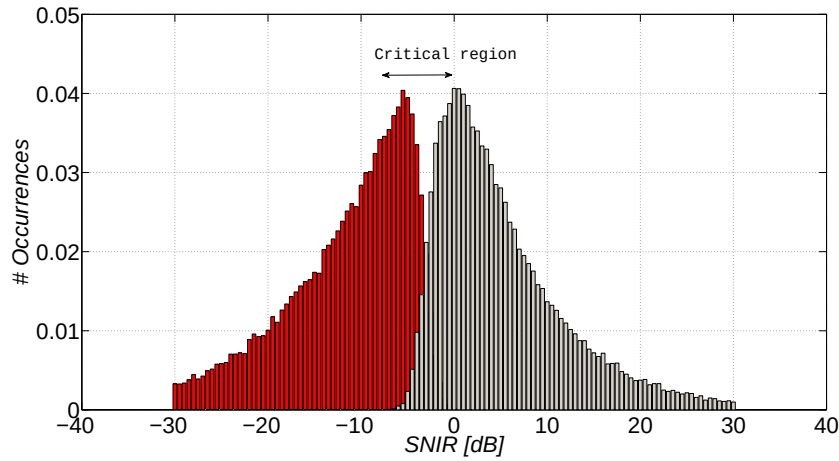


Figure 7.21: Normalized SNIR histogram distribution for the MiXiM *Decider* default implementation under Collision Scenario 5. Red bars represent the number of occurrences for the packets received with failure, while grey bars refer to the packets received with success.

packet being overlapped, the required SNIR to obtain a non-null PSR must be higher than in the other collision scenarios. The values of the required SNIR to achieve a non-null PSR are summarized in Table 7.6 for the remaining collision scenarios.

To better evaluate the current *Decider* implementation the BER distribution for aforementioned collision scenarios was also plotted, whilst considering different SNIR values, as presented in Figure 7.23. In this graphic the random comparison performed in the current *Decider* implementation to decide whether the packet is accepted or not, is not taken into account. Thus, in Figure 7.23 the Collision Scenarios 1, 2 and 3 present the same BER distribution. While the Collision Scenarios 4 and 5 present other BER distribution. The latter collision scenarios for lower SNIR values present lower BER values than in the former collision scenarios (1, 2 and

Table 7.6: Values of the SNIR for a non-null PSR under different collision scenarios.

Collision Region	SNIR [dB]
1	≥ -4
2	≥ -4.3
3	≥ -2
4	≥ -6
5	≥ -6

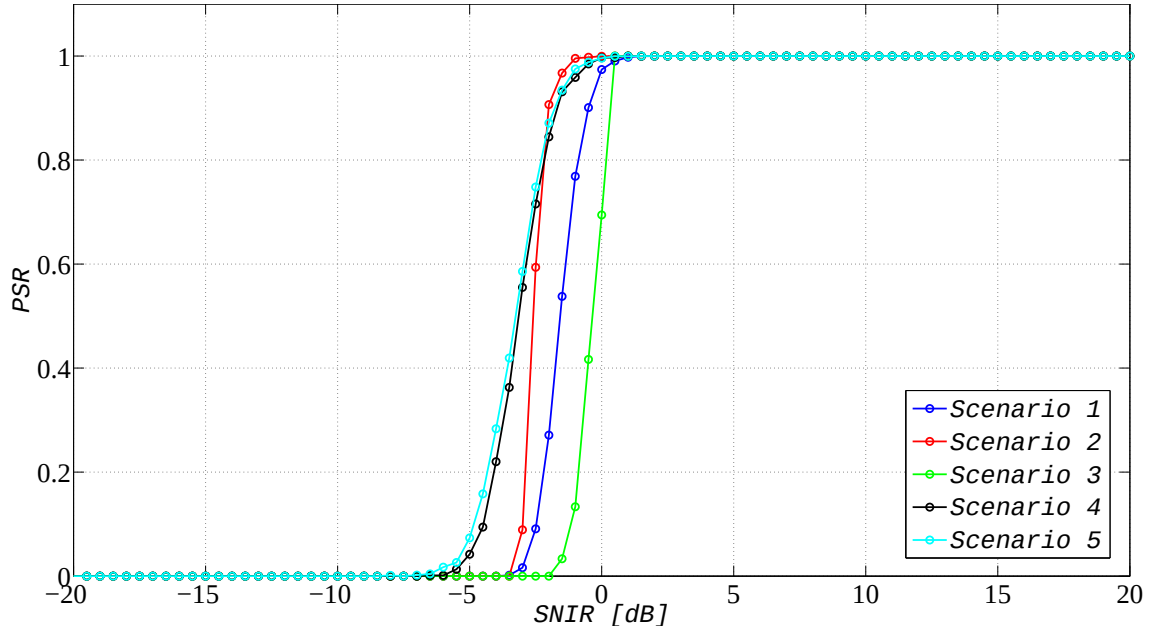


Figure 7.22: PSR versus SNIR distribution for all Collision Scenarios (1 to 5) of MiXiM *Decider* current implementation.

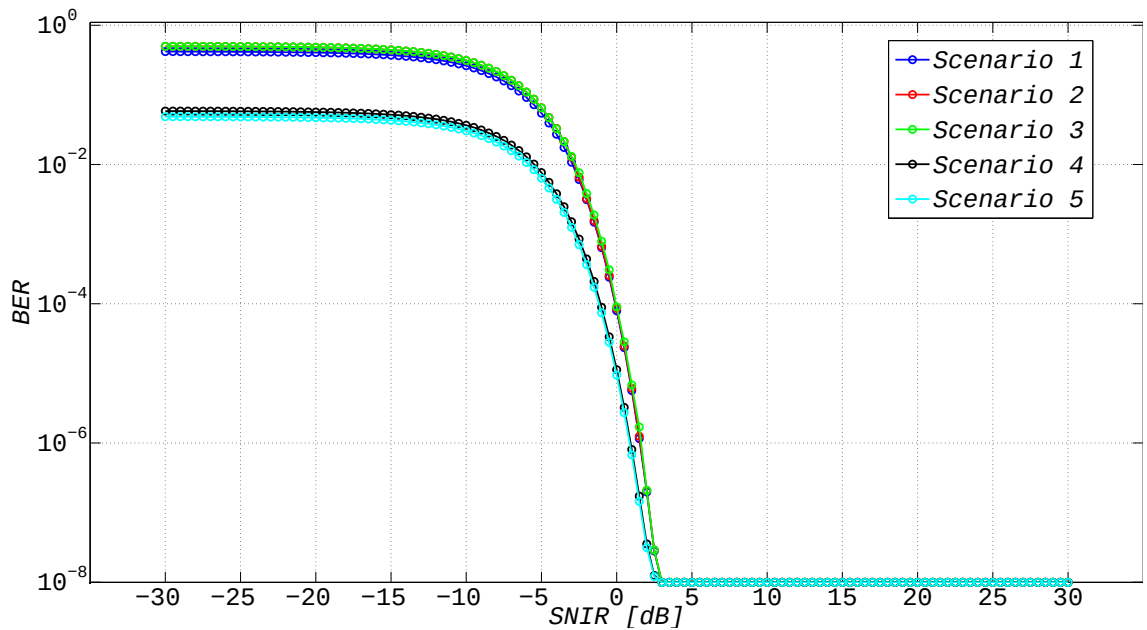


Figure 7.23: BER versus SNIR distribution for all the collision scenarios (1 to 5) in the MiXiM *Decider* default implementation.

3). Moreover, for all the scenarios the BER is always equal to 1×10^{-8} for SNIR values higher than 2.5 dB. To plot this distribution all the packets (in the presence and absence of errors) are considered.

7.7.2 Enhanced *Decider* with Frame Capture

After implementing the reliability decision algorithm as well as the frame capture capability in the MiXiM framework, implementation of the enhanced *Decider* was verified. The intention is to show the advantages of considering a physical layer with frame capture capabilities and a Enhanced Reliability Decision algorithm based on this evaluation.

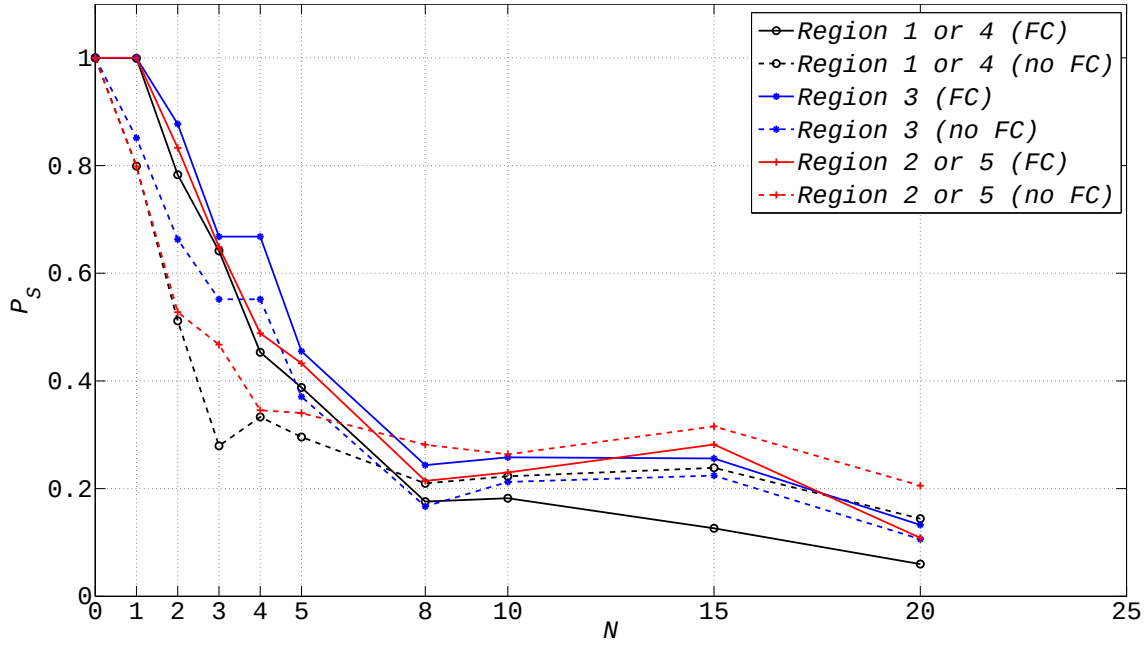


Figure 7.24: Probability of success versus the number of, N , interfering nodes for different collision scenarios, with the reliability decision algorithm ($\delta_1 = 0.9$), considering the FC effect enabled and disabled.

Figure 7.24 shows the variation of the probability of success within the number of interfering nodes, for each of the collision scenarios when the frame capture effect is enabled or disabled. A reliability of $\delta = \delta_1 = 0.9$ is considered. By comparing the curves, one can conclude that for $N < 8$ frame capture leads to higher values of the PSR in all the collision scenarios. It is also shown that for $N < 8$ interfering nodes there is no advantage of using frame capture. The collision scenarios evaluated in this work, are always the worst possible cases because the interfering frames overlap the desired packet for almost 95 % of the section. All the cases whose overlap is less than the ones studied in this work will present higher values for the PSR when frame capture is enabled, even for higher number of interfering nodes. The collision scenario that presents the highest values for the PSR (in average) is the Collision Scenario 3 (blue lines), while the one that presents the lowest PSR values (in average) are the Collision Scenarios 1 or 4 (black lines). One can also conclude from Figure 7.24 that, for all collision scenarios, the values for the PSR decrease sharply as N increases up to eight interfering nodes. For a number of interfering nodes higher than eight, the value of the PSR decreases at a slow rate as the interfering nodes increases.

To measure the gains achieved when using a physical layer with frame capture enabled the Mean Absolute Error (MAE) for the different collision scenarios was calculated (for a value of the reliability $\delta = \delta_1 = 0.9$). These MAE values are shown in Figure 7.25. The highest gain achieved with frame capture enabled is about 38 % in the Collision Scenarios 1 or 4 (dashed line). In the Collision Scenario 3 (solid line) the highest achieved value for the MAE is 21 %, while for the Collision Scenarios 2 or 5 (dotted line) the highest value of the MAE is 30 %. All these values for the MAE are compared with the *Decider* in which the frame capture effect feature is disabled, but the reliability decision algorithm is maintained.

The values presented in Figure 7.25 are the absolute values of the gain, and may not reflect the negative gains (i.e., loss) that the use of the frame capture presents when $N \geq 8$. The use of the frame capture effect in Collision Scenarios 1, 2, 4 and 5, $N \in \{8, 10\}$, leads to a negative gain of 5 %, while, for $N = 20$, it leads to a negative gain of 10 %. The negative gain means that

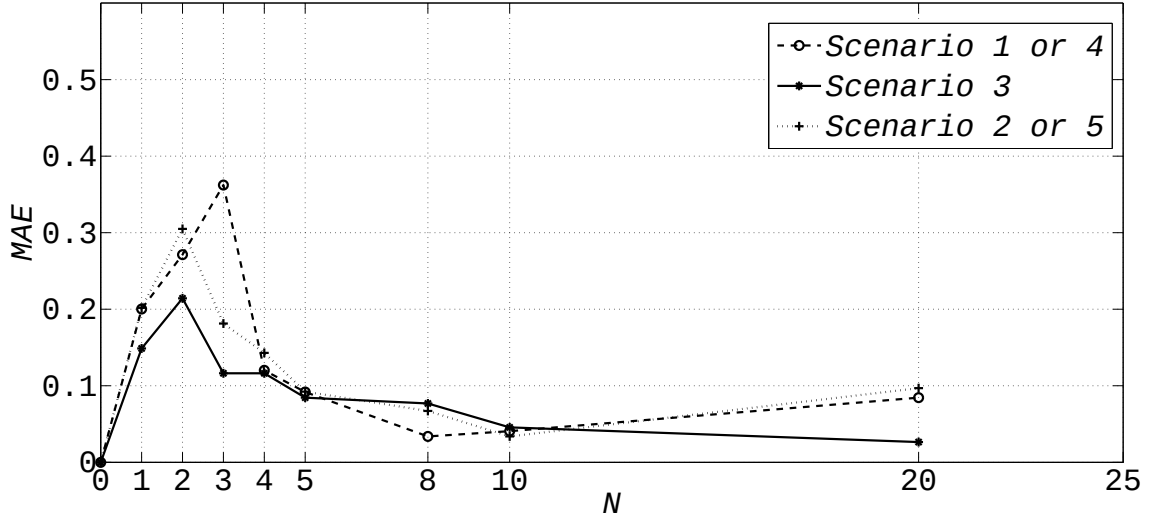


Figure 7.25: Mean absolute error for all collision scenarios in the case the FC effect is enabled or disabled, ($\delta_1 = 0.9$).

Table 7.7: Comparison of the average gains (%) between the cases of frame capture feature enabled and disabled.

Collision scenario	Gain		
	Absolute	Non absolute	Absolute ($N < 8$)
Collision Scenario 1 or 4	13.39	9.85	17.43
Collision Scenario 3	9.21	9.21	11.33
Collision Scenario 2 or 5	12.46	8.06	15.39

the employment of the frame capture effect in a specific situation is not advantageous, which leads to performance losses. Only in the Collision Scenario 3 there is a positive gain of about 5 %, for $N \in \{8, 10\}$, and 3 %, for $N = 20$. Table 7.7 presents a summary of the comparison of the average gains between the cases when frame capture is enabled and disabled.

In Table 7.7 there is a distinction between the absolute and the non absolute values. The former are based on the values of the MAE (in which the gains are always positive) from Figure 7.25. The latter are based on the difference of the probability of success between the cases when the frame capture is enabled and is disabled (in which the gains can be either positive or negative). All these mean values are calculated for all the points presented in Figure 7.25. However, the last column of Table 7.7 only refers to the average gain for each collision scenario when $N < 8$ (when the frame capture is advantageous). The Collision Scenario 3 presents the same value of the gain when considering absolute or non absolute values, because all the gains achieved for the different number of interfering nodes are positive (the use frame capture effect is always advantageous).

After evaluating the packet success ratio in different collision scenarios with and without frame capture feature, the influence of the reliability on the probability of success was analyzed. In this analysis, the Collision Scenario 3 was considered, because it is the scenario in which the interfering frame completely overlaps the desired signal, becoming the worst possible scenario. All other collision scenarios, presenting a lower packet overlapping percentage, will result in higher values for the PSR. Figure 7.26 presents the variation of the probability of success for the Collision Scenario 3, with the frame capture effect enabled and disabled, with $\delta = \delta_1 = 0.9$ and $\delta = \delta_2 = 0.99$.

In Figure 7.26 the probability of success for a reliability of $\delta = \delta_1 = 0.9$ is always higher than

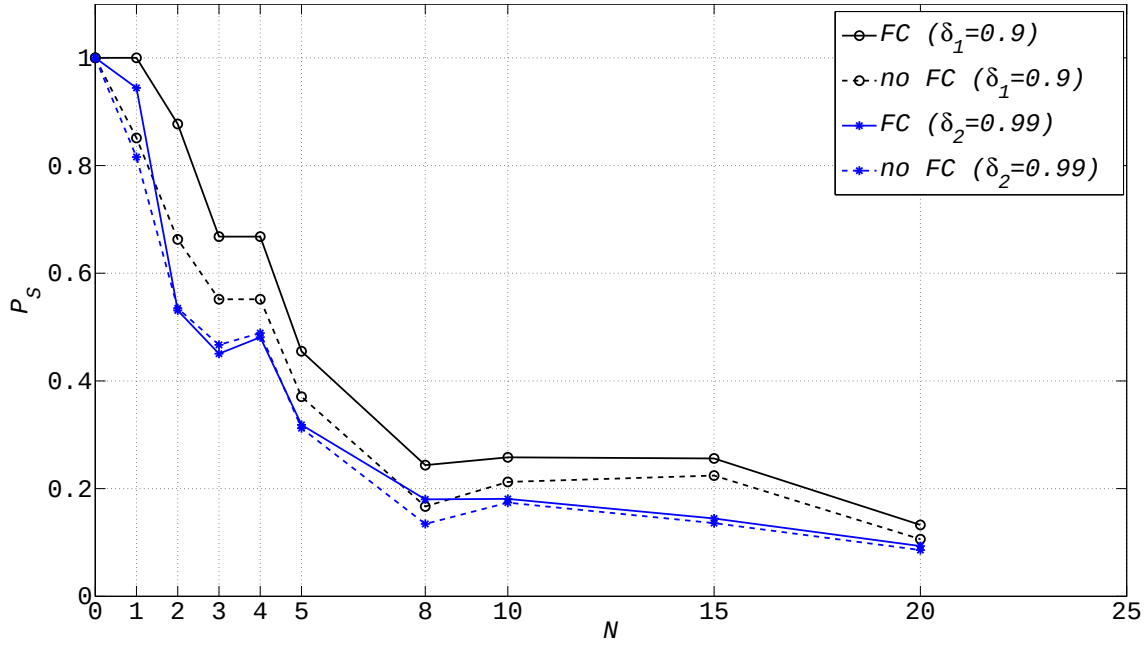


Figure 7.26: Probability of success as a function of the number of interfering nodes, N , for the Collision Scenario 3, with the FC effect enabled and disabled, with $\delta_1 = 0.9$ and $\delta_2 = 0.99$.

for $\delta = \delta_2 = 0.99$ (with and without frame capture enabled). This result is expected since, with the increase of the reliability the minimum BER required to accept a packet becomes higher. For $\delta = \delta_2 = 0.99$ (blue lines), the behaviour is similar to the case of $\delta = \delta_1 = 0.9$, as the number of interfering nodes increases. Moreover, for a reliability of $\delta = \delta_2 = 0.99$ the gains obtained from enabling the frame capture feature are not so notorious as for $\delta = \delta_1 = 0.9$. With $\delta = \delta_2 = 0.99$ (differently from considering lower values of δ), these values can be interpreted as approximately the lowest (worst case) achievable probability of success when considering a physical layer with and without frame capture.

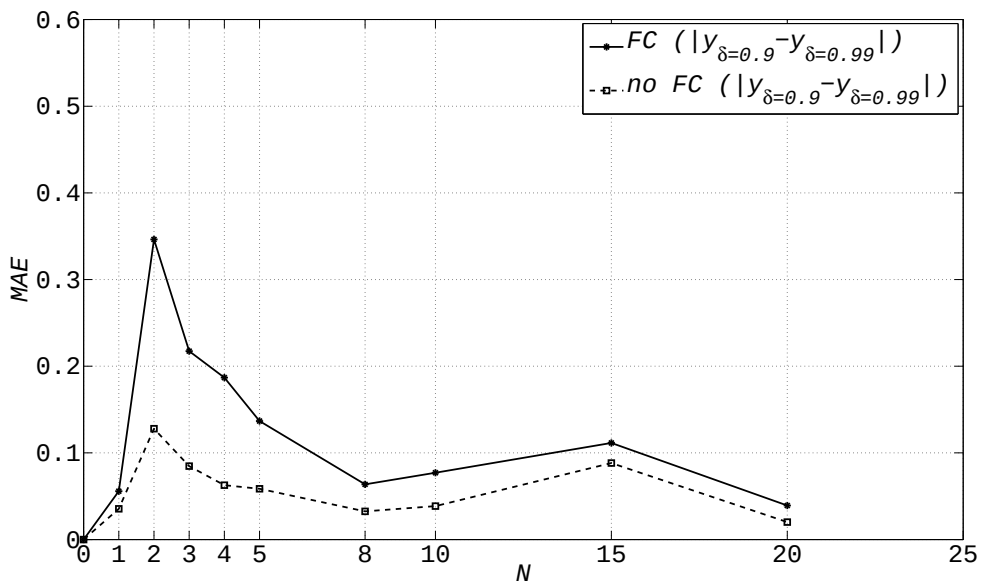


Figure 7.27: Variation of the mean absolute error with N for the Collision Scenario 3, with the FC enabled and disabled ($\delta_1 = 0.9$ and $\delta_2 = 0.99$).

Figure 7.27 shows the MAE as a function of N for $\delta = \delta_1 = 0.9$ and $\delta = \delta_2 = 0.99$ and the frame capture effect enabled or disabled. By analyzing Figure 7.27, the case of $N = 3$ (interfering nodes) corresponds to the highest value of the MAE for both the cases of frame capture enabled and disabled. The highest values of MAE are 35 % and 12 %, respectively. To have a better comprehension of the difference between considering a lower value of the reliability over a higher one, the average gain was calculated. The average gain with the frame capture effect enabled, is equal to 12.48 %. For the case of the frame capture effect disabled, whilst defining a lower reliability parameter the mean gain is equal to 5.12 %. A higher reliability means less packets received successfully. However, it guarantees that packets with lower bit errors are delivered at the MAC layer level. Therefore, these tradeoffs should be balanced in the choice of the reliability to be considered in the simulator.

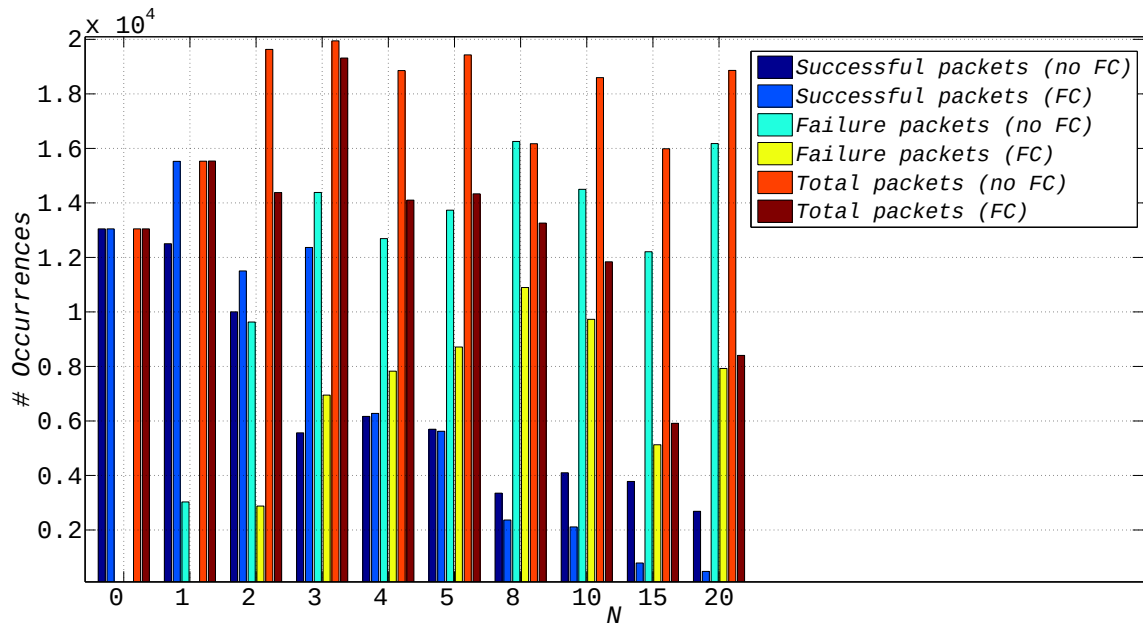


Figure 7.28: Histogram with total, successful and discarded packets for the Collision Scenarios 1 or 4, with the FC enabled and disabled, with $\delta_1 = 0.9$.

Figures 7.28, 7.29, and 7.30 present the histograms for the total, successful and discarded packets for each collision scenario when the frame capture effect is enabled and disabled, with a reliability $\delta = \delta_1 = 0.9$.

By analyzing all these figures for the total number of packets received, not all the cases show a total of 19998 packets, as it may be expected. This is explained by the propagation model (IEEE 802.15.4 Outdoor model) considered in the simulator and the random mobility from the nodes. The cases that show a total number of packets lower than 19998, correspond to cases where the distance between the source and sink nodes were not enough to establish a link. Therefore, the packet never reached the sink node. It is however worthwhile to note that when this happens, the packet is not registered in the sink node metrics. In all the histograms for the case of no interfering nodes, the successful packets (with and without the frame capture effect enabled) are the same as the total received ones, as expected. In the Collision Scenarios 1, 2, 4, and 5, for $N < 8$ the number of successful packets is always higher for the case with frame capture enabled. In the same collision scenarios, but considering $N \geq 8$ the packets received with success are always higher for the case with frame capture disabled, as discussed earlier. In the Collision Scenario 3 the number of packets received with success is always higher if the frame capture effect is enabled.

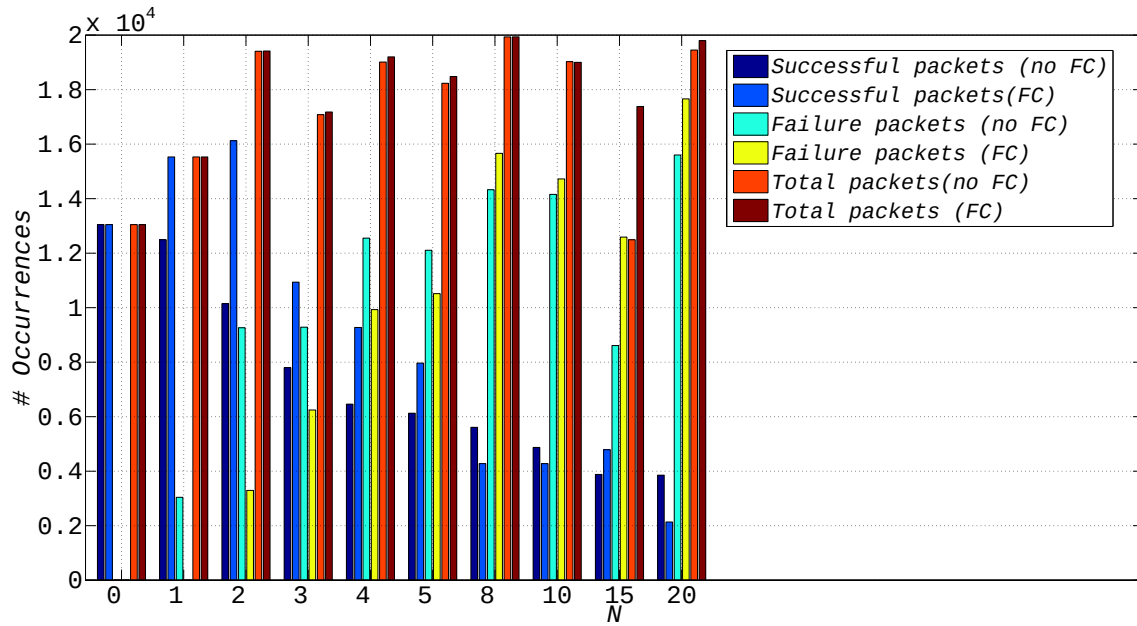


Figure 7.29: Histogram with total, successful and discarded packets for the Collision Scenario 3, with the FC effect enabled and disabled, with $\delta_1 = 0.9$.

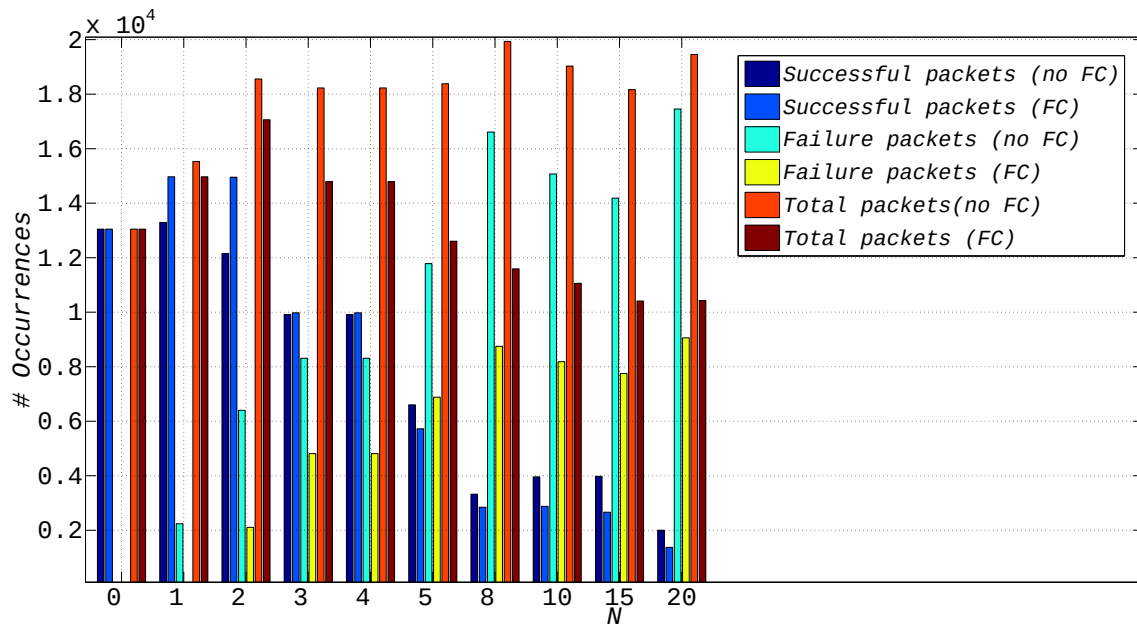


Figure 7.30: Histogram with total, successful and discarded packets for the Collision Scenarios 2 or 5, with the FC enabled and disabled, with $\delta_1 = 0.9$.

Note that, in all the collision scenarios, for $N > 0$, the total number of packets received by the sink when the frame capture is disabled is always higher than in the case of frame capture enabled. However, the number of packets received with errors when the frame capture is disabled is always higher than in the case when the frame capture is enabled. At first glance this could be interpreted as a bad performance of the frame capture feature. However, the ratio between the number of successful packets and the total packets received by the sink is better in the case with frame capture enabled, for $N < 8$. For higher values of N there is no notorious advantage of using frame capture. The reason for the total number of packets received by the sink when frame capture is disabled is because of the absence of the frame capture capability

that does not tries to receive the stronger signal and due to the SNIR mappings that are simpler than the ones implemented just for the frame capture feature.

7.7.3 SCP-MAC Throughput and Delivery Ratio with Frame Capture

In the previous sections, behaviour of the packet success ratio was evaluated in different collision scenarios, with and without enabling the frame capture feature. Moreover, conclusions on how the reliability influences the probability of success were also obtained. Since the previous results consider a simple MAC protocol that does not include any kind of carrier sensing or collision avoidance mechanism, some simulations were conducted with the frame capture effect feature enabled/disabled considering the SCP-MAC protocol.

This analysis considers the Collision Scenario 3, because this is the scenario in which the interfering frame completely overlaps the desired signal, becoming the worst possible scenario.

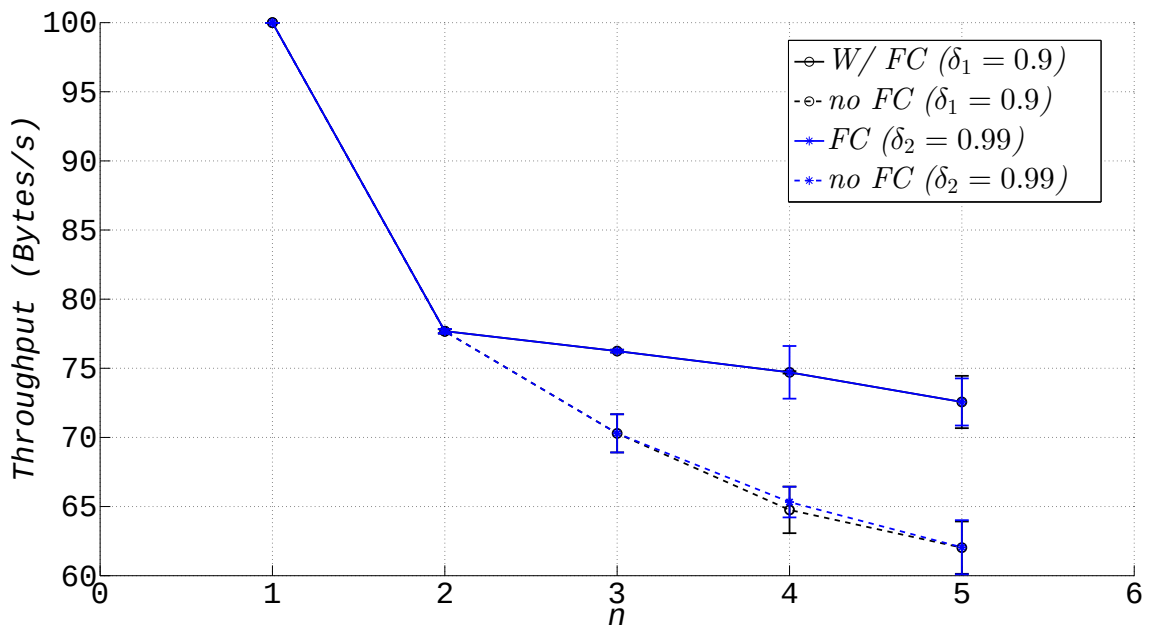


Figure 7.31: Throughput of SCP-MAC protocol in the case of FC enabled and disabled with $\delta_1 = 0.9$ and $\delta_2 = 0.99$.

Figure 7.31 presents the throughput obtained for the SCP-MAC protocol as the number of transmitters, n , in the network increases. These results consider the frame capture feature enabled and disabled, as well as reliabilities of $\delta = \delta_1 = 0.9$ and $\delta = \delta_2 = 0.99$. Figure 7.31 shows that, for $n \geq 2$ when the frame capture is enabled, the achieved throughput increases up to 10 %, compared with the achieved throughput when the frame capture is not enabled. For the SCP-MAC protocol, since the nodes are all synchronized, the only possible overlapping scenario is the Collision Scenario 3 (the interfering frame completely overlaps the desired signal). By comparing the achieved gains (when frame capture is enabled) with the gains presented in Table 7.7 (for the Collision Scenario 3), we conclude that the values are similar and consistent. Other performance metric analyzed with the SCP-MAC protocol is the delivery ratio, which is deeply related with the throughput. In Figure 7.32, the delivery ratio is always higher when the frame capture effect is enabled (for both reliability values) when $n > 1$. For $n > 1$ the gains achieved present a maximum value of around 75 % for $n = 3$, and a minimum value of around 42 % for $n = 5$. Besides, the delivery ratio gain decreases as the number of transmitters increases, but at a slower rate. Based on the early conclusions for the frame capture effect and

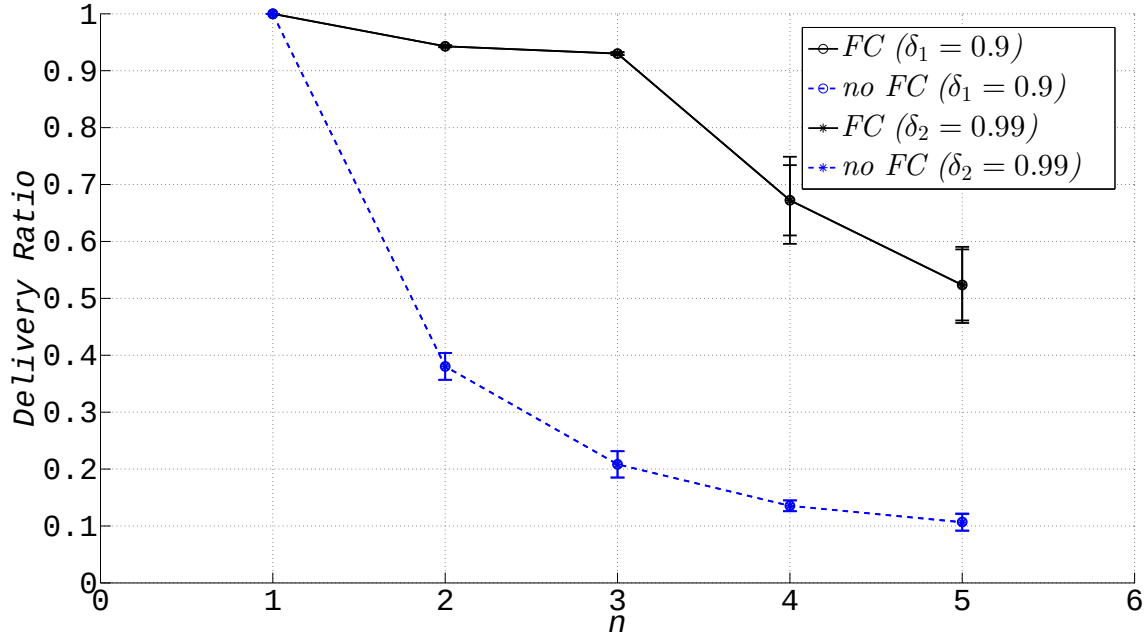


Figure 7.32: Delivery ratio for the SCP-MAC protocol with the FC effect enabled and disabled, with $\delta_1 = 0.9$ and $\delta_2 = 0.99$.

on the decrease of the delivery ratio (with the frame capture effect enabled), as the number of transmitters increases it is expected that, for $n > 8$, it is not worthwhile to apply the frame capture effect.

7.8 Summary and Conclusions

This Chapter proposes the Enhanced Reliability Decision Algorithm in the physical layer and addresses the implementation of the frame capture effect feature in the IEEE 802.15.4 compliant physical layer from the MiXiM simulation framework. The proposed decision algorithm utilizes the Signal to Noise-plus-Interference Ratio (SNIR) and the size of the packet ($nBits$) to guarantee the delivery, to the MAC layer, of a packet received at the PHY layer with a certain reliability (δ). The implementation of the frame capture effect considers five situations of packets overlapping (Interference region 1 to 5), depending on the field of the target packet that is being overlapped by the interfering packet(s). The considered regions are as follows:

- Interference region 1 - the interfering packets overlap the data field from the target data packet;
- Interference region 2 - the interfering packets overlap the data and synchronization fields from the target data packet;
- Interference region 3 - the interfering packets overlap the entire target data packet;
- Interference region 4 - the interfering packets overlap the preamble and synchronization fields from the target data packet;
- Interference region 5 - the interfering packets overlap the preamble field from the target data packet;

It has been shown that enabling the frame capture effect leads to different delivery ratio gains (G_n) for each one of the regions. Interference region 1 and 4 attains $G_n=17.43$ %, interference region 3 achieves values of $G_n=11.33$ % while interference region 2 and 5 attains values of $G_n=15.39$ % for a maximum number of eight interfering nodes. Region 3 is considered as the worst case possible (full frame overlapping), in which the frame capture is always advantageous. The Probability of Success (PS) (in the presence or absence of FC) is always higher for a reliability of $\delta = \delta_1 = 0.9$ than for $\delta = \delta_2 = 0.99$. With the increase of reliability, the minimum BER required to accept a packet is higher than for lower values of the reliability. Results are also presented for the SCP-MAC protocol, while enabling the FC effect for different values of the reliability. These results have shown that, for $n \geq 2$ with the FC effect enabled, the achieved throughput increases around 10 % compared to the case where the FC is not enabled. In the SCP-MAC protocol, since the nodes are all synchronized, the only possible overlapping scenario is the interference region 3 (the interfering frame completely overlaps the desired signal). By comparing the gains achieved (when frame capture is enabled) with the gains presented in Table 7.7 for the interference region 3, one concludes that the values are similar and consistent. Another considered performance metric is the delivery ratio, which is deeply related with the throughput when FC is enabled. The delivery ratio (for both values for the reliability) is always higher when $n > 1$. For $n > 1$, the gains achieved present a maximum value of approximately 75 % for $n = 3$, and a minimum value of approximately 42 % for $n = 5$. It is also observable that the delivery ratio gain decreases as the number of transmitters increases.

Chapter 8

Multi-Channel-Scheduled Channel Polling Protocol

This chapter proposes the Multi-Channel-Scheduled Channel Polling (MC-SCP-MAC) protocol a new protocol based on SCP protocol but envisaging multi-channel features, and is organized into seven sections. Section 8.1 describes the motivation to propose and implement a new MAC protocol for WSNs. Section 8.2 describes the main states of the MC-SCP-MAC protocol, namely the startup, synchronization, slot channel choice, discovery and addition to the network and medium access algorithm. Section 8.3 addresses the study of the fundamentals of the proposed protocol. This section comprises the enhanced two-phase contention window mechanism, packet structure, influential range concept and denial channel list. In addition, the investigation of the frame capture effect applied to the new MAC protocol is addressed in this section, as well as aspects of the extra resolution phase algorithm, useful to mitigate packet losses. Section 8.4 describes the state transition diagram for the MC-SCP-MAC protocol, jointly with the associated table of events and transitions between states. Section 8.5 addresses the comparison of different performance metrics (i.e., the collision probability, energy consumption, delay, aggregate throughput, delivery rate and throughput fairness index) between the MC-SCP-MAC and MC-LMAC, as well as SCP-MAC, CSMA and MMSN protocols. This is followed by a discussion about the achieved results. Section 8.6 presents enhancements that can be implemented in the MC-SCP-MAC protocol. Extra results of the MC-SCP-MAC protocol are given in Appendix J. Finally, conclusions are drawn in Section 8.7.

8.1 Motivation

Multi-Channel-Scheduled Channel Polling (MC-SCP) is a scheduled and channel polling multi-channel MAC protocol. Its main rationale is based on the single-channel SCP-MAC [YSH06] protocol, which is an energy-efficient medium access protocol designed for WSNs. The SCP protocol goes one step further in preamble sampling based protocols by combining scheduling with channel polling to minimize energy consumption. Compared to [HNS⁺06, YV06], the SCP's main aspects are:

- Two-phase collision avoidance mechanism employs a wake-up tone on a single channel between the two contention windows. The wake-up tone is similar to a busy tone and informs the other listening nodes of an ongoing transmission;
- It achieves synchronization by piggybacking the schedules in broadcast data packets;
- By default, nodes wake-up and poll the channel for activity. A sending node reduces the duration of the wake-up tone by starting it right before the receiver starts listening;
- Energy efficiency is also achieved, since channel polling together with the two-phase contention mechanism, mitigates the problems that may result from collisions and avoid the waste of energy.

Moreover, time-scheduled communication facilitates the coordination of multi-channel communication. Since the nodes (senders and receivers) have to switch their radio interfaces between different channels, coordination of channel switching is required. This channel switching mechanism facilitates that a sender and a receiver node to be simultaneously in the same channel, to exchange packets. Scheduled and synchronized access provides a way for the nodes to meet in the same channel.

In terms of the MAC contention mechanism, even though single window slotted contention protocols may suffer collisions as the transmitter node fails to successfully allocate the medium, SCP protocol employs a double slotted contention mechanism whilst minimizing the collisions at expense of small overhead. SCP alleviates the strict behaviour of TDMA MAC protocols (e.g., LMAC), which may lead to high values for the delay and low values for the throughput while presenting the advantage of collision-free access [lvHJH11].

In scenarios of high scalability, the proposed MC-SCP protocol is considered as an Hybrid MAC protocol. This is due to the employment of a deterministic TDMA-based channel hopping mechanism and a slotted contention basis that relies on an enhanced two-phase contention window mechanism similar to the one from the SCP protocol. Besides the SCP protocol, other mechanisms from other recent MAC protocols are also being considered and adapted, in order to increase the performance of the proposed multi-channel-scheduled channel polling (MC-SCP) protocol.

8.2 Main States of the MC-SCP Protocol

Apart from the denial channel list state nodes can be in one of the five main states: startup, synchronization, discovery-addition, slot channel, and medium access, as shown in Figure 8.1. Further details are given in Section 8.4.

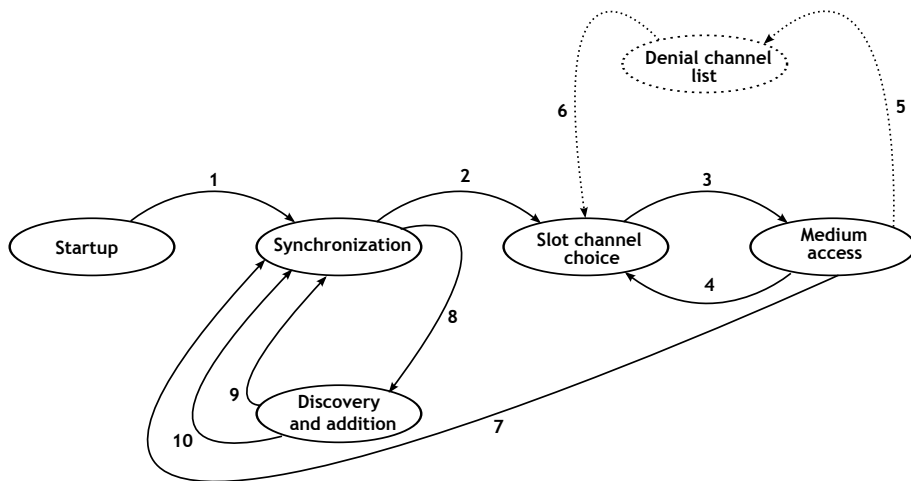


Figure 8.1: General FSM of MC-SCP.

8.2.1 Startup State

All the nodes that were recently deployed or rejoin the network, due to a reset or a battery replacement, are in the Startup state. In this state, the nodes sample the medium for an incoming SYNC packet sent by the sink node in the dedicated channel for control messages.

After the node receives the SYNC packet it synchronizes with the network and enters into the Synchronization state. Here the child nodes are the Reduced Function Devices (RFD) nodes, while the Full Function Devices (FFD) are the remaining ones (coordinator and forwarders). FFDs are considered to be the parent nodes.

8.2.2 Synchronization State

The synchronization is performed by a hierarchical scheme similar to the one from the MC-LMAC protocol [lvHJH11]. Every node synchronizes with its parent. Every node chooses a parent node from the set of nodes that are closer to the sink node in terms of number of hops. In the MC-SCP protocol, a parent node is defined as a node closer to the sink node that is at one-hop distance from the sender node. This synchronization mechanism is similar to the one employed in the single channel SCP MAC protocol [YSH06]. In the MC-SCP protocol, one of the channels is defined as the SYNC and control channel, which is dedicated to transmission and exchange of control messages, including SYNC packets. Therefore, each node has a single radio, that is used for both control and data packets [lvHJH11].

When the nodes are switched on, they go to the receive mode and the channel is, by default, the SYNC and control channel. Since the synchronization is initiated at the parent nodes, the remaining nodes (the RFD ones) are awaiting for an incoming SYNC packet. The first SYNC packet is always disseminated by the PAN coordinator [IEE07]. When the neighbours from the coordinator receive the SYNC packet, they synchronize their clock with the coordinator's clock. The synchronization continues hop-by-hop while each node synchronizes with the associate forwarder node, as the RFD node does not have a direct link with the coordinator. Since the coordinator node cannot have a direct link with every node of the WSN, some FFD nodes have to assume the function of forwarder, in order to forward the received packets to the coordinator.

Synchronization Procedures

Every node that receives packets targeted to it, is considered as a parent node. It always forwards the packets to or not to the the lower layers (until it reaches the PAN coordinator). The PAN coordinator is the only one that does not forwards packets in the WSN. The remaining nodes are the child ones. The coordinator node has a field in its address that identifies it as a unique entity in the network. The node that receives a SYNC packet from a parent node (coordinator or forwarder) is locked onto this parent node. The sensor node performs the Carrier Sense (CS) of the radio channel for collision avoidance. After performing the CS for $1920 \mu s$ if the medium is free, the sender gets access to the medium and can start the SYNC packet transmission. This SYNC packet contains fields from the address of the sender and the time of its next wake-up. Immediately after the CS the sensor node transmits the SYNC packet (21 bytes). The parent node sends a SYNC packet to the child node. This SYNC packet containing the ID of the parent node, the time when the child nodes initiate the discovery-addition state and the time when SYNC packet was sent. This waiting time allows for the child nodes to stabilize the internal registers of the microprocessor and radio transceiver.

If the child node receives a SYNC packet from a parent node, it first verifies what type of packet has been received. If the type of received packet is a SYNC packet the child node extracts the parent node ID, the time when the SYNC packet was sent (t_{tx_sync}) and updates the schedule table. Besides, it also stores the time instant when the corresponding SYNC packet was received. This time instant is obtained from the clock of the child node, which is not synchronized with the clock of the parent node yet. Based on these time instants, the child node

synchronizes its clock with the parent node clock. Some nodes may miss the synchronization with other nodes at beginning of the synchronization period, due to packet collisions that could occur on the dedicated radio channel. As a consequence, a single contention window is employed to mitigate the possible SYNC packet collisions. This scheme is further explained in Section 8.4. Periodically updating each of the schedule tables prevents long-time clock drift. This procedure of sending SYNC packets is repeated after a synchronization period, T_{sync} , but can be suppressed by piggybacking in the data packets schedules. This periodic synchronization is performed by the parent node by means of the control channel. After the first synchronization procedure the child nodes employ the piggybacking technique, in which the data packets sent to the parent node include the packet generation time. This piggybacked time instant is useful to the parent node be aware of possible child node clock drifts. Due to possible clock drifts, synchronization errors may occur from time to time. Besides the parent nodes, child ones also detect synchronization errors during their normal operation. This is achieved by using guard intervals that ensure receivers to be ready to listen before the senders start transmitting, leading to small timing differences. It has been shown in [YSH06] that, if the nodes synchronize to every frame then a maximum drift of about 2 clock ticks is observed. Hence, in this work it is considered a guard interval of 2 clock ticks before and after the expected time of a message reception, whilst considering synchronization of nodes every frame by means of piggybacking. If the child nodes detect a time difference in the synchronization clock, the nodes transit back to the start-up state. The child nodes are not the only ones that are aware of clock drifts. The parent nodes may also enable a similar mechanism. This mechanism considers a “warning” packet that is sent immediately after receiving the data packet from the child node. In the slot structure from the child node there is a field named SYNC_EM, which is a SYNC packet that it is transmitted on the same channel that the child node used to transmit the data packet. In order to save energy, the child nodes after sending the data packet perform a CS with a duration of 9 Bytes, just to check if the parent node sends any packet to set the SYNC clock.

Based on the piggybacked time synchronization information in data packets, the MC-SCP uses a technique similar to the one from EM-MAC [TSGJ11b], to keep a track of the clock drifts, after the first synchronization with his parent node. This technique is called Adaptive Time modelling that allows a sender and a receiver node to accurately predict the time of each node that sends/receives a packet. The child node keeps track of the drifts based on the modified ACK/NACK packets sent by the parent node after receiving correctly or not the data packets. With this ACK packets, there is no need to repeat SYNC packet transmission and reception for the nodes that are already in the WSN.

Implementation Details

The parent node (coordinator or FFD) broadcasts the SYNC packets only for new nodes that are in his range and have a direct link with the coordinator. This is possible because the PAN coordinator has extended processing capabilities and unlimited power supply. In MC-SCP, the child nodes model the time clock as a one-way message dissemination scheme [WCS11]. Parent nodes broadcast their timing information to various child nodes, while these nodes record the arrivals times of the broadcast message, as presented in Figure 8.2. The dependence of the current time of the child node, $T_{2,n}$, on the current time of the parent node, $T_{1,n}$, is defined as follows [WCS11]:

$$T_{2,n} = T_{1,n} + \psi + \omega + X'_n \quad (8.1)$$

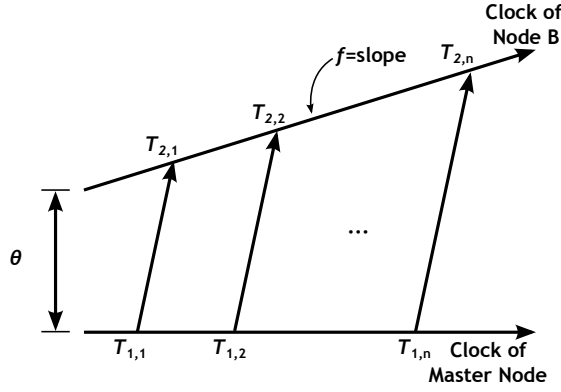


Figure 8.2: One way message dissemination.

here, the clock offset, ω , and the delay, ψ , cannot be distinguished. Nevertheless, assuming that the fixed delay, ψ , is negligible, X'_n denotes the non-fixed delays in the transmission from the parent to the child node. The clock skew, f , is the slope that needs compensation and is approximately 1. More details about this assumption are given in [WCS11]. Hence, Equation 8.1 can be approximated by

$$T_{2,n} \approx f \cdot T_{1,n} + \omega + X'_n \quad (8.2)$$

After collecting all the time stamps and putting Equation 8.2 into the form of a matrix, the authors from [WCS11] state that the Least Square (LS) estimation for f and ω is possible to be obtained. However, this procedure can be computationally demanding for the sensor node. However, if a simple adaptive clock modelling is considered, based on the reception of a SYNC packet or an ACK/NACK packet by the child node, the procedure becomes less demanding. The clock offset ω is the initial time difference between the two nodes (child and coordinator nodes). When the child node receives the first packet it assumes that $f = 1$ and models the time of the parent node using the equation $T_{2,n} = T_{1,n} + \omega$. Hence, the child node assumes the new clock modelling as his clock reference for all the packets exchange. Depending on the reception of the SYNC information from his parent node by means of ACK/NACK or SYNC packets, the child node applies an algorithm to readjust its clock model. This is achieved by considering the last synchronization time related variables as well as the new ones. This can be translated into $T_{2,0} = f \cdot T_{1,0} + \omega$ and $T_{2,1} = f \cdot T_{1,1} + \omega$, in which $T_{2,0}$ is the previous received time sample of the parent node, while $T_{2,1}$ is the more recent received time sample from the parent node. The time variables $T_{1,0}$ and $T_{1,1}$ are the corresponding time stamps when the packets from the parent node are received by the child node. Based on these time samples, the child node is able to compute the values of f and ω , which allows for the node to be synchronized with the parent node. Theoretically, the time stamps added by the child node should be exactly the time when the packet was received by the child node. However, in real sensor hardware, a gap can be induced due to several factors, such as the operating system, carrier sensing, or radio backoff. Therefore, special attention must be paid to remove possible errors that may appear while applying this method in real sensor node hardware. The work of the authors from [TSGJ11b] had the same problem and managed to remove these errors in the time stamps. A more detailed description of the EM-MAC protocol is presented in [TSGJ11b]. Another important issue is the maximum allowable deviation time between the child and the parent nodes, ρ_{dev} . If the child node needs to send a packet to the parent node within the time window allocated for the chosen channel by the child node, the clock deviation time of the child

node cannot be too large. Otherwise, the child node had changed to the same channel of the parent node either too early or too late. Based on [TSGJ11b], the time needed to switch channel is $305 \mu\text{s}$ (10 ticks) for the considered TelosB platform. They considered a hopping period much larger than $305 \mu\text{s}$ and that synchronizing nodes within 6 ticks of deviation (i.e., $\pm 183.1 \mu\text{s}$) in 95 % of the time is sufficient for this purpose. The maximum deviation time considered by the authors from [TSGJ11b] is about 60 % of the channel switch time. In our case, the considered channel switch time is $200 \mu\text{s}$ for evaluation purposes for the CC2420 transceiver. Therefore, the maximum considered deviation time considered in this work is $0.6 \times 200 \mu\text{s} = 120 \mu\text{s}$. A predictive wake-up mechanism based on a pseudo-random number generator is considered in order to properly wake-up a child node whilst turning its radio on right before the intended receiver (parent node) wakes-up the sender and the receiver for packets exchange. The full description of this pseudo-Random Number Generator (pseudo-RNG) is given in Section 8.2.3.

8.2.3 Slot Channel Choice State

This section explains the methods for channel choice, the multi-channel extension of the two-phase contention window mechanism of the SCP protocol, and for the pseudo-random number generator that defines the choice of the channel which facilitates the delivery of data packets to the parent node (coordinator or FFD node).

Predictive Wake-Up Mechanism

After synchronizing the child nodes with the parent node, the child and the parent nodes should define a way of delivering the data packets within the different channels. Since the parent node (coordinator) is continuously switching the channel, the child nodes need to know which channel the coordinator is at at a certain time instant. When the switching time interval coincide with the start of a data packet transmission, this continuous channel switching may cause packet losses. Therefore, the solution to avoid that the parent nodes are continuously switching among the channels, causing high packets losses and energy inefficiency, is to use a deterministic TDMA-based mechanism. This TDMA-based mechanism relies on the number of the channel and the start of each time interval, provided by a pseudo-random number generator. The MC-SCP protocol can use any pseudo-random function to generate the wake-up schedule for a node, based on the chosen channel of the child node. Recent MAC protocols like PW-MAC [TSGJ11a] and EM-MAC [TSGJ11b], utilize this type of pseudo-RNG to enable a sender to accurately predict the wake-up schedule rather than waking up on a truly random schedule. If a pseudo-random wake-up schedule is preferred, rather than a fixed schedule, the behaviour is also predictable, but more inefficient (e.g., WiseMAC [EHD04]). Hence, the possibility of neighbouring nodes to simultaneously wake-up for different channels is avoided. A mechanism is needed that prevents nodes from choosing different channels or the same time instant (to initiate packet transmission). As the sensor node has only one radio transceiver it can only choose one channel at a time. The number of packets lost because the parent node is not in the same channel of the sender node considerably decreases when this pseudo-random predictive mechanism is enabled. In terms of the chances of collision, the possibility of neighbouring nodes to simultaneously wake-up, may significantly increase the probability of collisions between the senders. This is verified in the PW-MAC [TSGJ11a] and EM-MAC [TSGJ11b] protocols. However, in this work, the two-phase contention window mechanism is adapted to work with multi-channels. In our case, the probability of collisions may also increase if no predictive mechanism is considered, since the senders will randomly choose the channel for the transmission in each

frame. The predictive channel based wake-up mechanism can be applied to receiver initiated duty cycling MAC protocols (e.g., RI-MAC) as well as in sender-initiated approaches, since it provides a good packet success rate performance for the sender node, when the predictive wake-up mechanism is considered. This mechanism allows for sensor nodes (senders) to deliver packets to the receiver in a rendez-vous basis. In the MC-SCP case, there are many suitable pseudo-random number generators. Since the sensor node has limited computing capabilities the best choice is the Linear Congruential Generator (LCG) [Knu97]. The LCGs are preferred to WSNs as shown in the PW-MAC and EM-MAC protocols in [TSGJ11a, TSGJ11b], since they are efficient in terms of computation and storage. The LCG generates a pseudo-random number, X_{n+1} , as presented in Equation 8.3:

$$X_{n+1} = (aX_n + c_+) \bmod(m_{l_{cg}}) \quad (8.3)$$

Here, $m_{l_{cg}} > 0$ is the modulus, a is the multiplier, c_+ is the increment, and X_n ($0 \leq X_n < m_{l_{cg}}$) is the current seed. Each of the X_{n+1} generated values can be used as a pseudo-random number and becomes the new seed. In our protocol a suitable LCG can be the one proposed in the work of Park and Miller [PM88] with the form $X_{n+1} = 16807 \cdot X_n \bmod(2^h - 1)$, to generate the different channels for a node with a unique ID in the network. The value proposed for $m_{l_{cg}}$ is equal to $(2^{31} - 1)$. The presented values for a and c_+ are chosen following the suggested premises in [Knu97], in order to facilitate that the LCG has a full cycle for all the seeds. Since the sensor nodes have limited capabilities, there is no need to use the full cycle of the pseudo-random generator for the channels. Therefore, nodes can allow for repeating the channel sequence generation after a fixed number of hops, h . This allows for nodes that are far away from each other to reutilize the same channels, with low probability of other node to choose the same channel. The number of hops, h , must be larger than the number of available channels to decrease the value of $m_{l_{cg}}$ in the LCG. Hence, we assume $m_{l_{cg}} = 65536$. Figure 8.3 presents the LCG's cyclic behaviour that is a characteristic from these generators. After 65536 calls to the LCG function, it cyclically repeats all the generated numbers (i.e., slot channels choice). Hereafter, since the channels are going to be chosen by a pseudo-RNG the channel of the physical layer is defined as a slot channel.

After each node generates the value of X_{n+1} , it must be mapped to one of the 16 available channels (N_{ch}) from the IEEE 802.15.4 standard. In this standard, one channel is dedicated to control and synchronization messages exchange. Since we consider the CC2420 as the main radio transceiver in our scenarios and it utilizes the 2.4 GHz frequency band, the associated channels are between 11 and 26, (N.B., the control and synchronization channel is the channel 11). To map X_{n+1} to a number between 0 and $N_{ch} - 1$, a modular operation is applied to X_{n+1} , as presented in Equation 8.4:

$$\lambda_{ch} = X_{n+1} \cdot \bmod(15) \quad (8.4)$$

To map to the available channel that is assumed by the node, φ_{ch} , the following operation must be performed in Equation 8.5.

$$\varphi_{ch} = 12 + \lambda_{ch} \quad (8.5)$$

The slot channel 11 is reserved for SYNC packets transmission, while the remaining ones are available for data exchange. This LCG allows for a sender node to know to which channel its potential receiver will change to, when a multi-hop network is considered. If the sender node

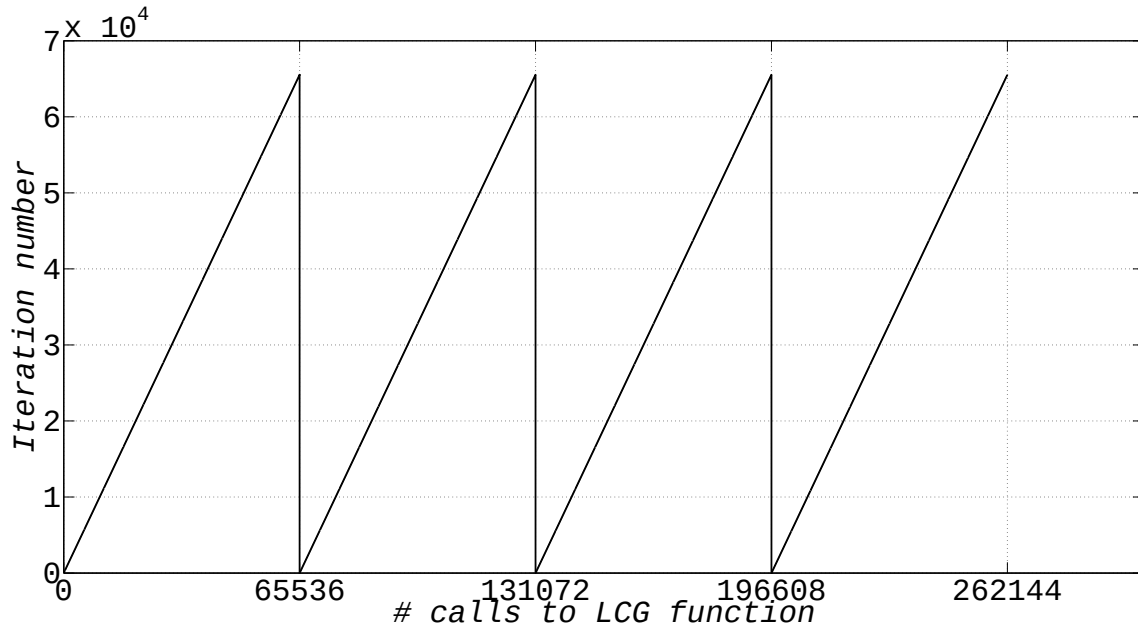


Figure 8.3: LCG cyclic behaviour.

needs to send a packet to the parent node (1-hop distance) it uses the LCG to choose the channel. However, since the PAN coordinator is hopping all the channels (frequency) during a frame, the sender node must “exactly” know when it should awake, depending on the chosen channel. Following the frame structure described in Section 8.2.5, if the sender node (after randomly choosing the channel) wants to deliver the packet to the parent node it has to wait for the proper time. Since nodes are synchronized, the sender node defines its next wake-up time, $\psi_{wake-up}$, as follows:

$$\psi_{wake-up} = \sigma_{current} + (\varphi_{ch} - 11) \times \Delta t_{SC} + \alpha_{add} - \theta_{switch} \quad (8.6)$$

where $\sigma_{current}$ is the current time of the node (already synchronized), φ_{ch} is the random channel chosen by the sender node, Δt_{SC} is the time interval that the parent node is switched to each channel, α_{add} is the time duration between consecutive frames, and θ_{switch} is the time needed by the sensor node to switch to the chosen channel. Figure 8.4 shows the probability of nodes choosing the same slot channel, P_{SC} . Here, as the number of nodes in LoS increases, the P_{SC} increases up to the maximum achievable probability (i.e., around 1). P_{SC} increases sharply for $n = 50$ and continues to increase for $n > 50$ but at slower rate, as the number of nodes increases.

Figure 8.5 shows the probability of nodes to choose the same slot channel as the size of the subset of nodes increases for neighbouring IDs of the nodes that are sequential or random. We averaged 100 Matlab simulation runs of 100000 s (in average) in each run for each point. The confidence intervals are negligible and are not presented. Here, the nodes subset corresponds to a set of nodes that present a node ID in sequence or random by, depending on the chosen scheme (sequential or random), having impact on P_{SC} . There are some differences in terms of P_{SC} when the IDs of the neighbouring nodes are sequential or random. If neighbouring nodes present non sequential IDs order, P_{SC} is lower when $n \in [20, 60]$, compared to the case of sequential IDs for the nodes. We can conclude that during a deployment if the neighbouring nodes IDs are randomly assigned the probability of a node to choose the same slot channel is

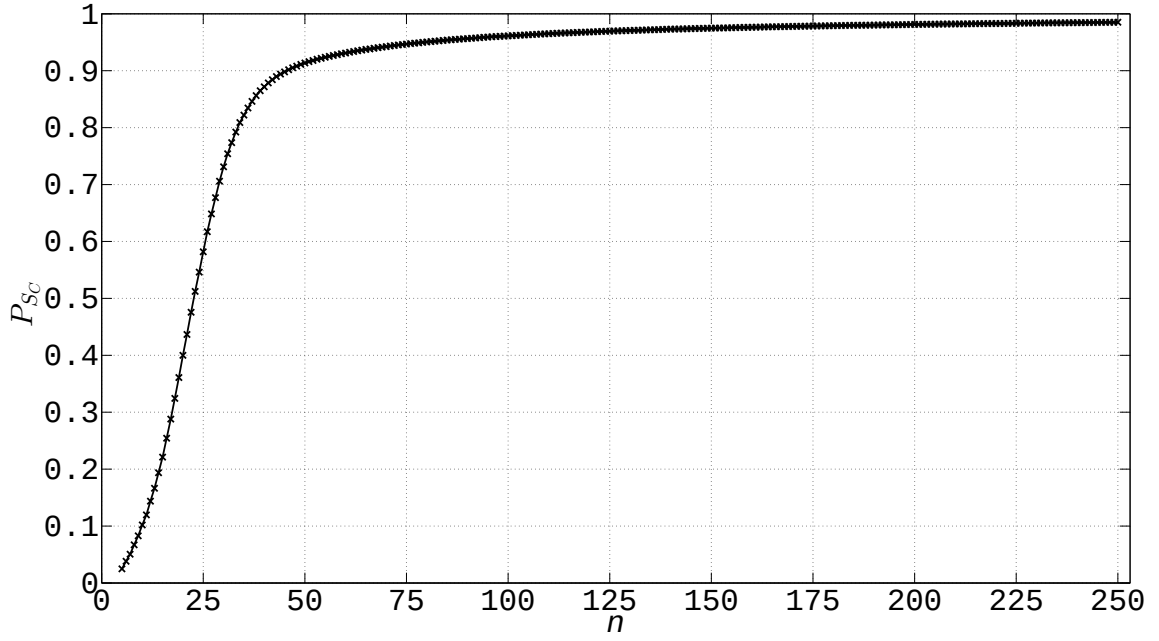


Figure 8.4: Probability of nodes choosing the same slot channel when $N_{ch}=15$.

lower than in the case when the neighbouring nodes IDs are assigned sequentially.

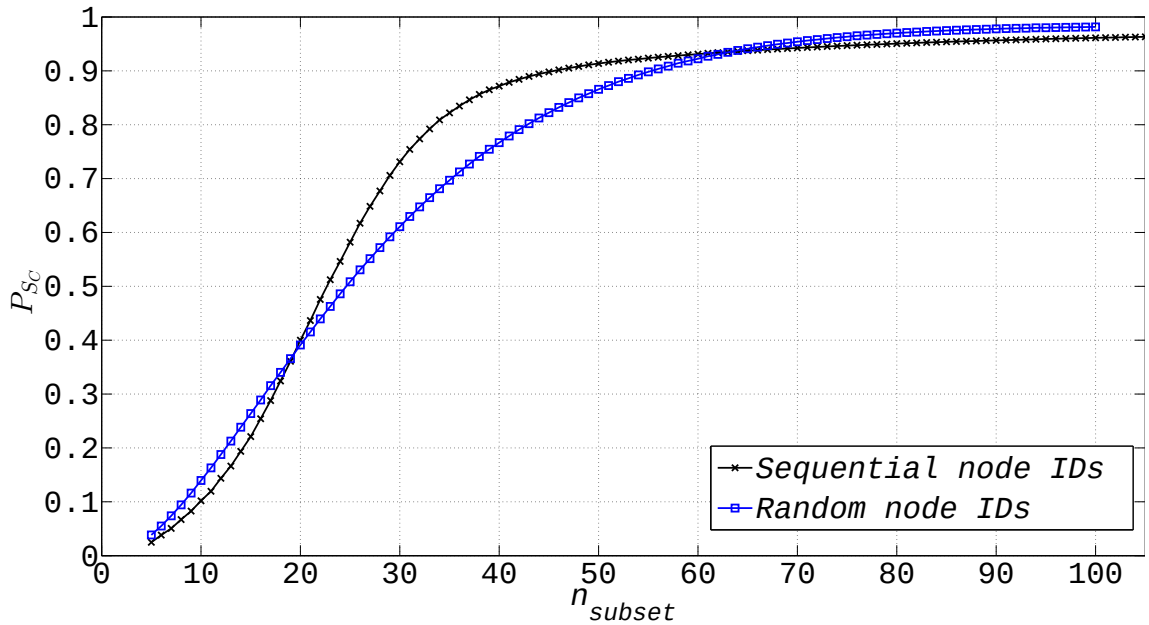


Figure 8.5: Probability of nodes choosing the same slot channel when $N_{ch}=15$ for the cases of neighbouring IDs of the nodes are sequential or random.

The sender node will wake-up only at the time when the parent node is switched to the same channel as the sender node. By employing a wake-up rendez-vous scheme, the sender nodes will save energy. If more than one node chooses the same channel an enhanced two-phase contention window scheme similar to the one employed in SCP protocol is considered, to mitigate collisions. This is going to be further developed in the proper Section 8.3.1.

8.2.4 Discovery-Addition State

In MC-SCP, the data packet includes the ID of the sender and the time when the packet was sent, along with the data collected from the sensors. Any node that receives this packet can adjust or set its internal clock and know the channel hopping sequence of the sender, based on the sender's ID, which is the seed of the LCG.

In this work, the sensor nodes that try to join the WSN for the first time must follow an algorithm that allows for joining the network and start sensing. There are two algorithms envisaged in MC-SCP-MAC protocol that allow the addition of nodes: first, the node uses the sensing node mechanism, in which it randomly chooses a channel and senses it for an initial period of 10 s. The channel choice is performed by considering a uniform distribution, as shown in Equation 8.7

$$\varphi_{ch} \in [12; N_{ch} - 1] \quad (8.7)$$

It is preferable the node performs a random channel choice based on uniform distribution than considering the LCG choice based on his ID, since it is less probable that any other node has chosen the same channel with a different seed.

When the new node detects a wake-up tone, a data packet or any packet being transmitted, it waits and receives it. With this procedure, the new node can synchronize his internal clock and assumes that the node that sends the received packet is the temporary parent node. The node is temporary because with the internal clock synchronized, the node can try to listen for the control and synchronization channel to check if it can directly communicate with the PAN coordinator. If so, it will keep the information of the 1-hop neighbour that it considers as a temporary parent node, just in case the PAN coordinator switch off or moves from the initial position (considering mobility). The time stamp stored in the packet must be taken after any queuing or any algorithm delay at the MAC layer.

If the new node does not senses any packet in the chosen channel, it will initiate a second mechanism called hopping sequencing, which hops throughout all the channels. However, it will sense each channel half or 1/4 of the maximum time a node can use each channel to communicate. By decreasing the sensing time in each channel, the number of times a channel is sensed by the node in a frame duration (1 s) is two times (if it senses half of the time of a slot channel) or four times (if it senses a quarter of the time of the slot channel). This mechanism is the last resource of the new node to join the network.

Required number of slot channels per frame

In slot contention-based MAC protocols with single channel, the required number of time slots in the MAC frame is a parameter of paramount importance. Since these protocols rely on the slot choice to perform a CS and send a packet when an idle medium is sensed, the number of time slots affects the probability of collision (i.e., characterizing nodes that choose the same slot) and the service time. The majority of single-channel slot contention-based MAC protocols (e.g., SCP-MAC [YSH06]) consider a fixed number of slots in the the MAC frame. However, some MAC protocols already consider a dynamic slot allocation mechanism. The required number of slots in a MAC frame depends on the expected number of nodes that compose the WSN. Moreover, tradeoffs must be established in the definition of the number of slots in the MAC frame by relating the number of slots, collision probability, and number of nodes. On the one hand, the choice of few slots in a high node density leads to high collision probability. On the other, the choice of a large number of slots in a low node density leads to low collision probability. However, the energy costs are higher due to the energy wasted while waiting for

packet transmission.

In the single-channel SCP-MAC protocol, within the 2^{nd} -hop neighbourhood a node should not use the same slot from the contention windows 1 or 2. Otherwise, if the sensor nodes sense the channel as idle and decide to transmit packets simultaneously a packet collision will occur.

Since MC-SCP-MAC is a multi-channel protocol, the nodes can choose one channel from the available ones to transmit their packets. As a consequence, in this case a node can use the same slot as the 2^{nd} -hop neighbours but on a different channel. In this case co-channel interference is negligible [HSSWM07]. The number of required slot channels dedicated to data exchange is calculated in the startup phase by considering the node density information. At the startup phase, since only a maximum of 15 channels can be used for a maximum number of nodes, n_{max} , deployed in the WSN, the following relation is considered:

$$N = \begin{cases} \lceil \frac{n_{max}}{2} \rceil & 0 < n_{max} \leq 2N_{ch} \\ 15 & n_{max} > 2N_{ch} \end{cases} \quad (8.8)$$

Only the default channel (slot channel 11, for synchronization purposes) is known and common to all the nodes. During the network startup the node knows the node density and assigns the number of channels to be considered by the channel choice mechanism. Here is assumed that a channel supports at most four nodes contending in the same channel. If new nodes are later added to the network, the parent node (PAN coordinator) can decide whether to restart the network or continue with the chosen number of channels. The associated collision probability is decreased by using an enhanced-two phase contention window mechanism, which considerably reduces the number of collisions compared to a single-contention window protocol (e.g., multi-channel MAC, (McMAC) [HSSWM07]).

8.2.5 Medium Access State and Algorithm

After the node starts up and synchronizes with the network while selecting the first slot channel, it enters into the enhanced-two phase contention window mechanism, corresponding to the medium access phase. In the medium access phase, the node follows the state transition diagram presented in Figure 8.6. For every packet the node wants to transmit, the node repeats the choice of the slot channel given by the LCG and the choice of the slot for each enhanced two-phase contention window mechanism phases, as further explained in Section 8.3.1 (N.B., this is one of the key mechanisms to reduce potential collisions in the same channel).

After the reception and transmission of the packets, the nodes will check if any packet is stored in the queue. If so, the child node uses the remaining time of the slot channel to send the packets without the need to perform the choice of the slot in the two contention windows. This greatly reduces the time needed to transmit all the remaining packets.

It is therefore important to explain the frame and channel assignment structure, i.e., the packet structure and the enhanced-two phase contention window mechanism involved in the message exchange procedure.

Frame and channel structure

A frame corresponds to a hopping sequence of the available channels, in which the parent node senses the data and the child nodes choose a channel to transmit their data packets. Each channel is assumed as a slot channel, S_c , as shown in Figure 8.6. The enhanced-two phase contention window mechanism is employed in each slot channel, in order to facilitate that

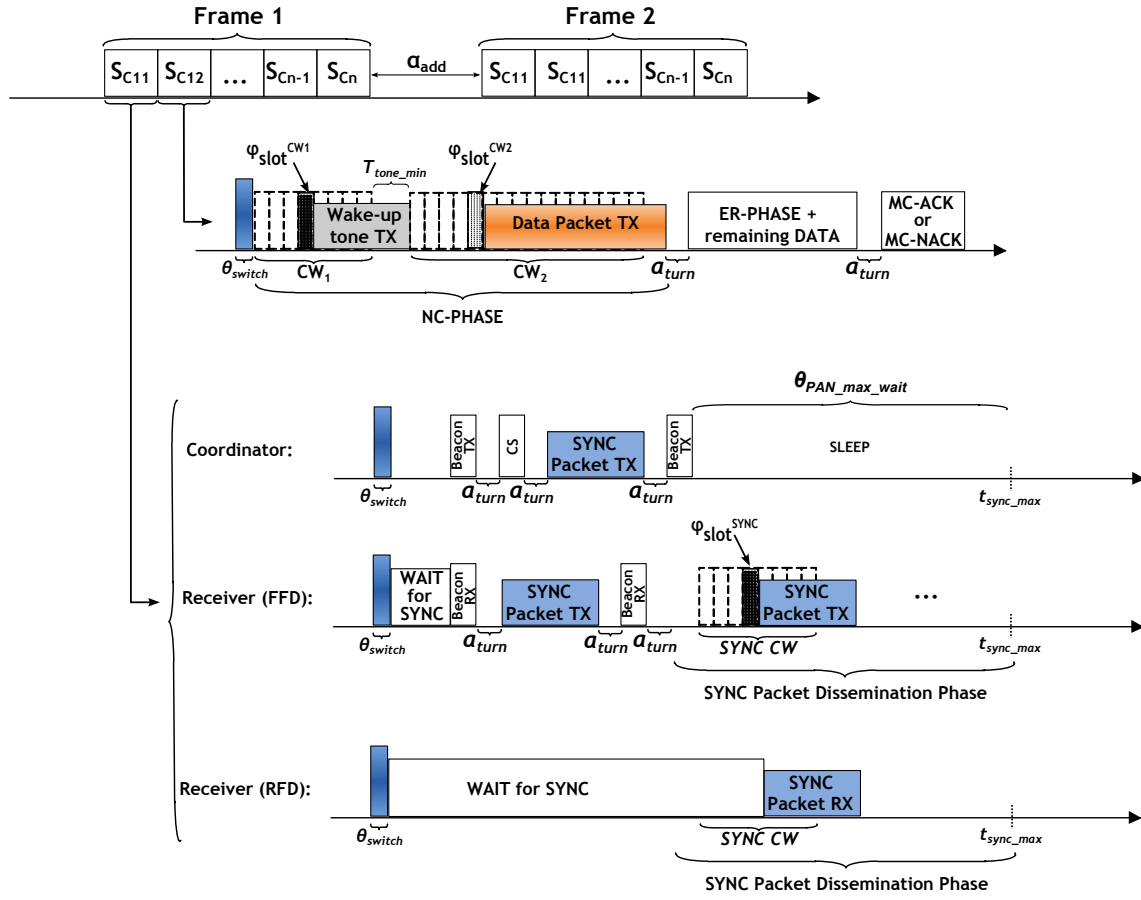


Figure 8.6: Frame structure for the MC-SCP-MAC protocol.

nodes contend for the channel. This time period is denoted as the node-contention (NC) phase. After the NC phase, the slot channel has an extra resolution (ER) phase, which can be used by the sensor nodes to transmit more packets that are stored in their queue, after winning the two phase contention window mechanism while having already sent the first data packet with no collisions. If the node needs to send more than one packet per slot channel, it must enable the “more bit” and include the number of remaining packets from the queue to be included in the control information from the first data packet sent to the parent node. This allows for the parent node to wait for the remaining packets, suppressing the need of performing all the two phase contention window mechanism when the sender needs to transmit consecutive packets to the parent node, in the current slot channel. This mechanism is already used by the WiseMAC [EHD04] protocol, in which a high performance is attained when consecutive transmissions are envisaged. After the ER phase, the node (child or parent node) will enter into the inactive phase, in which nodes go to sleep mode to save energy. The slot channel structure presented in Figure 8.6 is considered in all the available channels from the IEEE 802.15.4 standard, except for channel 11, which has a different purpose (SYNC and control packets exchange) and, consequently, a different slot channel structure. The slot channel structure for the SYNC and control channel is also presented in Figure 8.6.

The number of slot channels, S_c , is equal to the number of channels, and each slot channel

is indexed by a channel number. The slot channel S_{c11} is dedicated just for SYNC and control packets exchange, while the remaining ones ($S_{c12} \dots S_{c26}$) are dedicated to the node contention and data packets exchange. The number of slot channels on which the radio transceiver can be adjusted to, depends on the nodes density during the deployment, as expressed by Equation 8.8. However, there is the option to disable this dynamic channel adjustment, allowing for considering a fixed number of channels, independently of the nodes' density. This dynamic mechanism is more efficient for networks with low node density, since it uses less channels. The PAN coordinator will be more energy efficient, as the channel hopping sequence is performed for less slot channels, allowing for the nodes to consume less energy. In Figure 8.6, each frame has a duration of $t_F = 1$ s. The duration of each slot channel is $\Delta t_{SC} = t_F / N_{ch}$, with $N_{ch} = 16$. This means that the duration of each slot channel is $\Delta t_{SC} = 62.5$ ms. Figure 8.6 also depicts the different slot channels that are reserved for the senders of the packets whose number given by the LCG generator, is equal to the slot channel index (the first slot channel is reserved for the SYNC and control packets exchange, the second slot channel is for channel 12, and so on, up to channel 26). In the SYNC and control channel, S_{c11} , during the first time the child nodes are switched on, they initiate the sensing mode awaiting for the SYNC packet. Hence, the direct (1-hop) communication links between child and parent nodes can be established. The nodes (child and parent nodes) need to switch to the channel 11 before performing the synchronization procedure, as shown in Figure 8.6. This switching channel time in our protocol is $200 \mu s$. However, depending on the radio transceiver this switching channel time may vary. After switching to the slot channel S_{c11} , the child nodes wait for a beacon packet sent by the parent node, in order to initiate the synchronization of the nodes. As soon as the beacon packet is completely sent, the parent node initiates the transmission of the SYNC packet to the child nodes. This SYNC packet has a length of 18 Bytes. The control information in these 18 Bytes includes the time of the parent node, the source node ID, destination ID (broadcast), number of considered channels, and the next synchronization period. Once the child nodes receive the SYNC packet, they are able to synchronize their internal clocks with the clock of their parent node (the PAN coordinator). The length of the SYNC packet is equal to the one employed in SCP-MAC and is sufficient to the child nodes to receive it on time, even if serious clocks drifts persist in the child nodes. The first synchronization procedure finishes with the transmission of another beacon packet (by the PAN coordinator), to indicate to the child nodes that the synchronization procedure has finished and they could go to sleep mode until the next wake-up to send data packets. This synchronization procedure is equal to the one employed in the beacon-mode from the IEEE 802.15.4 standard.

8.3 Fundamentals of the Protocol

Since the MC-SCP protocol is a scheduled-based protocol, nodes should first synchronize in order to send and receive packets with the correct timing. To access the medium and send messages, nodes deterministically choose a channel/frequency from a maximum of N_{ch} channels (i.e., $N_{ch}=16$ channels in IEEE 802.15.4) by applying a LCG. In each channel the transmissions do not interfere with the concurrent transmissions in other channels. SCP-like double slot selection in the enhanced two phase contention window mechanism allows the node to contend for the medium and transmit its packets. The node delivers packets to the sink node in a deterministic TDMA manner, based on a pseudo-random number generator that defines the choice of the channel for the node as well as the corresponding time for the delivery to the sink node.

Table 8.1: Duration of CS, sensitivity channel switch time for CC2420 and AT86RF231 radio transceivers.

Radio transceiver	t_{CS} [μs]	S_{min} [dBm]	t_{switch} [μs]
CC2420	1920	-94	200
AT86RF231	528	-101	11

8.3.1 Enhanced-Two Phase Contention Window Mechanism

During the nodes' contention period and data packet exchange through the slot channels, an enhanced-two phase contention window mechanism, similar to the one from in SCP-MAC [YSH06], is employed. In these slot channels the contention based mechanism is preceded by the switching channel time, in order to facilitate that the child nodes communicate within the chosen slot channel. SCP [YSH06] uses two contention windows, CW_1 and CW_2 . CW_1 is divided into CW_1^{max} time slots of equal duration, as shown in Figure 8.7.

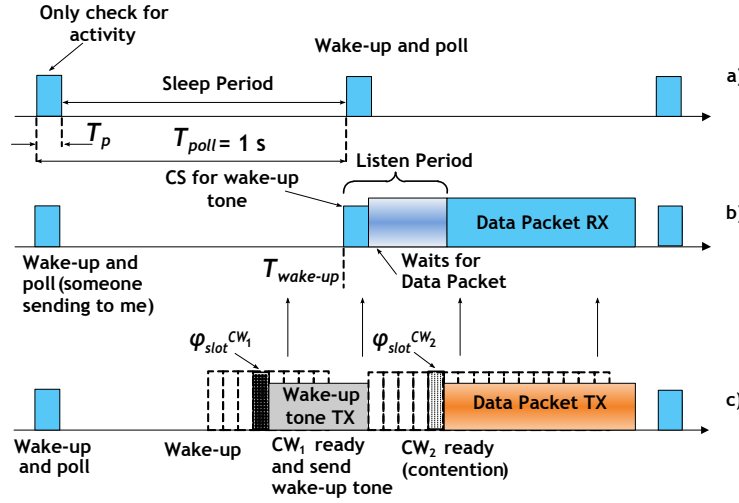


Figure 8.7: SCP two-phase contention window mechanism: a) Sensor node has neither data to send nor to receive; b) Sensor node is ready to receive data; c) Sensor node has data to be sent.

When a node wants to transmit a data packet, it randomly chooses a time slot, $\varphi_{slot}^{CW_1}$, in CW_1 , with a uniform distribution, whilst sensing the shared medium for the duration of that time slot. The choice of the slot (from the ones available in the interval) follows a uniform distribution:

$$\varphi_{slot}^{CW_1} \in [1; CW_1^{max}] \quad (8.9)$$

In our case, the first contention window is not going to be divided into slots of equal duration. Instead, the CW_1 time interval ($\Delta\sigma$) is defined, in which a node that wants to transmit a data packet will randomly choose a time value within $\Delta\sigma$, with a resolution of $\rho_{CW_1} = 32\text{ }\mu s$. The maximum value defined for $\Delta\sigma$ is two times the time required by a sensor node to perform the carrier sense of the channel, as follows:

$$\Delta\sigma_{max} = 2 \cdot t_{CS} \quad (8.10)$$

where the duration of the CS, t_{CS} , sensitivity, S_{min} , and channel switch time, t_{switch} , of the CC2420 and AT86RF231 radio transceivers are presented in Table 8.1.

The value chosen for the time to initiate the CS (of the medium) must guarantee that the CS is concluded before the end of the CW_1 . The resolution parameter defines the minimum time distance between two consecutive randomly chosen values for the CW_1 (i.e., it is the duration of a slot). However, the conducted performance evaluation tests considered the uniform slot

selection.

If no channel activity is detected (idle channel), a node sends a wake-up tone. The wake-up tone is sent after the node performs the CS, verifies that the medium is free and has a minimum duration of 62 Bytes (2 ms @ 250 kbps). This length, in Bytes (corresponding to a certain time duration) is extended for the duration of the remaining time slots (T_{subs_slots}) in CW_1 , as presented in Figure 8.8.

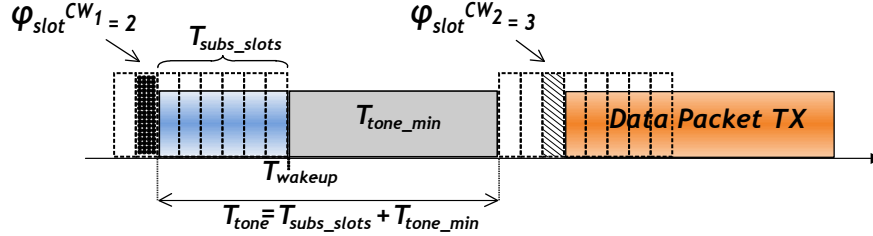


Figure 8.8: Wake-up tone duration as a function of the CW_1 chosen slot.

Like in SCP [YSH06], the wake-up tone in the MC-SCP protocol announces to other potential senders that a node is preparing to send data. The node enters in CW_2 immediately after the wake-up tone transmission. The second contention window is divided into CW_2^{max} time slots of equal duration. Only the nodes which have data to send utilize the two-phase contention window mechanism, while the remaining ones poll the channel. In both contention windows, a collision occurs if more than one node chooses the same slot (i.e., the wake-up tones collide, or simultaneous transmissions start in the same slot). Only nodes that succeed in CW_1 enter CW_2 . When more than one node succeeds in CW_1 (at least two nodes transmit the wake-up tones at the same lowest order slot), “effective” data packet collision happens in CW_2 if the nodes, which were successful in CW_1 , randomly choose the same time slot in CW_2 . This simultaneous choice of a time slot corresponds to an effective data packet collision event. If a node succeeds in sending the wake-up tone during CW_1 , it randomly chooses a slot $\varphi_{slot}^{CW_2}$ from CW_2 by using a uniform distribution:

$$\varphi_{slot}^{CW_2} \in [1; CW_2^{max}] \quad (8.11)$$

The node then starts carrier sensing in CW_2 (with a duration of about 1920 μs [YSH06]), as shown in Figure 8.7. If the channel is sensed idle, it starts transmitting its packet. In SCP, after sending/receiving the data packet, the sender/receiver node checks whether there are any new data packets pending to be sent. If so, the node repeats the steps described above before going into sleep mode. However, in MC-SCP the winning node does not perform all the procedures of the two-phase contention mechanism if it has more packets in the queue to be sent during the slot channel. If the node has more than one packet in the queue, the “more bit” and the “remaining number of packets” must be added to the control information of the first data packet sent to the parent node. If the parent node receives the data packet with the “more bit” enabled it will enable the ER phase, in order to receive the remaining packets. The child nodes are the ones that request the ER phase, based on a decision mechanism that is further explained in Section 8.3.7. The maximum allowed packets that can be received by the parent node is limited to the remaining time of the slot channel and must take into account the ACK or NACK packet sent by the parent node. It allows for reducing the queuing delay at the parent node, especially when traffic bursts are considered. If the parent node receives the first data packet with the information that the child node has more packets ready to be

sent in the queue and misses receiving the last data packet of the sequence, it has a time out timer, $t_{guard} = 400 \mu s$. This timeout timer allows for the parent node to be aware of transmission errors in the packet sequence sent by the child node. As soon as the ER phase ends, the parent node sends an ACK or a NACK packet, depending on if it receives more than one packet or node from the child node, respectively. This ACK/NACK packet has a particular structure that allows for retransmissions and synchronization of the child nodes. The packet structure is going to be further discussed in Section 8.3.2. By considering two contention stages (CW_1 and CW_2), the collision probability decreases when compared to the single contention window case with equivalent length (sum of the lengths of CW_1 and CW_2). This is because only the nodes succeeding in CW_1 enter into CW_2 . This choice decreases the number of nodes effectively accessing the medium during the second contention stage. After the first phase of the contention procedure, only the successful nodes from CW_1 (the first one(s) that transmit the wake-up tone) contend in CW_2 . With less contending nodes, the effective collision probability is considerably reduced. Each slot channel can accommodate the transmission of multiple data packets from the child node that wins the contention, as shown in Figure 8.6. Each slot channel has a fixed length, but the NC and ER phases duration varies according to the number of data packets involved and the choice of slots in CW_1 and CW_2 . Since the number of slot channels depends on the number of nodes initially deployed, the nodes may maintain the same frame time, t_F , and use one of the 15 channels, leading to lower energy consumption.

8.3.2 Packet Structure

In order to establish communication between child and parent nodes, different packets are needed. In the context of MAC protocols, data and control packets are involved in the communications. The content of the data packet transmitted during the NC or ER phase are as follows:

- **Source ID:** it represents the node ID of the sender;
- **Destination ID:** it represents the node ID of the parent node (receiver);
- **Slot channel (S_c):** it represents the chosen channel;
- **Data:** it represents the sensor data sent to the parent node;
- **Current time stamp of the source:** it represents the time instant when the child node sends the data packet, and is used for synchronization by new nodes that try to join the WSN;
- **More bit:** a sensor node receiving a data packet with this bit set will continue to listen the current slot channel after finishing receiving the first data packet;
- **Number of remaining packets:** it represents the remaining number of packets that are in the sender's queue (if the "more bit" is enabled, this field is used by the parent node to know how long it must remain in the receiving mode, to receive the remaining data packets);

Figure 8.9 shows the corresponding fields for the data packets, along with their length. The control packets that may be exchanged during the MC-SCP are the following:

- **SYNC packet:** it contains synchronization information for the child nodes (with a fixed length);

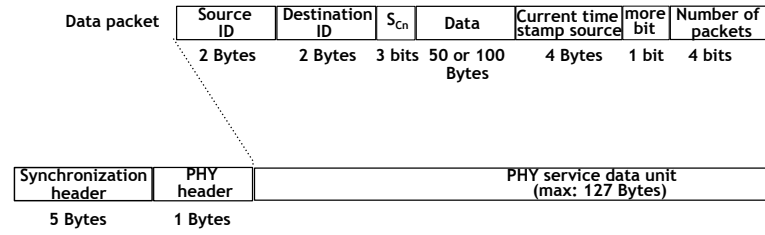


Figure 8.9: Structure for the data packet in the MC-SCP-MAC protocol.

- **Wake-up tone:** it contains the source ID, destination ID, current time stamp of source, and a field with random data (dummy bits) only used to occupy the packet (with variable size, and minimum length of 62 Bytes);
- **Beacon packet:** it consists of a packet that is used only to signal the beginning and end of the synchronization phase, and has a duration of 0.7 ms [BMS⁺08];
- **ACK packet:** consists of a packet that contains the source ID, destination ID, missed packets from sequence and current time of the parent (with fixed length);
- **NACK packet:** it consists of a packet similar to the ACK one, corresponding to the cases when the parent node does not received any data packet (with a fixed length).

Some modifications are needed in some control packets, such as the beacon, ACK, and NACK packets compared to the IEEE 802.15.4 standard. This was decided to enable that the MC-SCP-MAC protocol presents higher agility with multi-channel.

The content of the SYNC packet is similar to the beacon packet in IEEE 802.15.4. However, here the SYNC packet has a length of 18 Bytes.

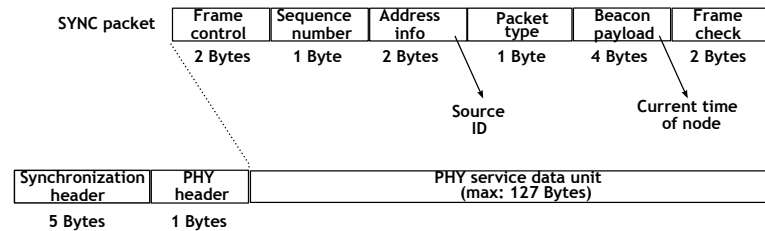


Figure 8.10: Structure for the SYNC packet.

To comply with the IEEE 802.15.4 standard, the SYNC packet format has to be modified without removing any field of the packet needed. The required modifications are the addition of the field “packet type”, which allows for the child nodes to check that the received packet is the SYNC one, and the consideration of 4 Bytes in the “beacon payload” field, to store the current time of the parent node, for synchronization purposes (internal clocks) in the child nodes. The wake-up tone is a packet whose fields are similar to the IEEE 802.15.4 beacon packet ones. However, it has a variable length (and a minimum length of 62 Bytes), since it depends on the remaining time/slots of the CW_1 in the NC phase. The content of the wake-up tone transmitted during the NC phase is shown in Figure 8.11. Compared to the IEEE 802.15.4, the only difference is in the beacon payload fields. The first field is the “packet type”, whose “wake-up” type is denoted by “2”. The second field is the “destination ID”, which, in this case, must be from the broadcast type, since the tone is used to warn potential contenders that other node has already won the medium in the CW_1 . Since this wake-up tone is from the broadcast type, a field named as “current time of the child node” is added to the packet structure, in order to enable

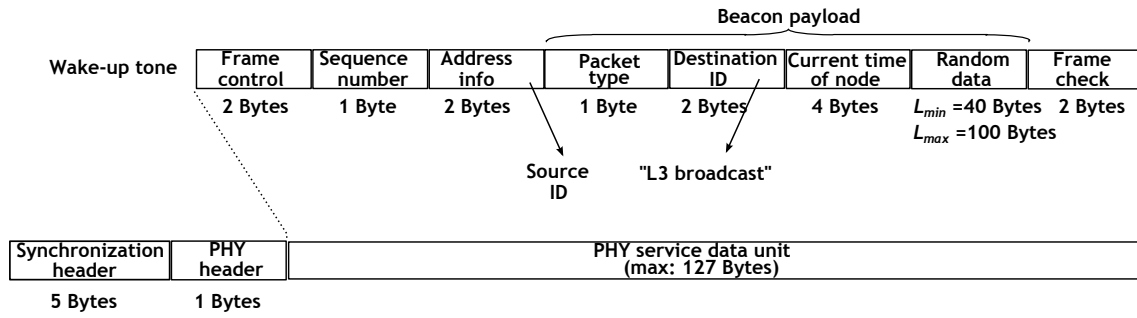


Figure 8.11: Packet structure for the wake-up tone in the MC-SCP-MAC protocol.

that other child nodes that are in the same slot channel and in the discovery-addition phase are able to obtain the first clock synchronization. Moreover, the parent node can keep track of the internal clocks of the child nodes and warn the child nodes when the clock drift is higher than the maximum allowable deviation, $\rho_{dev} = 120 \mu s$. The “random data” field presents a variable length and is used to increase or decrease the wake-up tone, depending on the remaining slots of CW_1 . Considering the default fields lengths, the “random data” field length varies from 40 Bytes up to 100 Bytes.

The content of the beacon packet is the one from the IEEE 802.15.4 standard, as presented in Figure 8.12. Since the beacon frame has to present a duration of 0.7 ms, the required length

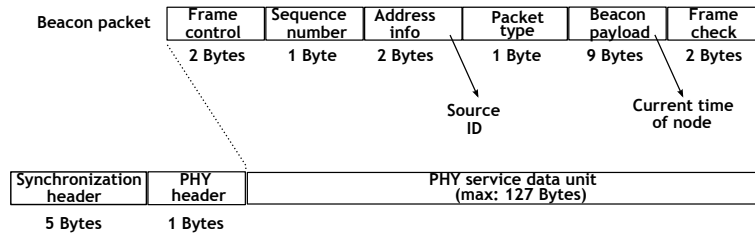


Figure 8.12: Beacon packet structure for the MC-SCP-MAC protocol.

for the field “beacon payload” is equal to 9 Bytes. With a total of 22 Bytes, the duration of the beacon packet is around 0.7 ms.

The ACK packet structure from the IEEE 802.15.4 standard, requires some modifications to facilitate that the MC-SCP protocol achieves a better performance. This modified ACK packet is named as MC-ACK packet. Its structure is simpler than the structure of the packets presented before. The contents of the IEEE 802.15.4 ACK packet and the necessary modifications to obtain the MC-ACK are presented in Figure 8.13. Compared with the standard structure of the IEEE

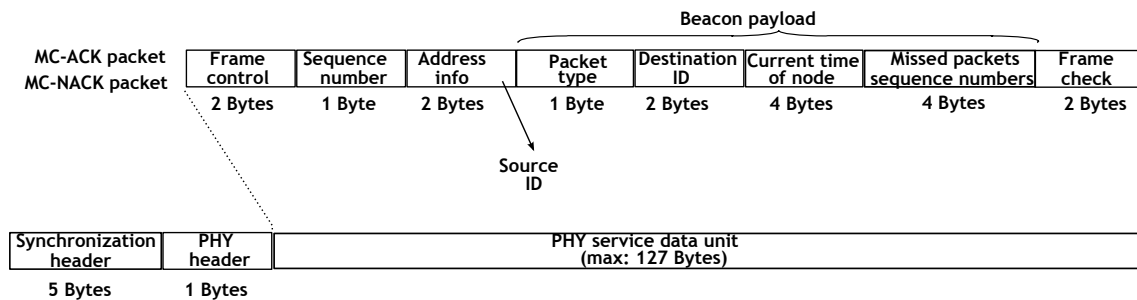


Figure 8.13: Structure for the MC-ACK and MC-NACK packets.

802.15.4 ACK packet, we verified the need to expand the structure, in order to include other important information, such as the “current time of the parent node”, the missed packets se-

quence number, as well as the packet type, source ID and destination ID fields. The new ACK packet allows for suppressing the explicit synchronization packets, since all the child nodes that are in the same slot channel receive the MC-ACK packet and use it to synchronize their internal clocks. As shown in the SCP MAC protocol [YSH06], the synchronization piggybacked in packets is truly efficient. If the parent node does not receive a data packet after sensing the wake-up tone in a slot channel, it sends a MC-NACK packet after the timeout timer expires. For the MC-NACK packet, the structure is similar to the MC-ACK packet presented in Figure 8.13. The “packet type” field is “5” for this type of packet.

Here, the overhearing of the MC-ACK and MC-NACK packets, by the child nodes that contend in the enhanced-two phase contention window but did not win the access to the medium, is considered to be beneficial. These child nodes receive the packet only to extract the synchronization information of the parent node.

8.3.3 Influential Range Concept

In IEEE 802.15.4 compliant WSNs, the overhearing problem appears during any normal operation of the network, and is widely considered as an energy waste in various MAC protocols implementations, as mentioned in [LGF07]. In [LGF07], the authors propose a so-called Influential Range (IR) that takes advantage of the overhearing in order to save energy. When a node sends a packet all the other nodes can overhear this packet. Considering contention based MAC protocols, the node(s) that loses the channel, changes to the receiving mode in order to listen to the transmission. It listens to the full transmission of the packet to know the packet destination. If the packet destination is not meant to it, then it simply drops the packet (overhearing problem). The authors from OB-MAC [LGF07] consider that, based on this overhearing, nodes in the same area probably sense the same information. Hence, all the nodes in a given area sense the same phenomenon, leading to the delivery of the same information to the sink node. This redundant transmission can be avoided by comparing packets with the ones in the queue, therefore reducing the energy waste.

In the majority of the MAC protocols, when a node receives a packet not intended to it, it simply discards the received packet. However, it spends time to receive it and decode it. After receiving and decoding the packet if it verifies that the packet destination ID is not equal to the node’s ID, then it discards the packet.

Based on this technique, even if the packet destination is not itself, the node compares the overheard packet with the stored packets in queue, if there is any packet containing the same information to be sent to the sink node. If so, the node discards the packet from the queue, since the same information has been already sent by neighbouring node(s). If the overheard packet information does not match any of the packet’s stored in the queue, the node discards the overheard packet and tries to send the packets stored in the queue at the proper time.

The authors from [LGF07] define the concept of influential range, which is a range where the nodes are likely to observe the same information. The IR must always be lower than the maximum achievable range of the radio transceiver, as shown in Figure 8.14. In Figure 8.14, the small circle is considered as the influential range, while the outer circle is the radio range. The employment of the IR concept by the authors of OB-MAC is restricted to a single channel. As it clearly presents improved energy efficiency due to the reduction of redundant transmissions, we strongly believe that applying the IR concept to a multi-channel MAC protocol, such as the MC-SCP, will lead to energy efficiency gains.

To achieve this energy efficiency, some premises must be fulfilled in order to decide when the

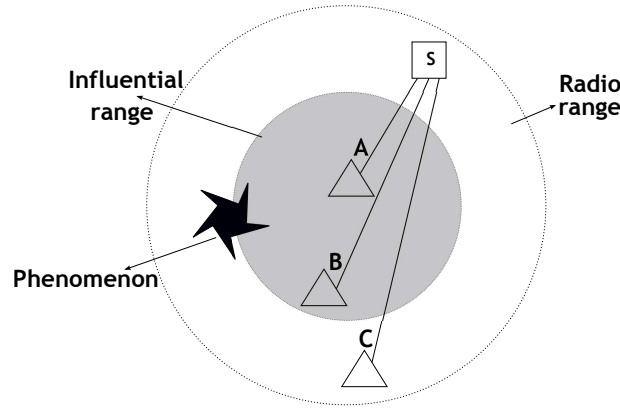


Figure 8.14: Influential range.

IR can be applied to the MAC protocol. The IR concept states that a node applies this technique if and only if it is within the influential range of the transmitting node. When the phenomenon has taken place, all the nodes that are within the area enable the IR verification. To apply this decision assertions, the node that overhears a packet needs to know if it is within the IR of the node that has sent the overheard packet while having the same parent node. Therefore, a suitable indicator of whether the node is in the IR, is the RSSI from the overheard packet. If the RSSI of the overheard packet is higher than a defined sensing range threshold (Π_{irmax}) the node is in the same IR. Otherwise, if the RSSI is lower than Π_{irmax} , the node is not in the same IR. If the node that overhears the packet is in the IR, the overhearing node performs information comparison.

As shown in Figure 8.14, if nodes A, B, and C contend for the channel and only node B wins the channel, while the remaining ones continue to listen to the medium. The node B sends its packet to the sink, but the nodes A and C overhear the node's A packet. Both nodes (A and C) verify if node B is in the same IR. If the node A checks that the RSSI of the overheard packet is higher than Π_{irmax} , then it verifies if any packet stored in the queue has the same phenomenon information. If so, it discards the packet stored in the queue. Otherwise, it sends the packet in the next attempt to transmit. For the node C, the comparison of the RSSI from the overheard packet with the value of Π_{irmax} allows for deciding of the packet is to be discarded (or not). Since the RSSI is lower than the threshold, the overheard packet is discarded and the queued packet is sent later. The defined threshold depends much on the density of nodes in the WSN. The more dense the WSN is the more overheard packets the nodes will receive in their IR. Therefore, reducing the value of Π_{irmax} will save more energy. The values of Π_{irmax} considered by the authors from OB-MAC protocol varies between -90 and -60 dBm.

8.3.4 Denial Channel List

In single-channel MAC protocols, the sensor nodes do not have the possibility to choose other channels when one of the channels is degraded due to severe interference. However, in multi-channel MAC protocols, as this degradation may also occur, the multi-channel MAC protocol can sense the channel conditions to mitigate this problem, in order to optimize the set of channels that present a higher reliability.

A similar mechanism is already considered by the EM-MAC [TSGJ11b] protocol. Nevertheless, in our case the MC-SCP differs on the EM-MAC, since it is based on a two-phase contention window mechanism based on slots to resolve the access to medium, while the EM-MAC is based

on the CSMA scheme. Also this decision is performed at the application layer, which considers a cross-layer design in MC-MAC and allows for the WSN application to use this sensing information for cognitive radio purposes.

Table 8.2: Reward and punishments for the degradation level metric from the denial channel list policies in MC-SCP-MAC.

Case scenario	Reward	Punishment
Performs CS in CW_1 and detects a free medium	+1	-
Performs CS in CW_1 and detects an occupied medium	-	-1
Performs CS in CW_1 passes to CW_2 and detects a free medium	+1	-
Performs CS in CW_1 passes to CW_2 and detects an occupied medium	-	-1
Performs CS in CW_1 passes to CW_2 and detects a free medium and wins contention in CW_2	+2	-
Performs CS in CW_1 passes to CW_2 and detects a free medium but loses contention in CW_2	-	-2
Performs CS in CW_1 , detects an occupied medium, receives successfully the data packet	+2	
Performs CS in CW_1 , detects an occupied medium, detects a data packet collision	-	-2
Node without data to TX, performs CS in CW_1 , detects an occupied medium, receives successfully the data packet	+2	-
Node without data to TX, performs CS in CW_1 , detects an occupied medium, detects a data packet collision	-	-2
Node receives a MC-ACK packet with success	$+1 \times n_{packets\_tx}$	-
Node receives a MC-NACK packet with success	-	$-1 \times n_{packets\_tx}$
Node TX data packets but does not receives MC-ACK or MC-NACK packets	-	-2
Timeout of the timer to receive MC-ACK or MC-NACK packets	-	-2
Timeout of the remaining timers in MC-SCP-MAC	-	-1

Each node maintains a denial channel list which contains the levels of “degradation” of each channel. This “degradation” level is a non-negative metric. When a node chooses a channel to transmit a packet, it switches to the chosen channel and performs a first CS within the CW_1 . If the node detects an idle channel it decreases the degradation level of the channel in one unit (the metric cannot be lower than zero), and passes to the second contention window (CW_2). Otherwise, the node increases the channel degradation in one unit. The nodes that passed to the CW_2 will perform another CS to the channel. In case an idle channel is sensed, the degradation level of the channel is decreased in one unit. Otherwise, the same metric is increased in one unit. Other conditions imposed to channel’s degradation level consider that a data packet collision increases the degradation metric by two units in all the nodes that won access to the CW_1 but lost the contention in the CW_2 while detecting a data packet collision. Besides, if a node sends a data packet and does not receives a MC-ACK it increases the channel’s degradation level by two units.

Based on the channel degradation level stored in the denial channel list, a node in MC-SCP

restricts the selection of channels it switches to. Since this denial channel list is locally maintained by each node, the node decides that a channel is considered severely degraded if the degradation level metric is higher than a defined threshold, D_{ch} . If so, the channel is added to the denial channel list and is avoided by the node during the data packet transmission. If the node chooses a degraded channel based on its pseudo-random generator, the node always chooses the next channel given by the pseudo-random generator and increases the sequence number from the sent of packets by one unit.

The maximum number of channels stored in the denial channel list is the total number of considered channels minus one. This limitation is required for the cases when all channels are considered degraded. However, the least degraded one is removed from the list. This forces the node to use a single-channel until the remaining channels reduce their degradation level metric and get removed from the denial channel list. If the number of degradation channel levels was not limited to the total minus one, the node can get isolated from the remaining nodes, mainly due to the restriction of not being allowed to use any channel to communicate. The denial channel list policies for the degradation level metric in the MC-SCP-MAC simulator are summarized in Table 8.2. The degradation level metric allows for the nodes to consider the less degraded slot channels, which leads to a more efficient use of the medium to transmit the data packets.

8.3.5 Frame Capture

Existing MAC protocols assume a typical physical layer based on the IEEE 802.11 standard. In this context, when the radio transceiver simultaneously detects two frames the occurrence of a collision is assumed. The frames will interfere with each other. As a consequence, the receiver will not be able to decode either one of them. Although this is theoretically true, in the last years, the work from some researchers [LRLK08] has shown that this assumption is not absolutely true.

Under certain channel conditions and circumstances, the frame capture effect occurs when the strongest signal causes the other signals to be treated as noise (or interference) and is filtered out by the receiver. As a consequence, a packet is received even though a collision occurred due to concurrent transmissions [LRLK08]. This phenomenon (of being able to receive a frame even in the presence of another interference frame) is called FC effect. This effect neglects the assumption of “*collision as failure*” in which packet collision leads to packet corruption. This assumption is commonly accepted in simulations [WWJ⁺05, SKA04], theoretical analysis [KT75], and collision avoidance schemes [PCB00]. The FC effect is considered in our MAC protocol due to the beneficial revenues that it can offer, such as prevention of packet collisions, increase of the network throughput, and decrease of the delay. In theory, frame capture can provide additional gains through collision detection and the recovery of the strongest packet from collisions [WWJ⁺05].

The FC effect is going to be considered in the simulations of the MC-SCP, but it can be disabled to observe how the MAC protocol behaves when this effect is not considered. The FC effect simulator implementation and work principles were discussed before in Chapter 7. Besides the FC effect implemented in the simulator framework, a reliability decision algorithm has also been implemented, jointly with the FC effect. This decision algorithm allows for the physical layer to decide whether a packet is correctly decoded or not. It tries to mimic the real-world constraints in the simulator, in order to decide if it accepts the packet based on the channel conditions.

8.3.6 Node Topology and Envisaged Real-World Scenarios

The IEEE 802.15.4 standard supports three types of networks topologies: star, peer-to-peer and tree topologies. Depending on the application of the WSN, a different topology can be chosen. The star topology does not ensure a reasonable scalability of the network. Besides, the peer-to-peer topology does not guarantee low energy consumption, since nodes are always active. Since the tree topology supports a higher scalability and presents low energy consumption, we focus on this topology as presented in Figure 8.15. The verification of the MC-SCP-MAC performance also aims at implementation on real-world scenarios. It is designed for dense deployment scenarios, such as tracking and localization, environmental monitoring or intrusion detection applications. Some works have been already done for the environmental monitoring, such as the one from the authors [TPS⁺05]. In turn, for the intrusion detection application the authors from [ADB⁺04] developed an application capable of detecting, classifying and tracking a target.

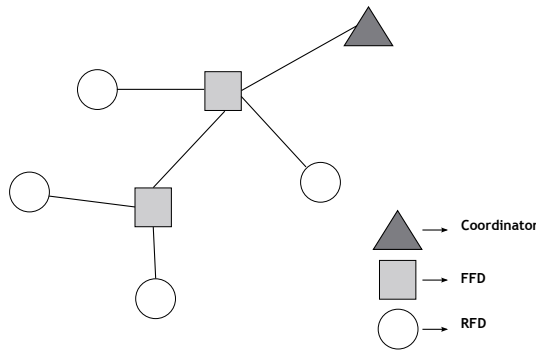


Figure 8.15: Considered topology: full tree topology scenario.

The MC-SCP MAC protocol considers the IEEE 802.15.4 standard. The sensor nodes are divided into two types: FFD and RFD. The FFD are capable of sensing events and route packets to other nodes. While the RFD has limited capabilities, since these devices can only communicate with FFD and perform the sensing of phenomena. Moreover, the FFD can support two types of roles:

- **PAN coordinator:** the PAN coordinator is the primary controller of the PAN. It initiates the network and often operates as a gateway to other networks. Each PAN must have exactly one PAN coordinator;
- **Coordinator:** is a FFD capable of relaying messages using data routing and network self-organization operations to achieve it.

In our case, we consider a coordinator that collects and processes information sent from the sensors (RFD and FFD). When an event is detected in a given area, every node senses it, creates a packet and sends the packet to the sink node (coordinator or parent node) throughout the FFD if multi-hop is considered. In multi-hop scenario the FFD forwards the packet to another FFD, until the packet reaches the coordinator.

The scenario presented in Figure 8.15 is considered as the full tree topology scenario. In order to observe the behaviour of the MC-SCP MAC protocol in single- and multi-hop scenarios, simpler scenarios have to be considered for evaluation purposes. Figure 8.16 (a) presents a topology where all the RFD nodes (child nodes) are directly connected to the sink node (coordinator or parent node). In the case of single-channel, if C is the aggregated throughput (i.e., the capacity of the medium), then each of the RFD entities from Figure 8.16 (a) theoretically transmits a

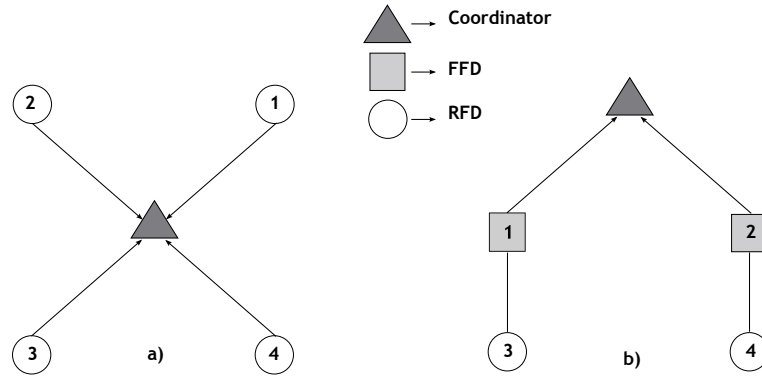


Figure 8.16: Considered single- and multi-hop scenarios.

capacity of $C/4$ per RFD. In the multi-hop case, presented in Figure 8.16 (b) if a suitable scheduling mechanism is considered (no interference between nodes) an aggregated throughput per node of $C/4$ is achievable. If no scheduling mechanism is considered, all the transmissions will interfere with each other, leading to throughput decrease. The achievable throughput drops to $C/6$ per node, since RFD 1 and 2 have to forward RFD 3 and 4 packets besides their own packets. By considering non-interfering channels (multi-channel based), the interference can be eliminated and the RFD and FFD can achieve a maximum aggregated throughput per node of $C/4$.

These scenarios are useful for comparison with the MC-LMAC protocol [lvHJH11]. Since MC-SCP protocol is based on SCP-MAC protocol [YSH06] it is worthwhile to compare both protocols in order to verify the improvements from using multi-channel based schemes. Other scenario that is going to be considered is the chain scenario (multi-hop) one, as it allows for observing the end-to-end delay of packets, as shown in Figure 8.17. The presented topologies are considered in the next sections to address the efficiency of the multi-channel MAC protocol, MC-SCP.

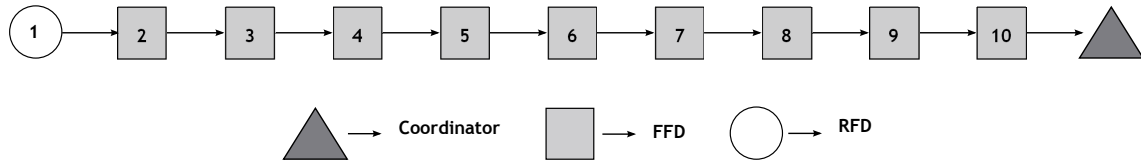


Figure 8.17: Chain scenario (multi-hop).

8.3.7 Extra Resolution Phase Decision Algorithm

Each slot channel has an ER phase, which can be used by the sensor nodes (child nodes) to transmit more packets that may exist in their queues after sending the first data packet. Since the channel can be degraded due to interference, or the nodes may move to other positions (mobility is considered), the node may transmit the data packets unnecessarily, since they will not be received by the parent node. Therefore, a decision algorithm is required to decide whether a child node sends all queued packets during the ER phase. The decision is based on the SNIR from the packet, the “degradation” level of the slot channel and the neighbouring nodes of the child node that intends to transmit the remaining data packets. The first component of the decision algorithm is based on the degradation level from the slot channel, already defined for the denial channel list. While the second component of this algorithm is based on the IR concept, on the last three accesses of the child node to the medium and the corresponding

packet delivery results.

A node that has more packets in queue to transmit compares the degradation level of the current slot channel (stored in the denial channel list) with the threshold, D_{ch} . If the channel is considered has “good” to send packets, then it passes to the second phase of the EC phase decision algorithm. In the second phase, the node checks the last three calls of the influential range algorithm. If the node receives at least three positive feedbacks in the IR algorithm for that channel for the same neighbouring nodes, then the node can use the ER phase to transmit the remaining packets stored in queue. In case the IR algorithm feedback is not possible to be checked, the node will check in the last three channel transitions if it has successfully transmitted the packets to the parent node. If so, then the node can utilize the ER phase to transmit the packet in the queue.

8.4 State Transition Diagram and Description

Nodes are in the *startup* state (Figure 8.1) when they are recently deployed or rejoin the network, due to hardware reset or batteries replacement. During the *startup* state the node senses the medium for an incoming packet to synchronize with the network. To achieve this, the nodes switch to channel 11, which is the SYNC and control slot channel and wait for the parent node to send the SYNC packet. When the nodes are switched on, they wait for 10 s to stabilize and switch to the SYNC and control slot channel and start sensing the medium. It is assumed that the parent node is also switched on during the first 10 s, but it sends the first SYNC packet only after another 10 s. This allows for the child nodes stabilize properly the hardware related issues and be ready to receive the SYNC packet. If such packet is received, a node passes to the *synchronization* state and synchronizes with the parent node (who sends the SYNC packet). For the cases of child nodes with no direct link with the parent node, the child node has to send his packets to a FFD node and consequently the FFD node relays the packets to the parent node. To achieve this goal, during the *synchronization* state the nodes that receive the SYNC packet will have to retransmit this SYNC packet in the next attempt. This is essential for the nodes that do not have direct communication with the parent node and need to send their packets to the parent node. Therefore, the nodes that are going to retransmit the SYNC packets will utilize a slot choice based on a single contention window, since other nodes will utilize the same channel to retransmit SYNC packets during the *synchronization* state. After winning the access to the medium and retransmit the SYNC packets for the other nodes, it will be assumed by the nodes as their parent node.

Once the *synchronization* phase finishes, a node follows the schedule to deliver packets to the coordinator (single-hop) or the FFD (multi-hop). If a node needs to join to the network after the *synchronization* phase (with a maximum duration of 1 minute) it enables the first of the two mechanisms that allows for the synchronization. If the random channel slot selection algorithm allows the node to synchronize with a parent or FFD node, then it passes to the *synchronization* state. If the first mechanism fails, the node initiates the fast slot channel hopping mechanism (a secondary mechanism). Both these mechanism are fully described in Section 8.2.4. If the new node has success in one of these mechanisms, it enters in the *synchronization* phase. After the network synchronization, the child nodes wake-up periodically, to check the medium for any potential incoming packets. This check lasts for 1920 μ s (time to perform the CS) and only occurs when the node does not have any packets in queue to be sent. The slot channel choice is given by the current pseudo-random generator value. If it does not detect any traffic during

the CS, the node goes immediately to sleep mode, whilst scheduling the next wake-up. If the node has packets in the queue (it senses an event) it transits to the *slot channel choice* state. Here, the node chooses and switches to slot channel given by the pseudo-random generator of the parent node. Then, it passes to the medium access phase, in which it contends for the channel by employing the enhanced two-phase contention window mechanism. If the contention is successful in both contention windows the packet is transmitted and waits for the MC-ACK. If the contention fails, the node waits for the MC-ACK packet that may utilize to synchronize his internal clock.

Each generated packet will make the node to transit from the *medium access* state to the *slot channel choice* state, in order to the node gets the corresponding slot channel of the parent node and the time instant when the parent node is in the current slot channel. After a node collects the slot channel information, it enters into the *medium access* state, in which it performs the two-phase contention window mechanism resolution. If the node receives a warning of collision in a specific slot channel, it transits to the *denial channel list* state. After updating the degradation level of the slot channel in the Denial channel list, the node(s) passe(s) to the *slot channel* state. If a node detects or is warned by the parent node that the synchronization error is higher than the maximum allowable deviation time, ρ_{dev} , then the node transits to the *synchronization* state, to resynchronize its internal clock. The nodes enter in the *discovery and addition* state in two situations. First, when the nodes fail to receive a SYNC packet from a parent node, the node transit to the *discovery and addition* and tries to resynchronize later. Second, when nodes are turned on and try to join the WSN, the nodes try to receive a SYNC packet from a parent node.

We have proposed a possible FSM. The objective of this FSM is to give a detailed specification of why and how the simulator changes between the different states, while explaining the associated actions and events as shown in Figure 8.18. The corresponding transition events and actions are listed in Table 8.3.

This state machine is based on twenty five states, described as follows:

- **STARTUP:** The node is switched on;
- **WAIT FOR SYNC:** The node is waiting for SYNC packets. It switches to the SYNC and control slot channel ($S_C = 11$);
- **SYNCHRONIZATION:** All the nodes, during the startup, switch to SYNC and control slot channel and listen for the incoming SYNC packet sent by the coordinator. The synchronized nodes retransmit the SYNC packets to the neighbouring nodes by employing a SYNC contention window;
- **RETRANSMIT SYNC PACKET:** The node already synchronized will contend for the medium based on the chosen slot in the SYNC contention window; if it detects an idle channel it sends a SYNC packet for the neighbouring nodes (RFDs). This is useful when multi-hop is considered;
- **SLEEP:** The node “turns off” the radio and put CPU in low power consumption mode;
- **DISCOVERY & ADDITION:** The new nodes that want to join the WSN may employ two mechanisms that allow for the new nodes to synchronize with the remaining nodes of the WSN, including the coordinator (if it is in range);
- **IDLE:** The node is waiting for a task to perform;



Table 8.3: MC-SCP events and actions.

Events	Actions
1	State: WAIT FOR SYNC Schedule: Switches to SYNC and control slot channel; Wait for the SYNC packet; SYNC_TIMEOUT_START;
2	State: SYNCHRONIZATION Schedule: Finish_SYNC; Remains in SYNC and control slot channel; Choose the slot in SYNC CW to retransmit SYNC packet;
3	State: SYNCHRONIZATION Schedule: New node joins the network; Random_channel_slot_selection mechanism enabled; Detect a packet from node that allows for synchronization; 1 st mechanism time out;
4	State: SYNCHRONIZATION Schedule: New node joins the network; Random_channel_slot_selection mechanism fails; Fast_slot_channel_hopping mechanism enabled; Detect a packet from node that allows for synchronization; 2 nd mechanism time out;
5	State: RETRANSMIT SYNC PACKET Schedule: SYNC_Contention_Window_Initiate; Update: Chooses a slot for SYNC CW and performs CS;
6	State: IDLE Schedule: SYNC_RETRANSMISSION_FINISHED; WAITS_FOR_PACKET_IN_MAC_QUEUE;
7	State: IDLE Schedule: If a new node that tries to join, transits directly to IDLE state;
8	State: CHECK_QUEUE Schedule: Verifies packets in queue;
9	State: SLOT CHANNEL CHOICE Schedule: SWITCH_TO_CHANNEL; if (number_packets_in_queue $\geq$ 1) TX_DATA_PACKETS Update: Switches to same slot channel of parent node ; if (number_packets_in_queue == 0) CHECK_MEDIUM_FOR_DATA_PACKETS Update: Switches to current slot channel of the node that initiates the sensing;
10	State: SAMPLE WAKE-UP TONE Schedule: CHECK_WAKE-UP_TONE; Update: Performs CS to the channel;
11	State: WAIT FOR DATA PACKET Schedule: RX_DATA_PACKET; INITIATES_DATA_PACKET_TIMEOUT;
12	State: RX DATA PACKET Schedule: Check if “more bit” is enabled if (more bit == 1) ER phase enabled; if (more bit == 0) ER phase disabled; RECEIVE_PACKET; Update: Check piggybacked clock information of the child node by the parent node for deviations;
13	State: ER PHASE Schedule: Finish receiving data packets; Update: Remaining packets from sender node;
14	State: END RECEIVING ALL PACKETS Schedule: Transmit MC-ACK/MC-NACK packet; Update: Packets in queue to be transmitted or retransmitted to coordinator;
15	State: IDLE Schedule: MEDIUM_FREE; Go to SLEEP state;

Events	Actions
16	State: SENDING MC-ACK/MC-NACK Schedule: TX MC-ACK/MC-NACK with piggybacked SYNC information;
17	State: TRANSMIT Schedule: TX MC-ACK/MC-NACK packet;
18	State: IDLE Schedule: IDLE_TO_SLEEP; Update: Degradation channel level;
19	State: SLEEP Schedule: EVENT_SENSING; CHECK_QUEUE;
20	State: SENDING MC-ACK/MC-NACK Schedule: TRANSMIT MC-ACK/MC-NACK packets with piggybacked SYNC information;
21	State: WAKE-UP TONE TX Schedule: CONTENTION_WINDOW_1_INITIATE; Update: Chooses a slot/time for the CW ₁ ; Performs CS to the channel;
22	State: IDLE Schedule: MEDIUM_BUSY; Stops the transmission of the packet and goes to IDLE; Switches radio transceiver to RX mode;
23	State: TRANSMIT Schedule: TRANSMIT WAKE-UP TONE;
24	State: DATA PACKET TX Schedule: CONTENTION_WINDOW_2_INITIATE; Update: Chooses a slot in CW ₂ to contend for the channel; Performs CS;
25	State: ER PHASE DECISION ALGORITHM Schedule: Verifies the three conditions to enable this phase: 1) Queue has more than one packet to be sent; 2) Slot channel does not has a high degradation level; 3) Mobility/reduced mobility is not present by means of IR algorithm metric; Update: if (all conditions == true) sets the "more bit" in data packet specify number of packets in queue of sender if (all conditions = false) resets the "more bit" in data packet ASSESS POSSIBILITY TO USE ER PHASE
26	State: TRANSMIT Schedule: Transmit N data packets;
27	State: CHECK MAC QUEUE Schedule: VERIFY MAC QUEUE FOR MORE PACKETS TO BE SENT;
28	State: DATA PACKET TX Schedule: TRANSMITS REMAINING DATA PACKETS; Update: Remaining number of packets to be sent in the data packet field;
29	State: WAIT RESPONSE MC-ACK/MC-NACK Schedule: MC-ACK/MC-NACK TIMEOUT; WAIT MC-ACK/MC-NACK;
30	State: RECEIVING MC-ACK/MC-NACK Schedule: UPDATES SYNC CLOCK; Degradation channel level;
31	State: UPDATE SYNC CLOCK Schedule: Extract piggybacked synchronization clock information; Update: Verifies clock deviation and synchronizes internal clock of child node;
32	State: DENIAL CHANNEL LIST Schedule: Influential range concept verification; Update: Degradation level of each slot channel;

Events	Actions
33	State: IR CONCEPT VERIFICATION Schedule: IR verification based on overheard data or MC-ACK/MC-NACK packets; Update: IR table;
34	State: WAIT FOR MC-ACK/MC-NACK Schedule: MC-ACK/MC-NACK TIMEOUT; WAIT MC-ACK/MC-NACK;
35	State: RECEIVING MC-ACK/MC-NACK Schedule: UPDATES SYNC CLOCK; Update: Degradation channel level metric;
36	State: CHECK CLOCK DEVIATION Schedule: Comparison of child node and parent node sync clocks; if (deviation $> \rho_{dev}$) Synchronization error Node goes to the SYNCHRONIZATION state if (deviation $\leq \rho_{dev}$) Node goes to the SLEEP state
37	State: IDLE Schedule: MEDIUM_BUSY; Stops transmission of data packet; Waits for data packet or MC-ACK/MC-NACK packet; Applies the IR concept algorithm and synchronization procedure (if possible);
38	State: SLEEP Schedule: EVENT_SENSING; Checks MAC queue;
39	State: SYNCHRONIZATION Schedule: Retries to synchronize due to high internal clock deviations;
40	State: DISCOVERY & ADDITION Schedule: When node is added to the WSN after first synchronization. Random_channel_slot_selection mechanism is enabled;
41	State: DATA PACKET TX Schedule: Node successfully contends in CW_2 ; Check MAC queue; Schedules data packet transmission;
42	State: UPDATE SYNC CLOCK Schedule: Check for clock deviation of the sending node; This transition only appears in the coordinator node;
43	State: WAKE-UP TONE TX Schedule: Node successfully contends in CW_1 ; Transmit wake-up tone;

- **CHECK MAC QUEUE:** Before choosing the slot channel (coordinator or parent node slot channel) the node verifies his MAC queue for any packets to be sent;
- **SLOT CHANNEL CHOICE:** After the node checks if it has packets in the MAC queue or not, the node changes to the receiving mode (in case it is an FFD and multi-hop is considered), or changes in transmission mode (in case it has packets to send), or go to sleep mode when the MAC queue has no packets and the node is not an FFD. It also checks the denial channel list to restrict the slot channel choices only to the best slot channels;
- **TRANSMIT:** The node transmits the packet, independently of its type;
- **SAMPLE WAKE-UP TONE:** The node samples for the presence of the wake-up tone;
- **WAIT FOR DATA PACKET:** When the node has no packets in the MAC queue (in case it is a FFD and multi-hop is considered), it waits for the reception of the data packet from the RFD node. If no wake-up is detected the node transits directly to IDLE state and goes to SLEEP state;

- **RX DATA PACKET:** The node receives the data packet and extracts the synchronization information, suppressing the transmission of explicit SYNC packets. Checks if the “more bit” included in the data packet is set;
- **ER PHASE:** In case the node receives a data packet with the “more bit” set, the receiving node extends its reception time in order to receive the remaining data packets from the sender node;
- **END RECEIVING ALL PACKETS:** The node enters this state after receiving all the data packets sent during the ER phase;
- **SENDING MC-ACK/MC-NACK:** After receiving all data packets the receiving node sends a MC-ACK / MC-NACK packet depending on if the packets have been successfully received or not, respectively;
- **DENIAL CHANNEL LIST:** The node that contends to transmit his data packets transit to this state if contention in CW_1 / CW_2 is lost, or in case it received a MC-NACK packet or a data packet. It updates the denial channel list based on these events;
- **IR CONCEPT VERIFICATION:** If the node loses contention in CW_1 or CW_2 , it verifies if it is in the influential range of the node that has sent the overheard data packet. Based on this, the node in the next attempts checks if the packets (to be sent) stored in the queue contain the same information. If so, the node does not send the stored packet with the same information as the one overheard. This mechanism avoids redundant data packets transmissions;
- **WAIT FOR MC-ACK/MC-NACK:** After receiving the overheard data packet then node waits for the MC-ACK / MC-NACK packet in order to check his internal clock in comparison with the node that sends the overheard packet (parent node or coordinator node);
- **RECEIVING MC-ACK/MC-NACK:** The nodes receive the MC-ACK / MC-NACK packet;
- **UPDATE SYNC CLOCK:** After receiving the MC-ACK/MC-NACK packet the node extracts the synchronization time sent by the coordinator/parent node;
- **CHECK CLOCK DEVIATION:** The node verifies if the internal synchronization clock presents a high deviation error compared with the value of ρ_{dev} ;
- **WAKE-UP TONE TX:** The node transmits the wake-up tone after the node contends successfully in the CW_1 ;
- **DATA PACKET TX:** After successfully contending in both contention phases, the node is in conditions to transmit the data packet. If the ER phase decision algorithm allows to expand the delivery of more data before the receiving nodes go to SLEEP state. The sender node after sending the first data packet continues to send the remaining data packets;
- **ER PHASE DECIDER:** The sender nodes assesses the possibility of using the ER phase to send more than one data packet before going to the SLEEP state. The decision is based on the denial channel list and IR concept information.

The different transitions between the states from the FSM are as follows:

- After the node is switched on (STARTUP) the node transits to WAIT FOR SYNC state (1);

- If the child node receives a SYNC packet from the coordinator it transits to the SYNCHRONIZATION state (2);
- After receiving the SYNC packet, the nodes will contend in the SYNC CW, in order to retransmit the SYNC packets to the remaining nodes that do not have a direct communication link with the coordinator (5);
- If the nodes successfully contends during the SYNC CW, it retransmits the SYNC packet for the neighbouring nodes. After this synchronization procedure the nodes pass to the IDLE state (6);
- If a new node wants to join the WSN after the main synchronization procedure the node transits from the STARTUP state to the DISCOVERY & ADDITION state (40);
- Here the node has two mechanisms that allow to synchronize with the WSN. The first mechanism is enabled, allowing the node to join the network. If the node is able to join the network it transits to the SYNCHRONIZATION state (3);
- If the first mechanism fails, the node enables the second mechanism (fast slot channel hopping mechanism). The node passes to the SYNCHRONIZATION state if successfully synchronizes with the nodes already in the WSN (4);
- In the SLOT CHANNEL CHOICE state the node verifies if there are any packets in queue to be sent. If the node has packets in queue, the node transits to WAKE-UP TONE TX (21), in which the node contends for the medium by choosing a slot randomly within the CW_1 ;
- The node transits directly to the IDLE state if it loses the contention in CW_1 (22);
- Otherwise, the node initiates the transmission of the wake-up tone in the WAKE-UP TONE TX state (43);
- To transmit the tone, the node transits to the TRANSMIT state (23);
- After transmitting the wake-up tone, the node transits to the second contention window and chooses randomly a slot to contend for the channel (24);
- In case the node successfully contends for the channel than it transits to the DATA PACKET TX state (41) and consequently to the ER PHASE DECIDER state, in which the node decides whether it is necessary to use the ER phase or not (25);
- Once the decision is taken, the node enables the “more bit” if the ER phase is necessary and resets it if the ER phase is not necessary. In case it is necessary, the node passes to the TRANSMIT state (26);
- After transmitting the first data packet, if the ER phase is enabled, the node moves to the DATA PACKET TX state (25). This procedure is repeated until the MAC queue has no packets to be sent;
- The transitions (22), (37) and (18) to the IDLE state are followed by the transition to the DENIAL CHANNEL LIST state (32). In the cases of the nodes that lost the contention (in CW_1 or CW_2) the nodes will overhear the data packet(s) in order to compute the degradation level of the slot channel, while updating the Denial channel list. In the case of the node that finished transmitting the data packet(s) the Denial channel list is also updated;

- Then the node transits to the IR CONCEPT (33) and only the nodes that overheard the data packet(s) will verify the redundancy of their data packets, in terms of information. In the case of the nodes that end the transmission of the data packet(s), the node will only change to the IR CONCEPT state after receiving the MC-ACK/MC-NACK packet;
- The node transits to the WAIT FOR MC-ACK/MC-NACK state (34), while it waits for the MC-ACK or MC-NACK from the coordinator/parent;
- After initiating the reception of the MC-ACK/MC-NACK packet, the node waits until it finishes receiving completely the MC-ACK/MC-NACK packet. The node passes to the RECEIVING MC-ACK state (35);
- The node extracts the synchronization clock information included in the MC-ACK/MC-NACK packet from the piggybacked information and updates its internal clock information in the UPDATE SYNC CLOCK state (31);
- The clock deviation verification procedure is performed by the receiving node of the MC-ACK/MC-NACK packets in the CHECK CLOCK DEVIATION state (36);
- If the node does not detect a clock deviation higher than ρ_{dev} , the node transits directly to the SLEEP state (38);
- Otherwise, the node passes to the SYNCHRONIZATION state due to the high clock deviation error (39). Here the node tries to resynchronize again;
- The IR CONCEPT state does not apply to the coordinator node, since it only receives packets from the child nodes. After the coordinator receives the data packet it transits to the DENIAL CHANNEL LIST state in which it updates the list and transits to the UPDATE SYNC CLOCK state (42) for synchronization clock deviations checking.

8.5 Discussion of the Simulation Results for the MC-SCP-MAC Protocol

8.5.1 Collision Probabilities

In this section, the CW_1 and CW_2 collision probabilities for the MC-SCP-MAC and SCP-MAC are obtained as a function of the number of nodes whilst considering the contention window size as a parameter. Six different random seeds are considered in simulations and the 95 % confidence intervals are represented. In this set of results, we consider a deployment scenario of 50×50 m², a maximum transmitter power of $P_{tx} = 1$ mW for both MAC protocols, maximum contention window sizes of $CW_k^{max} = 8$, $k \in \{1, 2\}$, data packet size of $L_{data} = 50$ Bytes, as well as different values for the traffic generation rate. Saturated and unsaturated traffic load regimes are considered for the MC-SCP-MAC and SCP-MAC protocols. One assumes a number slot channels for data utilized in these tests of $N_{ch} = 15$ for the MC-SCP-MAC protocol and $N_{ch} = 1$ (single-channel) for SCP-MAC.

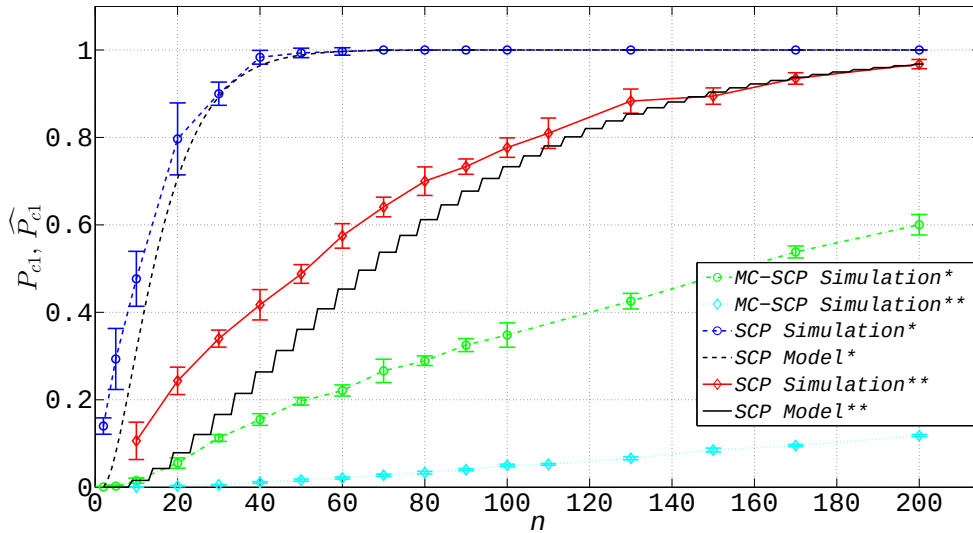


Figure 8.19: Comparison of the CW_1 collision probability between the MC-SCP-MAC and SCP-MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure 8.19 shows the comparison of the CW_1 collision probability for the MC-SCP-MAC and SCP-MAC protocols in the saturated and unsaturated regimes. Moreover, it addresses the verification of the validity of the CW_1 collision probability, under the saturated and unsaturated traffic regimes, as an extension to the protocol SCP-MAC already presented and discussed in Chapter 6. It is observable that the CW_1 collision probability is much lower for the MC-SCP-MAC protocol than for SCP (in both regimes). This is an expected behaviour since MC-SCP-MAC envisages the use of multi-channel jointly with an enhanced two-phase contention window mechanism to cope with possible data packet collisions. These mechanisms allow for significantly reducing the CW_1 collision probability. Results for the CW_1 collision probability and expected number of nodes that pass from CW_1 to CW_2 in Section J.1 from Appendix J are presented. Results include the saturated and unsaturated regimes for the MC-SCP-MAC protocol for $CW_1^{max} = 8$.

As an example, Figure 8.20 presents the expected number of nodes that pass from CW_1 to CW_2 , in the saturated regime, $E[S]$, and unsaturated regime, $\hat{E}[S]$. The Figure compares the MC-SCP-MAC and SCP-MAC protocols. The 95 % confidence intervals are also presented in the Figure. The curves for the SCP simulations have already been verified in Chapter 6. It is

verified that the difference between the modelling and simulation results “is negligible” for all the range of n . Despite the smaller model accuracy for low number of nodes, as n increases, the curve for the simulation results converges to the curve of the numerical solution for the expected number of nodes that pass from CW_1 to CW_2 . The expected number of nodes that pass from CW_1 to CW_2 in MC-SCP-MAC is much lower than for SCP, as expected. Since the number of nodes that pass from CW_1 to CW_2 decreases, the probability of a node to successfully deliver a packet is much higher than in the case of the single-channel SCP-MAC protocol.

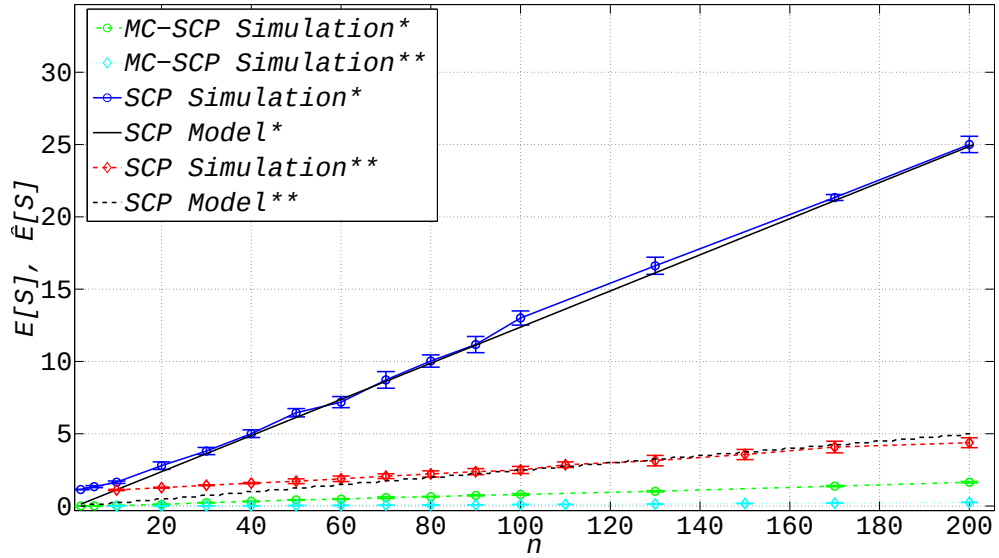


Figure 8.20: Comparison of $E[S], \hat{E}[S]$ between the MC-SCP-MAC and SCP-MAC protocols in the saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

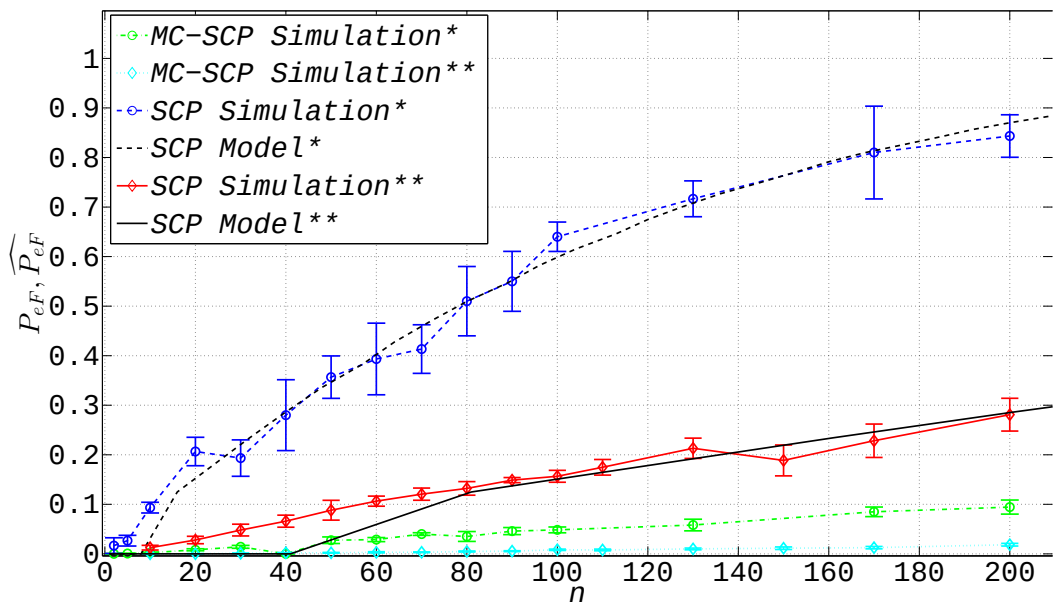


Figure 8.21: Comparison of the CW_2 collision probability between the MC-SCP-MAC and SCP-MAC protocols in the saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure 8.21 shows a comparison between the simulation and analytical results for the collision probability in CW_2 as a function of n for the saturated and unsaturated traffic regimes. The values of the collision probability in CW_2 are much lower for the MC-SCP-MAC protocol than for the SCP. In addition, the curve for the MC-SCP-MAC protocol in the unsaturated case is rela-

tively close to zero. We can conclude from these tests that the use of multi-channel features, jointly with an enhanced two-phase contention window mechanism, allows for achieving a much lower collision probability for the data packets, which increases the overall performance of the network at the expense of a small increase of complexity in terms of the protocol algorithm. Results for the the CW_2 collision probability of the MC-SCP under saturated and unsaturated regimes, whilst considering $CW_k^{max} = 8$, $k \in \{1, 2\}$ are presented in Section J.1 of Appendix J.

8.5.2 Energy Efficiency per Delivered Packet

This section addresses the evaluation of the energy consumption per packet successfully delivered when employing the MC-SCP-MAC and SCP-MAC protocols. This metric corresponds to the total energy consumed (Joule) divided by the total number of successfully delivered packets. In these tests, the energy consumed to receive and transmit as well as the energy consumed to forward the packets towards the PAN coordinator or sink node is analyzed. Also, the energy spent to transmit control messages, e.g., wake-up tones is also considered. In these simulations we have considered a deployment scenario of 50×50 m², maximum transmitter power of $P_{tx} = 1$ mW for both MAC protocols, maximum contention window sizes of $CW_k^{max} = 8$, $k \in \{1, 2\}$, different values for the periodic traffic generation rate, data packet size of $L_{data} = 50$ Bytes, as well as the power consumption parameters of the different radio transceivers presented in Table 6.4. Here, the saturated traffic regime is the only one considered for the MC-SCP-MAC and SCP-MAC protocols. One assumes a number slot channels for data utilized in these tests of $N_{ch} = 15$ for the MC-SCP-MAC protocol and $N_{ch} = 1$ (single-channel) for SCP-MAC.

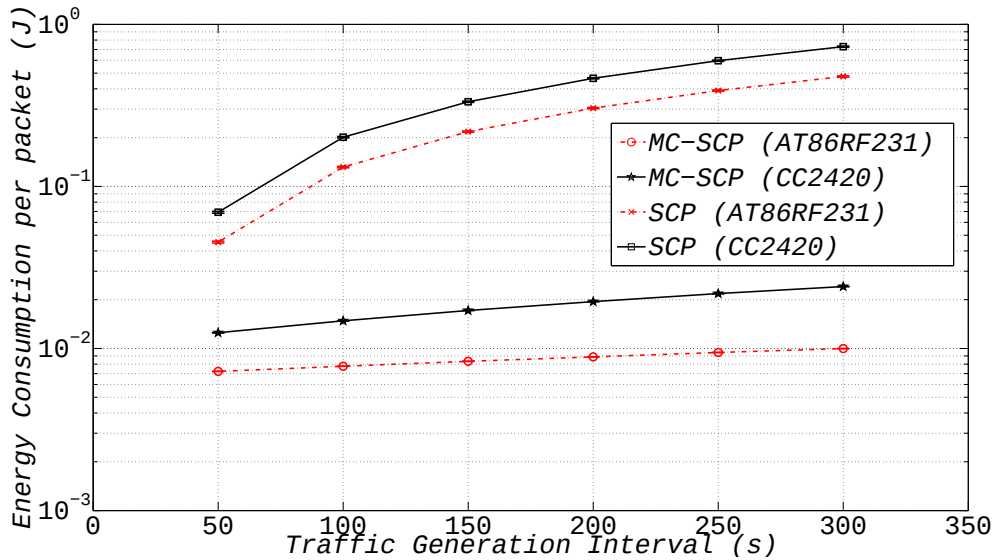


Figure 8.22: Comparison of the energy consumption per packet successfully delivered between MC-SCP-MAC and SCP-MAC protocols for the CC2420 and AT86RF231 transceivers.

Figure 8.22 presents the comparison of the energy consumption per packet successfully delivered between MC-SCP and SCP protocols for the CC2420 and AT86RF231 transceivers. The energy spent per delivered packet increases as the traffic generation interval increases due to the increase of the time that the node needs to dispatch all the packets. In comparison with the single-channel SCP-MAC protocol, the MC-SCP-MAC protocol presents the lowest values of energy spent per delivered packet for the AT86RF231 transceiver. This is due to the very high delivery rate that the use of multiple channels allows for, combined with the ultra-low power consumption feature of the AT86RF231 transceiver. The same holds for the CC2420 transceiver,

where the MC-SCP-MAC protocol also presents lower values of energy spent per delivered packet than the SCP-MAC protocol.

8.5.3 Collision Probability Performance

Figure 8.23 shows the CW_1 collision probability as a function of the number of slots channels in the saturated and unsaturated regimes, for maximum contention window sizes of $CW_k^{max} = 8$, $k \in \{1, 2\}$ for the MC-SCP-MAC and SCP-MAC protocols. For this set of results we consider a deployment scenario of $50 \times 50 \text{ m}^2$, a maximum transmitter power $P_{tx} = 1 \text{ mW}$ for both MAC protocols, a periodic traffic generation rate of $\lambda = 1/2 \text{ s}^{-1}$ and data packet size of $L_{data} = 32 \text{ Bytes}$. One assumes a number slot channels for data utilized in these tests of $N_{ch} \in \{3; 4; 7; 9; 15\}$ for the MC-SCP-MAC protocol and $N_{ch} = 1$ (single-channel) for SCP-MAC. The frame durations is $t_F = 1 \text{ s}$. The time allocated for each slot channel is given by $\Delta t_{SC} = t_F / (N_{ch} + 1)$, for the MC-SCP-MAC. In the SCP-MAC protocol the duration of each frame is $t_F = 1 \text{ s}$. Each node polls the medium after each second. The network size considered in these tests is $n = 99$ nodes, plus 1 PAN coordinator. The CW_1 collision probability for the SCP-MAC protocol does not vary as the number of slot channels increases, since it only considers one channel for data packets transmission. In Figure 8.23 for both MAC protocols the values of $\widehat{P}_{c1}$ under the unsaturated traffic regime hold the lowest values of the CW_1 collision probability. The 95 % confidence intervals are also presented in the Figure. However, for the MC-SCP-MAC protocol the CW_1 collision probability considerably decreases as the number of available slot channels increases. The increase of the slot channels allows for the nodes to select different slot channels; hence, decreasing the probability of a node to choose the same slot channel to transmit its data packets. The difference of the CW_1 collision probability between the MC-SCP and SCP MAC protocols is more noticeable in the unsaturated regime.

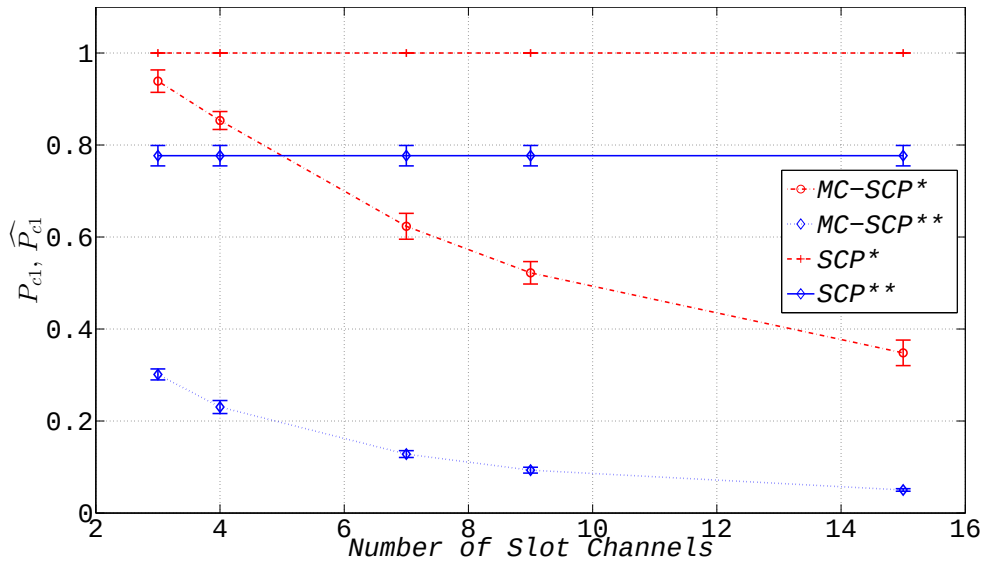


Figure 8.23: Comparison of the dependence of the CW_1 collision probability with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure 8.24 presents the dependence of the expected number of nodes that pass from CW_1 to CW_2 with the number of available data slot channels. In MC-SCP, the expected number of nodes that pass from CW_1 to CW_2 presents a behaviour similar to the one from the CW_1 collision probability. In the MC-SCP-MAC protocol and the saturated case, the expected number of nodes

that pass from CW_1 to CW_2 considerably decreases as the number of slot channels increases. For the unsaturated case, this decreasing behaviour is smoother compared to the expected number of nodes that pass from CW_1 to CW_2 in the SCP protocol.

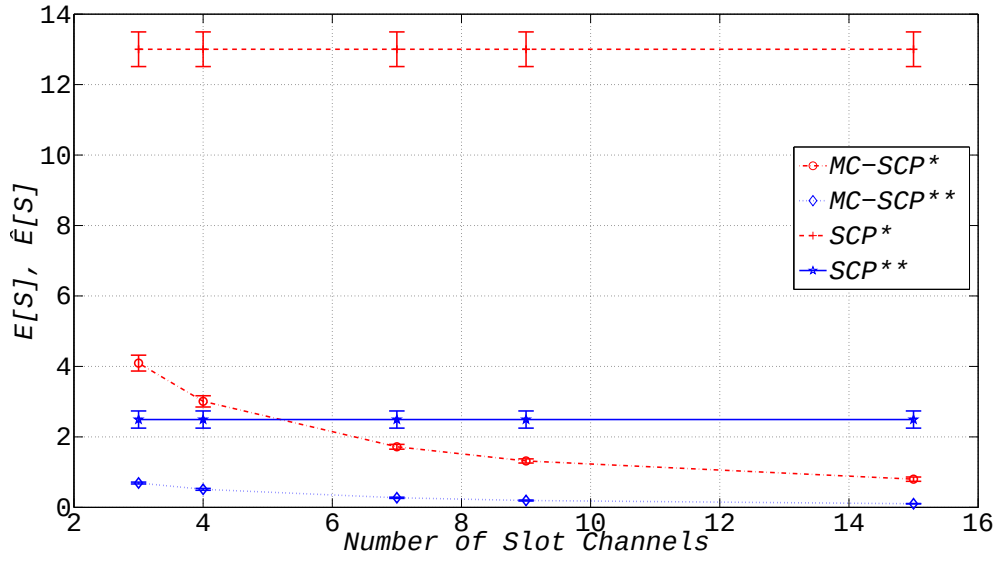


Figure 8.24: Comparison of the dependence of the $E[S]$, $\hat{E}[S]$ with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure 8.25 compares simulation and analytical results of the dependence of the collision probability in CW_2 with the number of data slot channels, for two different traffic regimes. For the MC-SCP-MAC protocol the curves of the CW_2 collision probability decrease as the number of slot channels increases. The CW_2 collision probability of the MC-SCP-MAC protocol is always lower than for SCP. This is due to the low values of the CW_1 collision probability resulting from the multi-channel feature, which leads to a low expected number of nodes that pass from CW_1 to CW_2 . It is worth noting that the unsaturated regime is the one that presents the lowest values for the CW_2 collision probability.

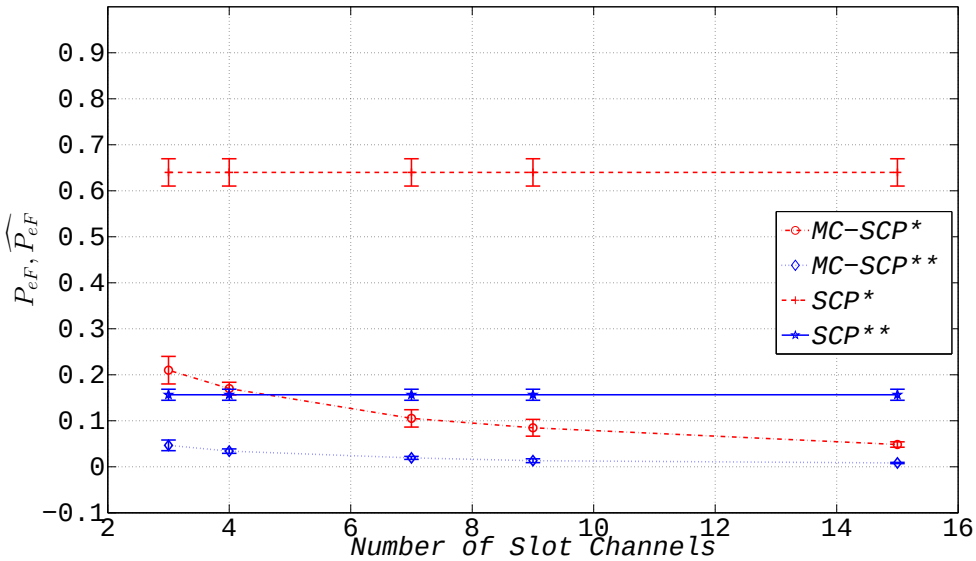


Figure 8.25: Comparison of the dependence of the CW_2 collision probability with the number of slots channels between the MC-SCP and SCP MAC protocols in saturated (*) and unsaturated (**) regimes, for $CW_k^{max} = 8$, $k \in \{1, 2\}$.

From this set of tests the conclusions are twofold:

- The increase of the number of slot channels along with an enhanced two-phase contention window mechanism allows for achieving a much lower collision probability for the data packets;
- The difference of effective collision probability between the MC-SCP and SCP MAC protocols is more notorious in the saturated case, as the number of slot channels increases.

8.5.4 Energy Efficiency with Multiple Slot Channels and Contention Window Sizes

This section analyzes the impact of the number of slot channels and different contention window sizes on the network performance. For this set of tests all the nodes initiate CBR streams towards the sink node and each node generates a packet every 2 s. In the MC-LMAC protocol, if the packet generation is quicker, buffer overflows start to occur. In the MC-SCP-MAC protocol this only happens when the traffic generation time is lower than the frame duration. Here, the frame duration is $t_F = 1$ s and the time allocated for each slot channel is given by $\Delta t_{SC} = t_F / (N_{ch} + 1)$ for the MC-SCP-MAC protocol. In turn, MC-LMAC considers a frame duration of $t_F = 1.6$ s. The MC-SCP-MAC considers $CW_k^{max} \in \{16, 32, 64, 80\}$, $k \in \{1, 2\}$ for the maximum contention window sizes. For this set of results we consider a maximum transmitter power $P_{tx} = 0.8$ mW for both MAC protocols. The data packet size is $L_{data} = 32$ Bytes. The number of slot channels for data utilized in these tests is given by $N_{ch} \in \{3; 4; 7; 9; 15\}$ for MC-SCP whereas MC-LMAC considers $N_{ch} \in \{3; 4; 7; 9; 10\}$. In this set of tests we considered a network composed by $n = 99$ nodes.

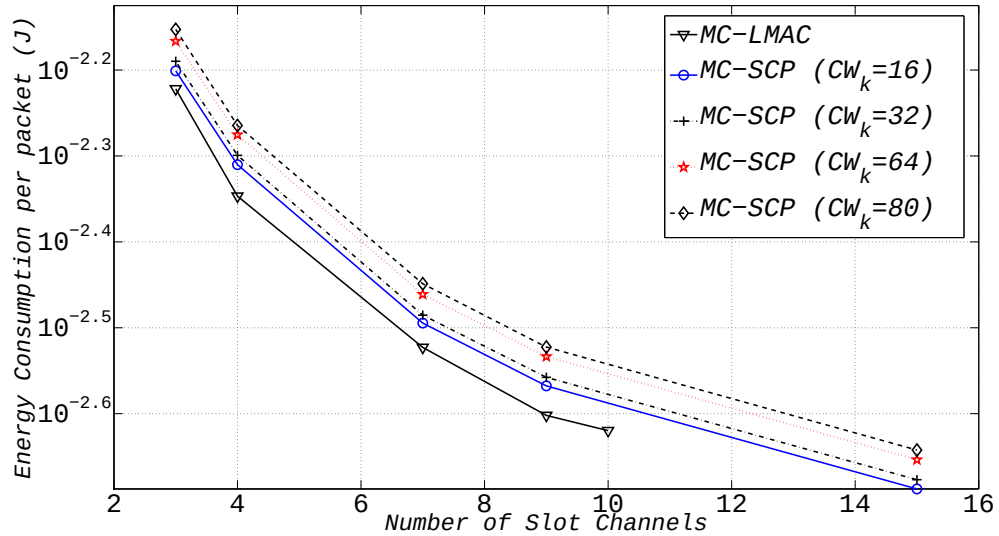


Figure 8.26: Energy consumption per delivered packet with variable number of slot channels and contention window sizes between MC-SCP-MAC and MC-LMAC, $k \in \{1, 2\}$.

The terrain size considered in the MC-LMAC and MC-SPC-MAC protocols is 150×150 m² [lvHJH11]. However, the authors from MC-LMAC [lvHJH11] consider that, in the multi-hop scenario, all nodes are in the carrier sensing range of each other. Nodes in the 2nd tier cannot directly communicate with the sink node. This assumption does not consider the hidden terminals problem. Since the nodes in the MC-SCP-MAC are deployed randomly, the nodes may not be in the carrier sensing range of all neighbouring nodes. Therefore, as the MC-SCP-MAC protocol envisages a more realistic scenario, it accounts for hidden terminals in the different deployments. The traffic generation can be considered as a periodic data collection, which is commonly used in

WSN applications. In both MAC protocols retransmissions are disabled i.e., we considered only best effort delivery, such that the lost packets are not retransmitted. With sufficient channels and retransmissions enabled, MC-SCP-MAC achieves to deliver 99 % of the packets, on average. Figure 8.26 shows the results for the energy consumed per successfully delivered packet. The energy spent per delivered packet is high for both MAC protocols when there are three slot channels available. The 95 % confidence intervals are also presented. This is due to the low delivery rate ratio achieved by each MAC protocol. Both MC-SCP-MAC and MC-LMAC consume less

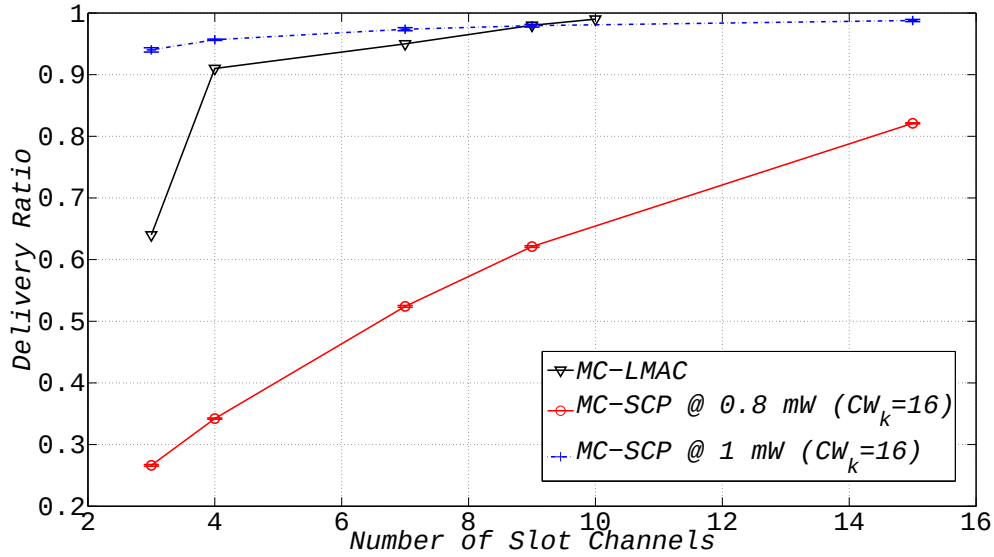


Figure 8.27: Comparison of the delivery ratio for different transmitter powers, for the MC-SCP-MAC and MC-LMAC protocols, $k \in \{1, 2\}$.

energy as the number of slot channels increases. This behaviour is expected, since the increase of slot channels decreases the probability of nodes to choose the same slot channel, and consequently increasing the delivery ratio. The energy consumed by the MC-LMAC protocol in these tests is always lower than the different contention window sizes of MC-SCP-MAC. However, for the MC-SCP-MAC case of $CW_k^{max} = 16$, $k \in \{1, 2\}$, the energy spent is quite similar to the one from MC-LMAC. In MC-SCP-MAC, as the contention window sizes increase the energy consumed increases, due to the increase of time spent by the node to contend for the channel during the two-phase contention window mechanism. Figure 8.26 shows the results for the delivery ratio in the tests of the MC-SCP-MAC, for a maximum number of slot channels $N_{ch} = 15$. An high delivery ratio leads to the lowest energy consumed per packet delivery. Since the MC-LMAC deployment scenario considers that all the nodes are at the carrier sensing range of each other, we decided to increase the transmitter power from 0.8 mW to 1 mW.

This increase allows for to having a more fair comparison with MC-SCP-MAC. This can be interpreted as a disadvantage due to the increase of the number of contention nodes. However, for the MC-SCP-MAC protocol, this is the main envisaged scenario. Figure 8.27 presents the dependence of the delivery ratio on the number of slot channels for the MC-SCP-MAC and MC-LMAC protocols, for different transmitter powers. In these results, we consider maximum contention window sizes of $CW_k^{max} = 16$, $k \in \{1, 2\}$. In both MC-SCP-MAC and MC-LMAC, as the number of slot channels increases the delivery ratio increases. Figure 8.27 shows that, for $P_{tx} = 0.8$ mW, the MC-LMAC protocol presents higher delivery ratios than MC-SCP-MAC. The low delivery ratio caused by the large number of hidden terminals leads to the failure in successful packets reception. For the MC-SCP-MAC, with the increase of the transmitter power the impact of the hidden terminals problem decreases, which leads to a significant increase of the delivery

ratio. The MC-SCP-MAC achieves delivery ratios higher than 90 % for all the number of slot channels presented in Figure 8.27. Figure 8.28 shows the comparison of the energy consumption per delivered packet for different transmitter powers for the MC-SCP-MAC and MC-LMAC. The energy spent per delivered packet is high in the presence of three slot channels. Here, the MC-SCP-MAC protocol with higher transmitter power ($P_{tx} = 1$ mW) presents a much lower energy spent per delivered packet than the MC-LMAC protocol. This is explained by the high delivery ratio presented in Figure 8.27 as the number of slot channels increases. From this set of tests, we can conclude that, in denser scenarios, MC-SCP-MAC can handle high contention on the medium due to the use of the enhanced two-phase mechanism with the multi-channel feature. Moreover, the increase of the transmission power eliminates the majority of occurrences of hidden terminals, which allows for achieving higher delivery ratio and, consequently, lower energy consumed per delivered packet.

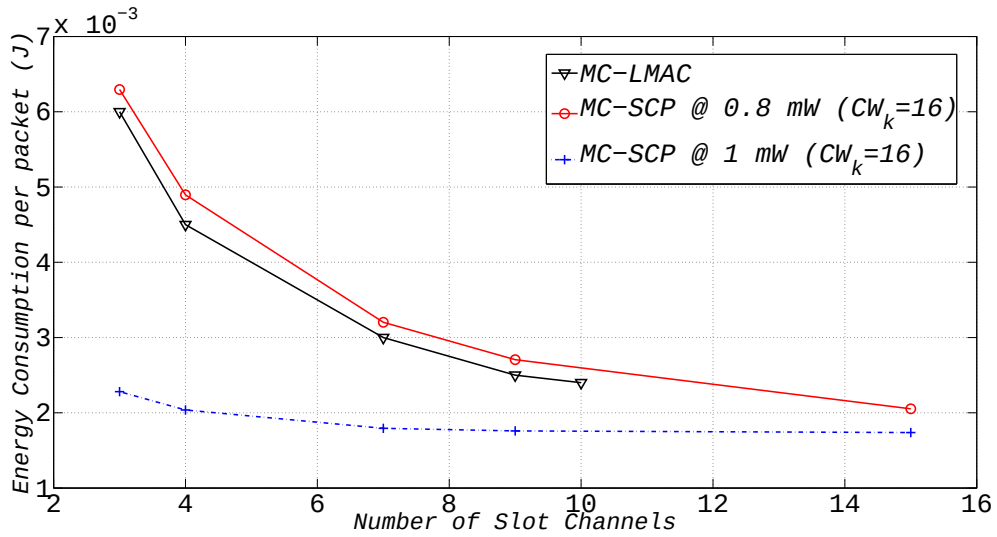


Figure 8.28: Comparison of the energy consumption per delivered packet for different transmitter powers, for the MC-SCP-MAC and MC-LMAC protocols, $k \in \{1, 2\}$.

8.5.5 IR Concept and Energy Performance Evaluation

Fixed Number of Channels

In this section, we analyze the impact, in terms of energy performance, of the influential range (IR) concept enabled in the MC-SCP-MAC. For this set of tests, all the nodes initiate CBR streams towards the sink node. We assume that each node generates a packet every 10 s and that the maximum contention window sizes are $CW_k^{max} = 16$, $k \in \{1, 2\}$. Besides, we consider a maximum transmitter power $P_{tx} = 0.8$ mW, a deployment area of 50×50 m², data packet size $L_{data} = 32$ Bytes and a number of slot channels $N_{ch} = 15$. Here the frame duration is $t_F = 1$ s. The time allocated for each slot channel is $\Delta t_{SC} = 0.0625$ s. The objective of these tests is to analyze the gains achieved when the IR concept is enabled, for different values of the sensing range, $\Pi_{irmax} \in \{-90; -80; -70; -60\}$ dBm. Figure 8.29 presents the average energy consumption per node when IR is enabled and disabled, for different sizes of the network. The 95 % confidence intervals are also presented in this Figure. Each node generates and transmits 50 packets to the PAN. When the IR is disabled it is observable that the energy consumption per node increases as the size of the network increases. Considering a value of $\Pi_{irmax} = -90$ dBm the lowest energy consumption is achieved for each size of the network when IR is enabled. By enabling the IR, the node that overhears a data packet and verifies that it has redundant data

in queue (to be sent to the sink) will exclude these packets. Discarding redundant data packets decreases the energy consumption per node, as shown in Figure 8.29. For higher values of the sensing range, Π_{irmax} , the influential range of each node is shorter, which leads to a decrease of the overhearing. As a consequence less redundant data packets are discarded. Therefore, the use of the IR reduces the redundancy of data packets and, consequently, decreases the energy consumed per node.

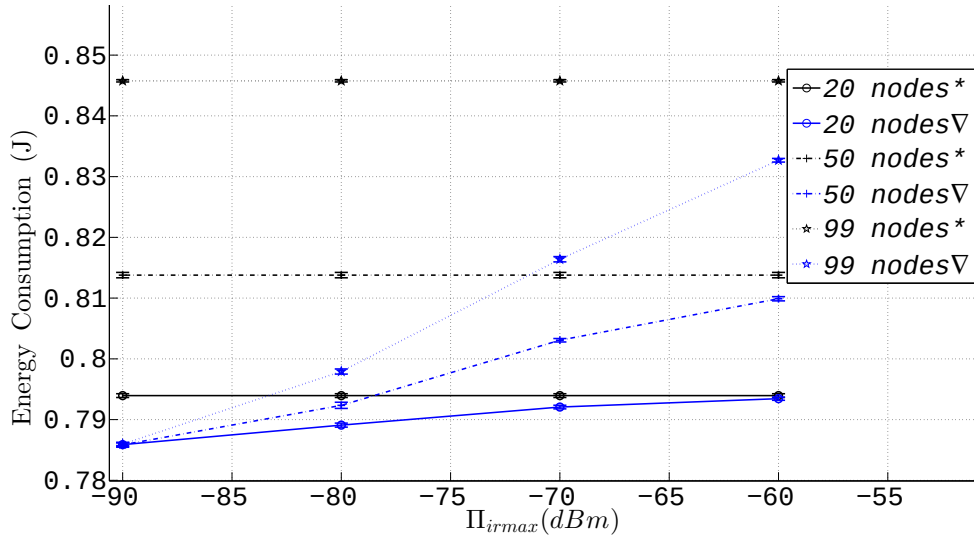


Figure 8.29: Average energy consumption per node when IR is enabled (∇) and disabled (*) for different sizes of the network (50 packets are transmitted from each node to the PAN).

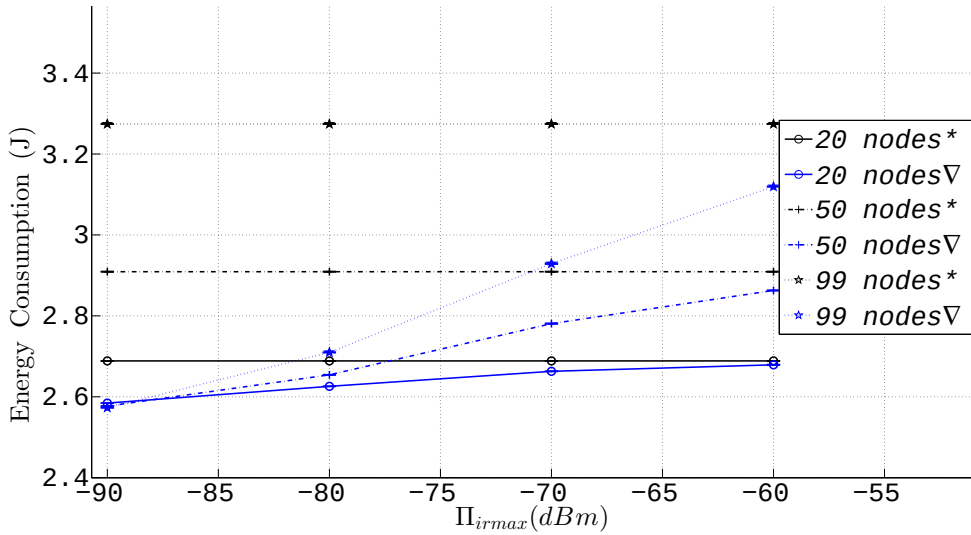


Figure 8.30: Average energy consumption per node when IR is enabled (∇) and disabled (*), for different sizes of the network (600 packets).

The analysis of the case where each node generates and transmits 600 packets to the PAN allows for evaluating the long-term energy consumption for MC-SCP-MAC, as shown in Figure 8.30. Again, for higher values of the sensing range, Π_{irmax} , the influential range of each node is shorter, which leads to a decrease of the overhearing. Therefore, it decreases the energy consumed per node. In the case IR is disabled, the curves for the energy consumption can be considered as upper bounds. The so-called “energy consumption saving” represents the difference, in terms of energy that a node can save when applying the IR concept and facilitates

to evaluate the benefits from using the IR concept in the MC-SCP-MAC protocol for different values of Π_{irmax} .

Figure 8.31 presents results for the energy consumption saving as a function of the sensing range, Π_{irmax} , when each node generates either 50 packets or 600 packets (to be sent to the PAN). The energy consumption saving is higher when the nodes send 600 packets to the PAN.

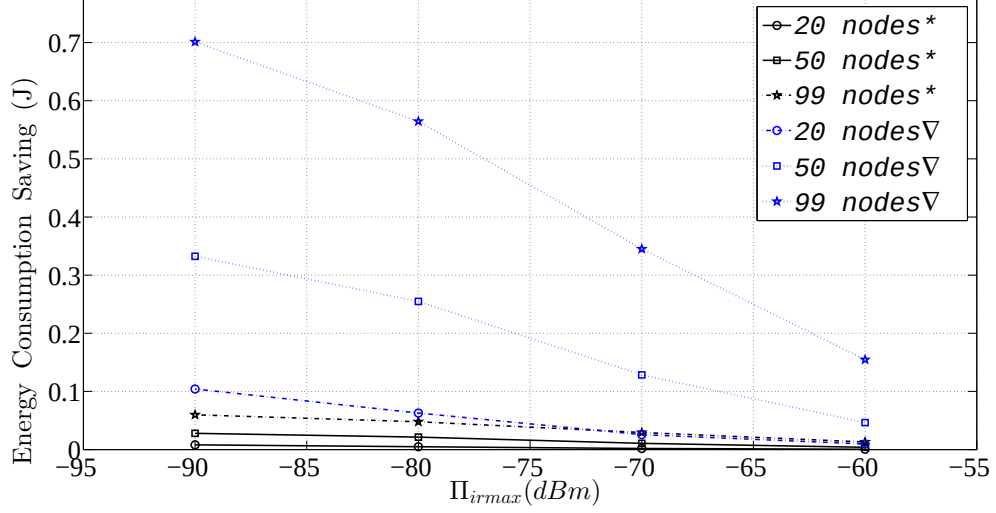


Figure 8.31: Energy consumption savings per node whit IR enabled, for different sizes of the network when each nodes generates either 50 packets (*) and 600 packets (∇).

Moreover, the higher is the network size the higher energy consumption saving is achieved. From Figure 8.31 it is observable that these energy savings are higher for $\Pi_{irmax} = -90$ dBm and decrease as Π_{irmax} increases. This is due to the reduction of the influential range area that causes a reduction of the overhearing of data packets by the node, decreasing the level of data packet redundancy, whilst leading to the increase of the energy consumption per node, (i.e., reduction of the energy consumption saving). While the energy saving can reach 21.42 % for 600 generated packets, it reaches up to 7.07 % for 50 generated packets.

Variable Number of Slot Channels

In this section, we analyze the impact of the number of slot channels and different network sizes while enabling the influential range concept in MC-SCP-MAC. For this set of tests all the nodes initiate CBR streams towards the sink node. Each node generates a packet every 2 s. Here the frame assumes two different values for the duration depending on the number of considered slot channels:

- For $N_{ch} = 8$, $t_F = 1.53$ s and $\Delta t_{SC} = 0.17$ s;
- For $N_{ch} = 15$, $t_F = 1$ s and $\Delta t_{SC} = 0.0625$ s.

The maximum contention window sizes are $CW_k^{max} = 80$, $k \in \{1, 2\}$. These long values for the contention window sizes enables to test how long they can be. We assume a maximum transmitter power $P_{tx} = 0.8$ mW and data packet size of $L_{data} = 32$ Bytes. The considered terrain size is 50×50 m². Retransmissions are disabled in these tests.

Figure 8.32 shows the average energy consumption per node when the IR concept is enabled for different sizes of network. Each node generates and sends 600 packets to the PAN. From Figure 8.32, it is noticeable that the increase of the number of slot channels leads to higher energy consumption. This is due to the increase of the available slot channels to send data

packets. As the value of Π_{irmax} increases the influential range of the node decreases, leading to the reduction of the overhearing and consequent decreasing of the discarded redundant data packets. Since discarding redundant data packets decreases as the values of the sensing range, Π_{irmax} increases, the node has to transmit more data packets which, in turn, increases the energy consumption per node. For $N_{ch} = 8$ slot channels, since a frame duration of $t_F = 1.53$ s is considered, the results presented in this section can be compared with the ones from MC-LMAC. This is possible because MC-LMAC considers a frame duration of $t_F = 1.6$ s.

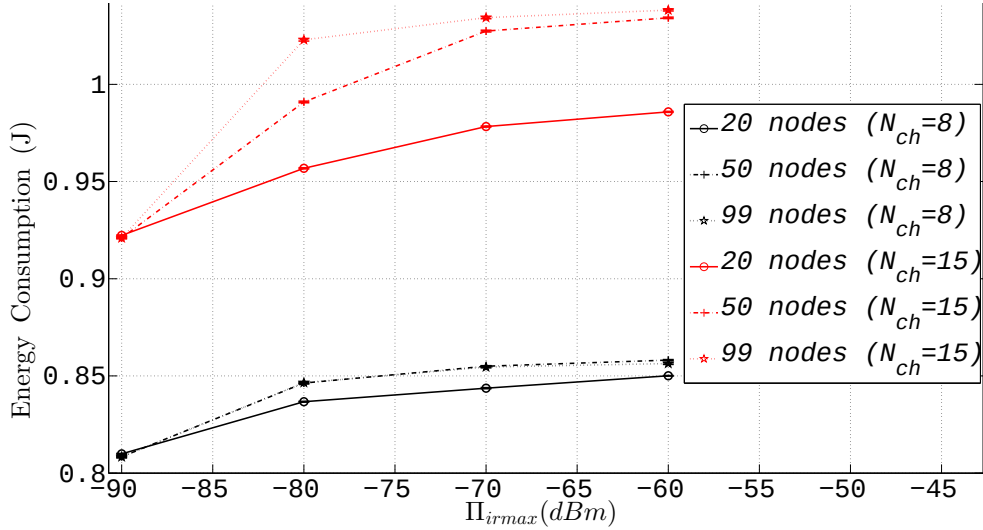


Figure 8.32: Average energy consumption per node when IR is enabled for different sizes of the network and number of data slot channels, i.e., $N_{ch} \in \{8, 15\}$ (600 packets).

Section J.2 from Appendix J presents the average energy consumption per node when IR is enabled for different sizes of network. Each node has 50 packets to be sent to the PAN.

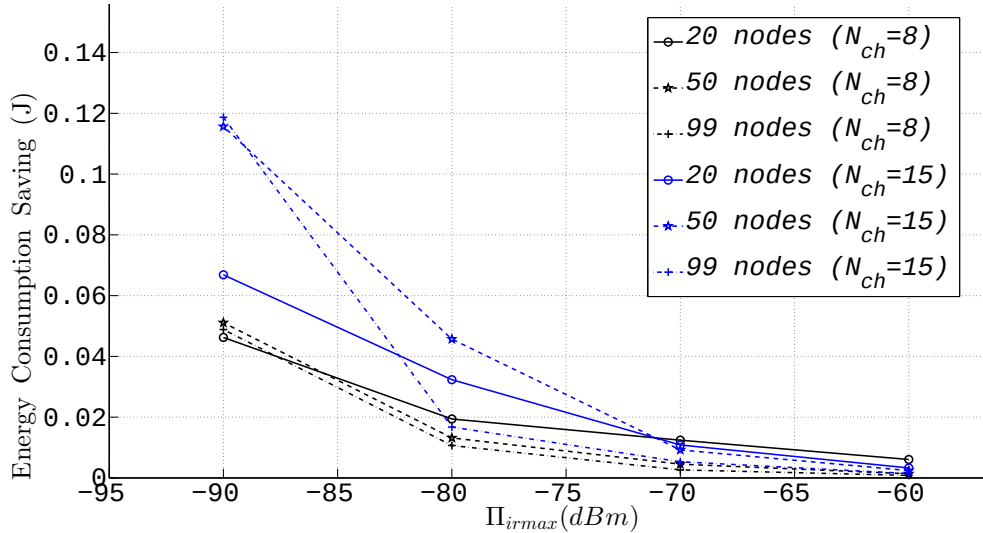


Figure 8.33: Energy consumption savings per node with IR enabled for different sizes of network and $N_{ch} \in \{8, 15\}$ (600 packets).

The evaluation of the benefits achieved by applying the IR concept in these tests is presented in Figure 8.33, where the energy consumption is presented as a function of the values of Π_{irmax} for different sizes of the network. For $\Pi_{irmax} = -90$ dBm the energy consumption saving is higher for $N_{ch} = 15$ slot channels. As explained before, the use of 15 slot channels leads to

higher delivery ratio (compared to the case $N_{ch} = 8$), which corresponds to a larger number of redundant packets dropped due to the application of the IR concept. In turn, the drop of a larger number of redundant data packets increases the energy consumption savings. For higher values of the sensing range, as the values of Π_{irmax} increases the influential range between the nodes decreases, which causes the decrease of the energy consumption savings. While the energy saving can reach 11.42 % for $N_{ch} = 15$, it reaches up to 5.94 % for $N_{ch} = 8$ slot channels.

8.5.6 Impact of Traffic Periodic and Exponential Patterns in the Overall Performance

Low Density of Nodes

In Section 8.5.4 we analyzed the impact of the number of slot channels on the network performance in a deployment scenario of $150 \times 150 \text{ m}^2$. Besides, the network performance metrics have been compared between MC-SCP and MC-LMAC. In this section, we analyze the different performance metrics, for the MC-SCP-MAC, MC-LMAC, CSMA and MMSN protocols while varying different parameters (e.g, number of sources nodes, number of slot channels, traffic generation intervals). The metrics include the aggregate throughput, delivery rate, energy consumption per node, energy consumption per packet and latency. We also assume that the nodes consider periodic and/or exponential traffic generation. The MC-LMAC, CSMA and MMSN protocols consider only periodic traffic, in which the traffic generation rate is $\lambda = 1/2 \text{ s}^{-1}$. In turn, both periodic and exponential traffic generation is considered in MC-SCP-MAC, in which $\lambda \in 1; 1/2 \text{ s}^{-1}$. The exponential traffic generation corresponds to a Poisson traffic profile, which is considered throughout the wireless communications literature as the one that offers the most realistic traffic generation profile. However, the authors from MC-LMAC [lvHJH11] did not account for this type of traffic in their tests.

Here, the frame duration is $t_F = 1.57 \text{ s}$. The time allocated for each slot channel is $\Delta t_{SC} = 0.17 \text{ s}$, for the MC-SCP-MAC. In turn, a frame duration of around $t_F = 1.6 \text{ s}$ is considered in MC-LMAC, CSMA and MMSN.

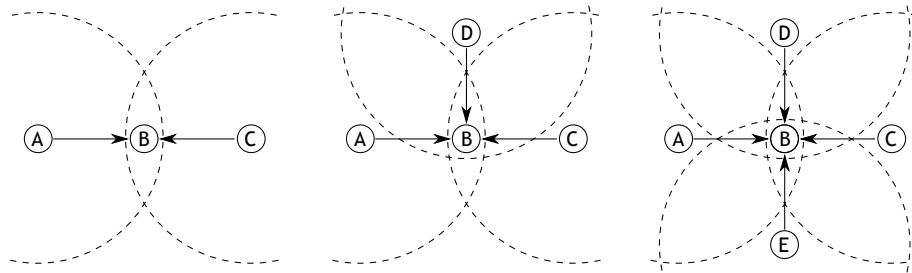


Figure 8.34: 1, 2 and 3-hidden terminal scenarios.

The MC-SCP-MAC considers maximum contention window sizes of $CW_k^{max} = 80$, $k \in \{1, 2\}$. For this set of results we consider a maximum transmitter power $P_{tx} = 0.8 \text{ mW}$ for all MAC protocols. Data packets size is $L_{data} = 32 \text{ Bytes}$. The number slot channels for data packets considered in these tests is $N_{ch} = 8$ for the MC-SCP-MAC, MC-LMAC and MMSN protocols. The CSMA protocol assumes a single-channel $N_{ch} = 1$. The considered terrain size is $150 \times 150 \text{ m}^2$ for the MC-SPC-MAC, MC-LMAC, CSMA and MMSN protocols. However, the authors from MC-LMAC [lvHJH11] consider that, in the multi-hop scenario, all nodes are in the carrier sensing range of each other while nodes in the 2nd tier cannot directly communicate with the sink node. This assumption does not considers the hidden terminals problem. Since the nodes in

MC-SCP-MAC are deployed randomly, they may not be in the carrier sensing range of all neighbouring nodes. Therefore, the MC-SCP-MAC protocol envisages a more realistic scenario, as it accounts for the hidden terminals presence in the different deployments.

Some insights can be explored in terms of the number of hidden terminals presented in each deployment. The authors from [CBCO12] have proposed an equation to calculate the number of hidden terminals. In [CBCO12], a scenario is first analyzed which is formed by a receiver, located in the middle, and a variable number (from 2 to 4) of source nodes. All the source nodes are hidden from each other and do not have any of transmitting neighbours, as shown in Figure 8.34. The term n_{hd} -hidden refers to the case where there are $n_{hd} + 1$ source nodes, therefore from each node point of view the number of hidden terminals is n_{hd} . As the distance from the different source nodes to the receiver is the same and the path loss model is used, no capture effect is possible (i.e., all packets that suffer a collision are lost). In the random scenario defined in [CBCO12], 99 sensor nodes are randomly placed in a given area, resulting in a given density of nodes. In our approach, as each node only sends packets to its parent, the routing effects are avoided. The number of neighbours per node and hidden terminals per communication pair can be addressed by considering the path loss propagation model and density of the nodes. The average neighbours (nodes that can sense the target node transmissions, i.e., in the carrier sense range) per node is obtained as: $n_{ngb} = \gamma \pi r_d^2 - 1$, where the radius corresponding to the radio range of the node is $r_d = 89$ m, the transmitter power is $P_{tx} = 0.8$ mW and γ is the node density (note that γ_{99} represents the density of our network, formed by 99 nodes plus the PAN coordinator). We also consider the IEEE 802.15.4 outdoor propagation model and a carrier sense threshold of -94 dBm. To compute the average number of hidden nodes, the exclusive area of two circles of the same radius, r_d , separated by a distance, d , is given by part of the area of one circle that does not belong to the other circle (range of the other node defining the coverage area of the hidden terminal):

$$A_e = \pi r_d^2 - \left[2r_d^2 \arccos\left(\frac{d}{2r_d}\right) - \frac{1}{2}d\sqrt{4r_d^2 - d^2} \right] \quad (8.12)$$

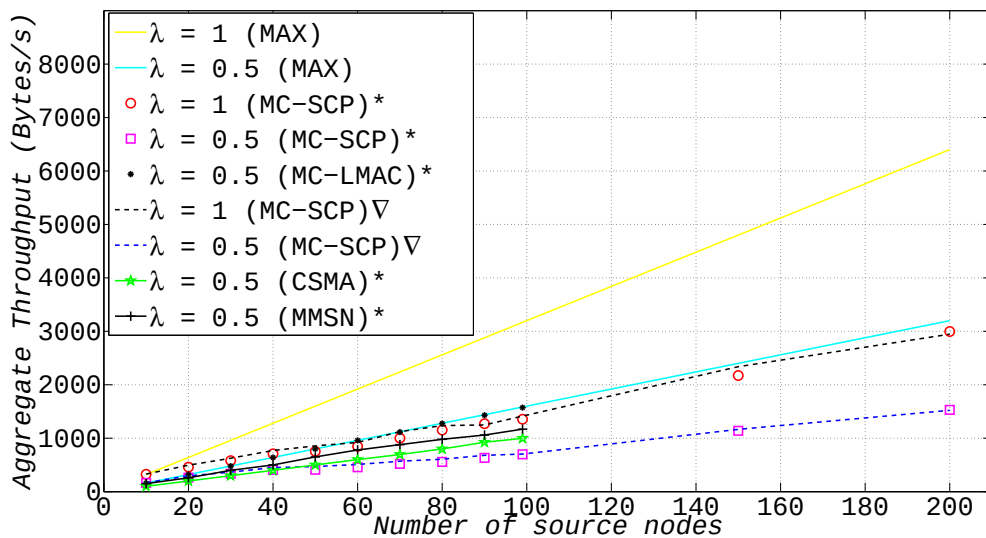


Figure 8.35: Aggregate throughput as a function of the number of sources for MC-SCP-MAC, MC-LMAC, CSMA and MMSN, with periodic (*) and exponential (∇) traffic patterns in the 150×150 m² deployment scenario.

The distance between the two centres that makes the inner (common) area equal to the outer (exclusive area) one is $d = 0.8079455 \times r_d$ [Slo91], therefore the number of hidden terminals (average number of nodes in the exclusive area) can be computed as $n_{hd} = \gamma A_e$. In these tests the considered density is $\gamma_{99}=0.0044$ nodes/m². To compute the exclusive area and the average number of hidden nodes (the ones in the exclusive area), we obtain 55 hidden terminals on average, for 100 nodes in the network (99 source nodes plus the PAN coordinator). The test performed with the MC-SCP-MAC accounts for these hidden terminals, while the remaining MAC protocols (MC-LMAC, MMSN and CSMA) do not consider the presence of hidden terminals. The retransmissions are disabled in all the MAC protocols, for the sake of fairness in the comparisons. Figure 8.35 presents the results obtained for the aggregate throughput, in the MC-SCP, MC-LMAC, MMSN and CSMA protocols by considering the active source nodes. In the case of **periodic traffic** generation with $\lambda = 1/2 \text{ s}^{-1}$ the aggregate throughput for the MC-SCP-MAC is close to the maximum until $n = 50$ nodes. However, the aggregate throughput starts to decrease as soon as the number of source nodes increases. This loss in the aggregate throughput is explained by the contention and hidden terminals. These problems lead to an increase of the packet loss in the PAN coordinator.

In this set of tests, MC-LMAC performs better since it assigns slots to all the nodes whether they are sources or not. With this feature, the performance of MC-LMAC is close to the maximum aggregate throughput. Similarly to MC-SCP-MAC, MMSN and CSMA also suffer from contention. However, they achieve a higher aggregate throughput than MC-SCP. This is because it is assumed by the authors from [lvHJH11, ZHY⁺06] that all nodes are in the same carrier sensing range, i.e., there are no hidden terminals. We also investigated the scenarios where nodes **exponentially** generate packets with $\lambda = 1/2 \text{ s}^{-1}$ for the MC-SCP-MAC protocol. In this set of tests the aggregate throughput is slightly higher than the one with periodic traffic, but it also suffers some loss. Even though MC-SCP-MAC achieves lower aggregate throughput, the presented results are more realistic than the ones for remaining the MAC protocols. One solution to mitigate this loss in the aggregate throughput from MC-SCP is to increase the transmitter power as verified in Section 8.5.4 or even to increase the number of available slot channels. Since MC-SCP-MAC is ready to cope with denser scenarios, another solution may be to increase the density of nodes.

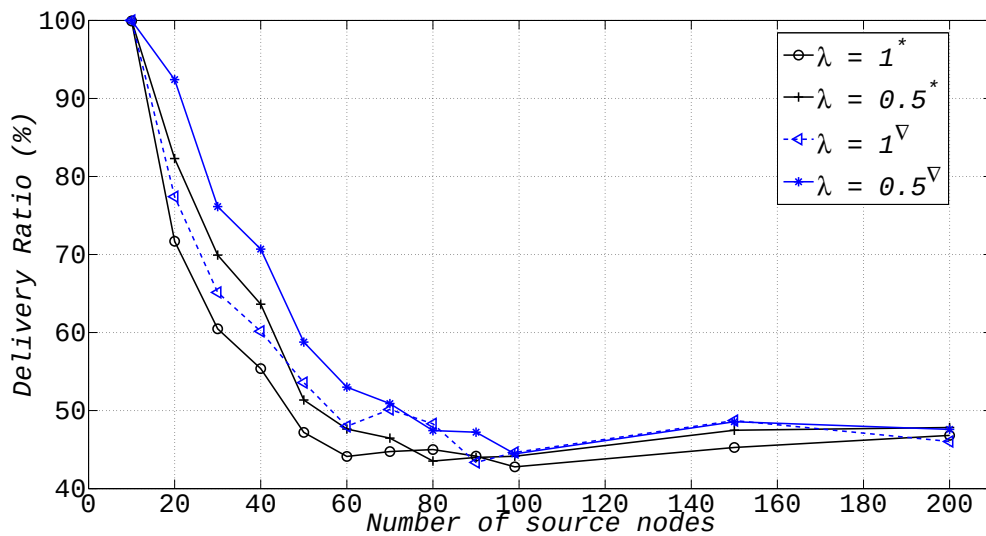


Figure 8.36: Delivery rate of MC-SCP-MAC as a function of the number of source nodes with periodic (*) and exponential (∇) traffic patterns in the 150×150 m² deployment scenario.

To verify this increase in the density of nodes in $150 \times 150 \text{ m}^2$ deployment scenario, we have increased the number of source nodes while obtaining new results. We have verified an increase of the aggregate throughput with the increase in the node density. The authors from MC-L-MAC [lvHJH11] also investigated scenarios in which nodes generate packets more frequently. In this case, all the protocols (MC-LMAC, CSMA, and MMSN) experienced buffer overflows. Although these MAC protocols did not succeed to cope with higher data generation rates, some tests have been performed for MC-SCP-MAC considering $\lambda = 1 \text{ s}^{-1}$ under periodic and exponential traffic patterns. The results from Figure 8.35 show that MC-SCP-MAC supports higher data generation rates but it continues to suffer losses in the aggregate throughput. The aggregate throughput is similar to the maximum aggregate throughput when $\lambda = 1/2 \text{ s}^{-1}$. Similar solutions to the ones mentioned before may be applied to mitigate these losses. Section J.3 of Appendix J presents detailed results for the aggregate throughput for the MC-SCP-MAC, MC-LMAC, MMSN and CSMA protocols with periodic and exponential traffic patterns.

Here, we evaluate the network performance in terms of the delivery ratio of the MC-SCP-MAC protocol, for periodic and exponential traffic patterns, with $\lambda \in \{1/2; 1\} \text{ s}^{-1}$. When the network is sparser, the achieved delivery ratio is lower. Figure 8.36 shows that the achieved delivery ratio decreases as the number of source nodes increases for all the traffic generation patterns considered here. This decrease is verified up to $n = 99$ nodes. As soon as the density starts to increase (i.e., $n > 99$) the delivery ratio starts to increase again. The exponential traffic generation profile is the one that presents the highest delivery ratio.

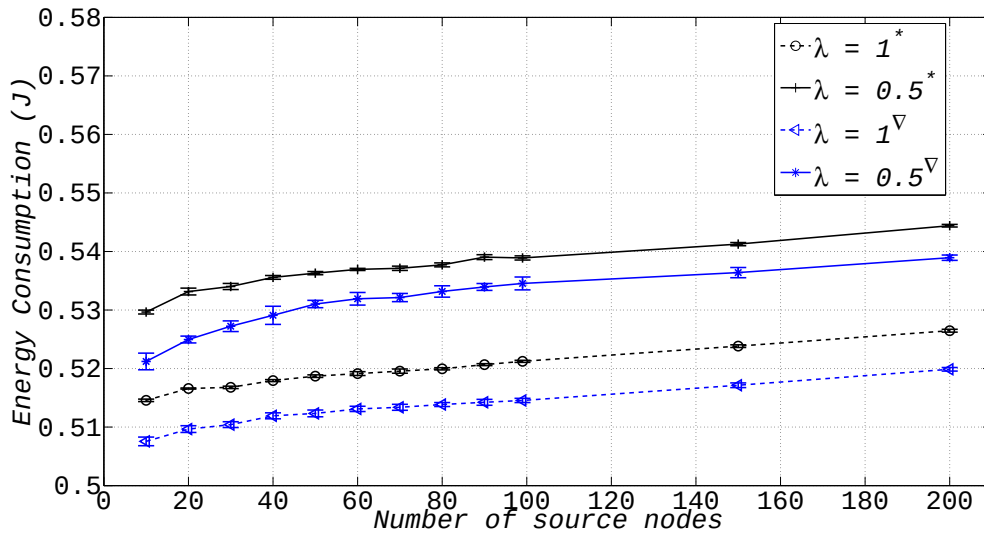


Figure 8.37: Energy consumption per node of MC-SCP-MAC as a function of the number of sources with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.

Figure 8.37 presents the dependence of the energy performance on the number of source nodes from MC-SCP-MAC for the traffic generation patterns considered within these tests. The 95 % confidence intervals are also presented in this Figure. Here, the energy consumption of the PAN coordinator is not taken into account, since this node has extended capabilities and is not limited by any energy constraint. In Figure 8.37 it is noticeable that as the number of sources increases, the energy consumption also increases, as expected. However, this increase occurs at a slow rate, which indicates an almost constant energy consumption per node, for all the considered densities. The higher traffic generation rates are the ones that present the lowest energy consumptions. The high traffic generation rate causes the nodes to quicker dispatch the packets to the PAN, which diminishes the active time of the node. Hence, the energy

consumption of the node is also reduced. The exponential traffic pattern, is the one that presents the lowest energy consumption.

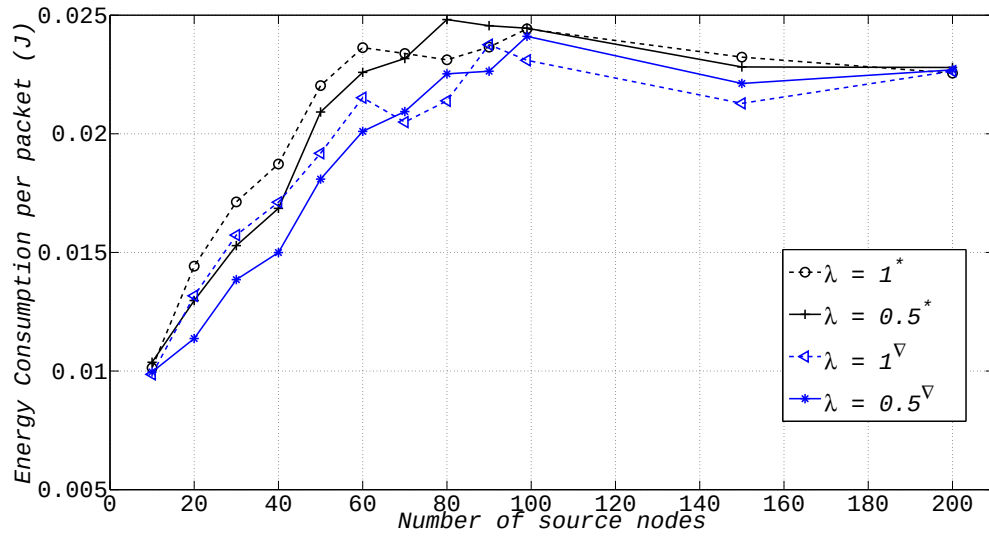


Figure 8.38: Energy consumption per packet successfully delivered of MC-SCP-MAC as a function of the number of nodes with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.

Figure 8.38 evaluates the energy consumption per packet successfully delivered by the MC-SCP-MAC protocol, for periodic and exponential traffic patterns with $\lambda \in \{1/2; 1\} \text{ s}^{-1}$. The periodic traffic pattern is the one that presents the highest values of the energy consumption per packet. This is explained by the highest energy consumption observed in Figure 8.37 for this type of traffic along with the respective low delivery rate, as shown in Figure 8.36. In turn, the exponential traffic patterns are the ones that present the lowest values, of the energy consumption per delivered packet. One interesting result is the decrease in the values of the energy consumption per delivered packet for $n > 99$ nodes. This is explained by the increase of the delivery ratio verified in Figure 8.36, jointly with the nearly constant energy consumption, which causes the decreasing of the energy consumption per delivered packet.

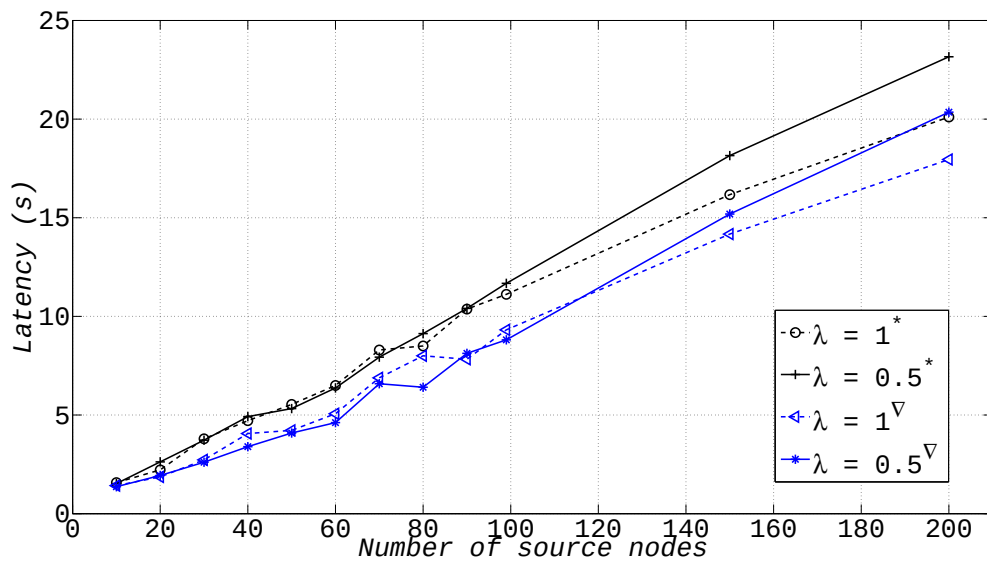


Figure 8.39: Latency of MC-SCP-MAC as a function of the number of sources with periodic (*) and exponential (∇) traffic patterns in the $150 \times 150 \text{ m}^2$ deployment scenario.

Figure 8.39 shows the results for the end-to-end latency (between the source node and the reception at the PAN coordinator). This metric accounts for the time from control messages in MC-SCP-MAC. The exponential traffic pattern is the one that presents the lowest values for the latency. High latency is typical from the scheduled-based MAC protocols, since the node has to wait until it senses a free medium to transmit the wake-up tone and, finally, the data packet. The MC-SCP-MAC protocol has an option that can be enabled in order to reduce the latency. This technique limits the time validity of the data included in the packet. If the data included in the packet exceeds its validity then it is dropped. This may reduce the delivery rate but it can decrease the latency. To achieve shorter latency, a technique can be used that shuts-down a wake-up state from the RFDs nodes if any neighbouring node wants to send packets to him. This method is going to be described in detail in Section 8.6. Other solution is to decrease the frame size. However, decreasing the frame duration may cause the decrease of the delivery ratio to the sink. A fair tradeoff between the frame size, delivery ratio and latency is therefore needed.

High Density of Nodes

With high density nodes, we also analyze the aggregate throughput, delivery rate, energy consumption per node, energy consumption per packet and latency, for the MC-SCP-MAC, MC-L-MAC, CSMA and MMSN protocols. We study the dependency of these parameters on the number of sources nodes, number of slot channels, as well as traffic generation intervals. For this set of tests, we also consider periodic or exponential traffic patterns. Here, the frame duration is $t_F = 1.57$ s and the time allocated for each slot channel is $\Delta t_{SC} = 0.0625$ s for MC-SCP-MAC. In turn, MC-LMAC, CSMA and MMSN consider a frame duration $t_F = 1.6$ s. The MC-SCP-MAC protocol considers maximum contention window sizes $CW_k^{max} = 80, k \in \{1, 2\}$. For this set of results we consider a maximum transmitter power $P_{tx} = 0.8$ mW for all MAC protocols and a data packet size of $L_{data} = 32$ Bytes. The number of slot channels for data utilized in these tests is

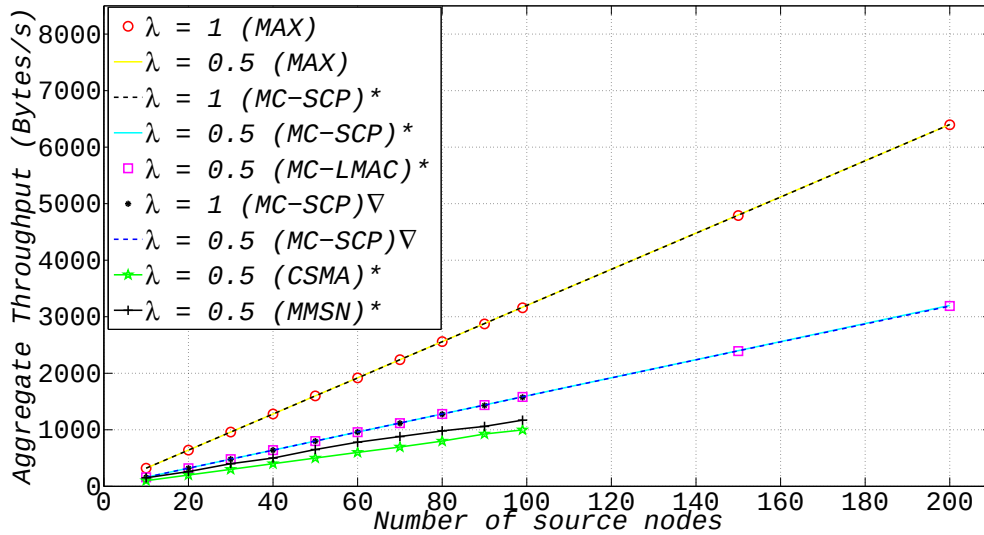


Figure 8.40: Aggregate throughput for the MC-SCP-MAC, MC-LMAC, CSMA and MMSN protocols with periodic (*) and exponential (∇) traffic patterns for different number of sources in the 50×50 m² deployment scenario.

$N_{ch} = 8$ for the MC-SCP-MAC, MC-LMAC and MMSN protocols, while a single-channel ($N_{ch} = 1$) is considered for CSMA. Since the MC-SCP-MAC protocol achieves better results in scenarios with higher densities of nodes, for a given number of nodes the terrain size considered in these tests for the MC-SCP-MAC protocol is 50×50 m², whereas for MC-LMAC, CSMA and MMSN protocols an

area of $150 \times 150 \text{ m}^2$ is considered. By decreasing the area of deployment of the MC-SCP the nodes will be in the carrier sensing range of each other, which, in turn, mitigates the hidden terminals problem allowing for comparison with the MC-LMAC, MMSN and CSMA protocols. In all the MAC protocols, the retransmissions are disabled, for fair comparison. Figure 8.40 shows the variation of the aggregate throughput with the number of source nodes for the MC-SCP, MC-LMAC, MMSN and CSMA, in terms of active source nodes. For **periodic traffic** (uniform distribution) generation with $\lambda = 1/2 \text{ s}^{-1}$ the MC-SCP-MAC is close to the maximum aggregate throughput as the number of sources increases. The same holds for the MC-LMAC protocol. We also investigated the scenarios where nodes generate packets with **exponential** distribution at a rate $\lambda = 1/2 \text{ s}^{-1}$ for the MC-SCP-MAC protocol. In these tests the aggregate throughput is also near the maximum of the aggregate throughput. With low density of nodes $150 \times 150 \text{ m}^2$ (sparser scenario) in MC-SCP-MAC, under periodic and exponential traffic pattern, the aggregate throughput was much lower than the maximum achievable. However, in the $50 \times 50 \text{ m}^2$ scenario the density of nodes is higher yielding an aggregate throughput close to the maximum, as shown in Figure 8.41. These results show the best performance of the MC-SCP-MAC protocol in high density scenarios.

However, the presence of hidden terminals may lead to degradation of the aggregate throughput as the number of source nodes increases and a method that decreases the impact of the hidden terminal problem may be needed. We can also conclude that the increase of the traffic generation frequency is well supported by MC-SCP-MAC when the hidden terminals is not an issue. Section J.4 of Appendix J presents detailed results for the aggregate throughput of the MC-SCP-MAC, MC-LMAC, MMSN and CSMA protocols with periodic and exponential traffic patterns.

Figure 8.41 shows the variation of the delivery rate as a function of the number of source nodes for MC-SCP-MAC protocol for periodic and exponential traffic patterns, for $\lambda \in \{1/2; 1\} \text{ s}^{-1}$. It is shown that the delivery rate is always near the maximum, even for large number of source nodes, corresponding to values of the aggregate throughput near the maximum in Figure 8.40.

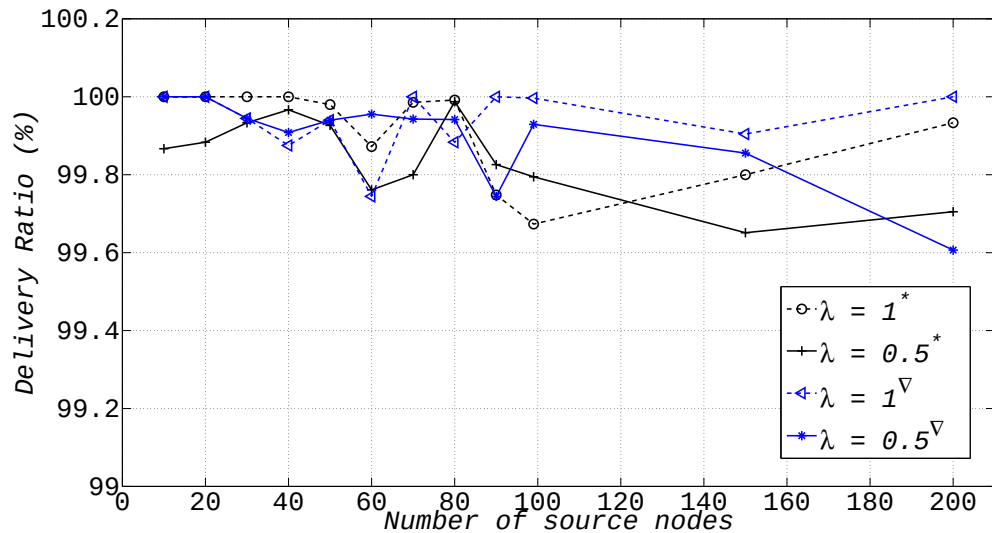


Figure 8.41: Delivery rate for the MC-SCP-MAC protocol with periodic (*) and exponential (∇) traffic patterns for different number of sources in the $50 \times 50 \text{ m}^2$ deployment scenario.

Figure 8.42 presents the dependence of the energy performance on the number of source nodes from MC-SCP-MAC for the traffic generation patterns considered within these tests. The 95 % confidence intervals are also presented in this Figure. Here, the energy consumption of the

PAN coordinator is not taken into account, since this node has extended capabilities and is not limited by any energy constraint. In Figure 8.37 it is noticeable that as the number of sources increases, the energy consumption also increases, as expected. However, this increase occurs at a slow rate, which indicates an almost constant energy consumption per node, for all the considered densities. By comparing Figure 8.42 with Figure 8.37 it is observable that the reduction of the area from the deployment scenario leads to a slight increase of the energy consumption, whilst attaining higher aggregate throughput and delivery rate. Similarly to the results for the energy consumption in Figure 8.37 these tests show that higher traffic generation rates lead to the lowest values for the energy consumptions.

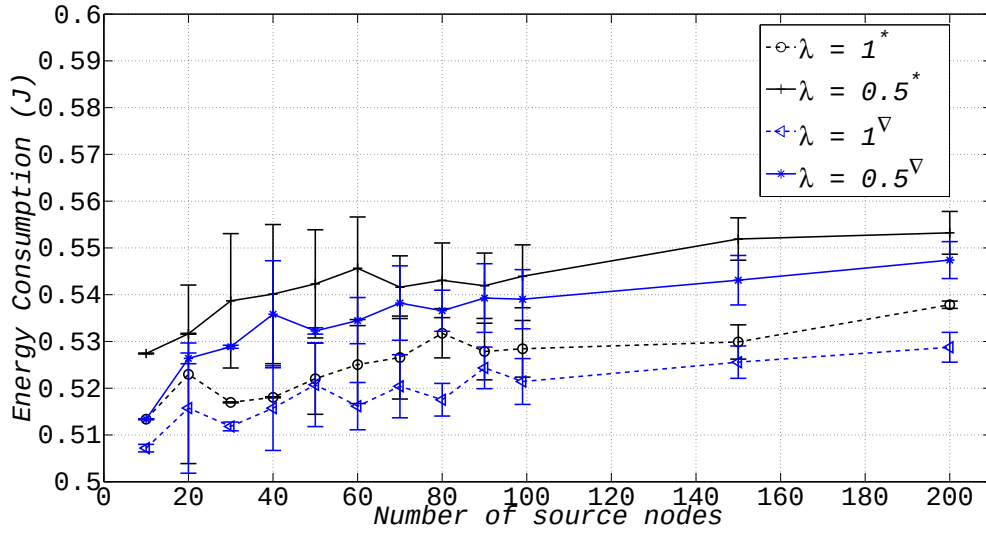


Figure 8.42: Energy consumption per node of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$.

Figure 8.42 evaluates the energy consumption per packet successfully delivered by the MC-SCP-MAC protocol, for periodic and exponential traffic patterns with $\lambda \in \{1/2; 1\} \text{ s}^{-1}$ for a scenario with high density of nodes than the one in Section 8.5.6.

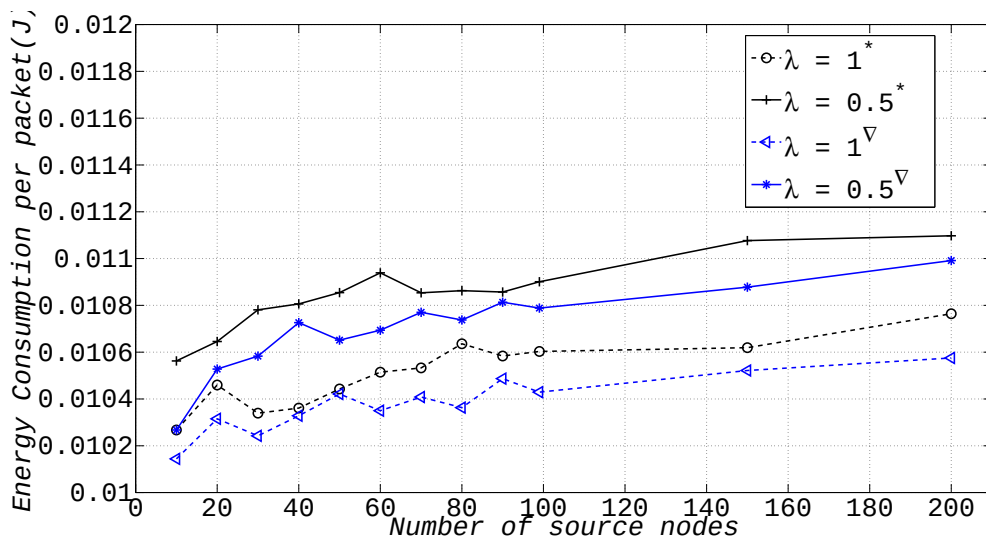


Figure 8.43: Energy consumption per packet successfully delivered of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$.

In Figure 8.43 it is noticeable that the curves for $\lambda = 1/2 \text{ s}^{-1}$ are the ones that present the

highest energy consumption. This is explained by the highest energy consumption observed in Figure 8.42 jointly with the high delivery rate presented in Figure 8.41 that cause an effective decrease of the energy consumption per delivered packet, compared with the results presented in Figure 8.38. Therefore, we conclude that a deployment scenario with higher density of nodes allows for mitigating the hidden terminals problem while achieving less energy waste per successfully delivered packet.

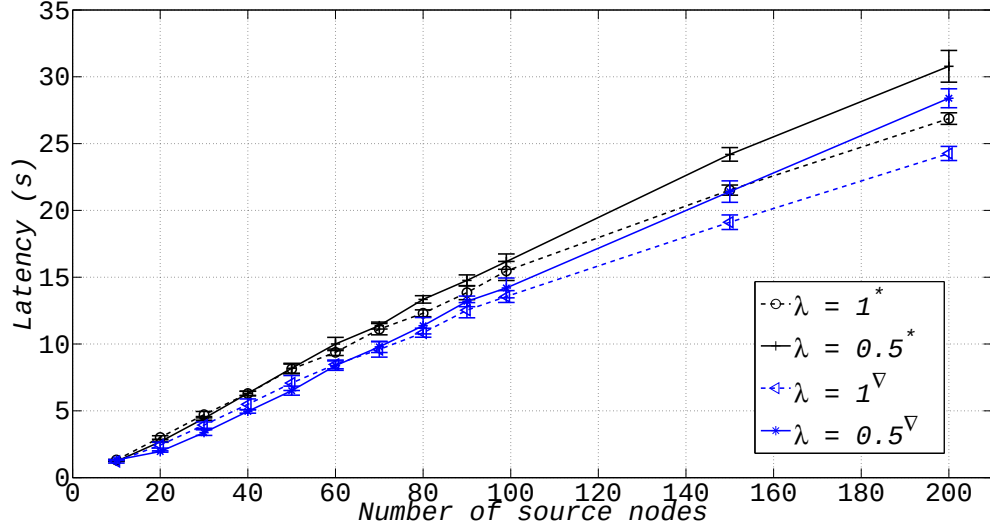


Figure 8.44: Latency of MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation for different number of sources in deployment scenario of $50 \times 50 \text{ m}^2$.

Figure 8.44 addresses the results obtained for the end-to-end latency. The 95 % confidence intervals are also presented in this Figure. The exponential traffic patterns is the one that presents the lowest values for the latency (as the number of source nodes increases). By comparing the results from Figure 8.39 with these ones (higher density of node) we conclude that the values for the latency present similar values up to $n = 30$. However, for a number of source nodes higher than 30, the latency is longer in the $50 \times 50 \text{ m}^2$ deployment scenario. This is explained by the increase of the number of contention nodes and the capability of all nodes to sense each other which facilitates to detect nodes more often in the data packet transmission phase. Hence, less collisions are originated but the latency becomes longer.

8.5.7 Impact of the Density of Nodes

The results for the aggregate throughput, and delivery ratio, from MC-SCP-MAC are compared with the ones from MC-LMAC, and CSMA protocols. In order to test the scalability of the MC-SCP-MAC protocol we have varied the density of the node deployments from $50 \times 50 \text{ m}^2$ to $75 \times 75 \text{ m}^2$, $100 \times 100 \text{ m}^2$, $125 \times 125 \text{ m}^2$, $150 \times 150 \text{ m}^2$ and $200 \times 200 \text{ m}^2$. The authors from MC-LMAC [lvHJH11] claim that with random deployment beyond a side length (L) of 225 m, unconnected nodes appear. Although we have performed tests with larger deployments, unconnected nodes only start to appear after for side lengths larger than 400 m. However, for the sake of fair comparison with the other MAC protocols we only consider side lengths up to 200 m. For this set of tests nodes we assume periodic or exponential traffic patterns. Here, the frame duration is $t_F = 1.57 \text{ s}$ and the time allocated for each slot channel is $\Delta t_{SC} = 0.17 \text{ s}$ for MC-SCP-MAC, and $t_F = 1.6 \text{ s}$ for MC-LMAC and CSMA consider. Maximum contention window sizes are $CW_k^{max} = 80$, $k \in \{1, 2\}$ for the MC-SCP-MAC protocol. We consider a maximum transmitter power $P_{tx} = 0.8 \text{ mW}$ for

all MAC protocols and data packet size of $L_{data} = 32$ Bytes. The number slot channels considered in these tests for data is $N_{ch} = 8$ for the MC-SCP-MAC and MC-LMAC protocols, while a single-channel ($N_{ch} = 1$) is considered in CSMA. The objective of these tests is to analyze the gains achieved when the IR is enabled for different values of $\Pi_{irmax} \in \{-90; -80; -70; -60\}$ dBm. In all the MAC protocols, the retransmissions are disabled for the sake of fairness in comparisons. Figure 8.45 shows the variation of the aggregate throughput with the side length, L , for the MC-SCP-MAC, MC-LMAC, and CSMA protocols. A periodic traffic with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$ is considered. MC-SCP-MAC presents high values of the aggregate throughput if the scenario deployment is denser and IR is enabled. Beyond a side length of 100 m, the aggregate throughput from MC-SCP-MAC starts to decrease, while the aggregate throughput of MC-LMAC continues to increase. However, for a side length of 150 m, the aggregate throughput of MC-LMAC starts to decrease due to the sparsity of the scenario, while the aggregate throughput of MC-SCP-MAC starts to increase. If the IR is disabled, the aggregate throughput of the MC-SCP-MAC achieves its highest values. When the IR is enabled the values of aggregate throughput are always lower owing to the drop of redundant packets. It reduces the aggregate throughput but it increases the node lifetime while decreasing the latency, as discussed in earlier sections. For denser scenarios (e.g., $L = 50$ m) the MC-SCP-MAC protocol achieves much higher aggregate throughput than the remaining MAC protocols.

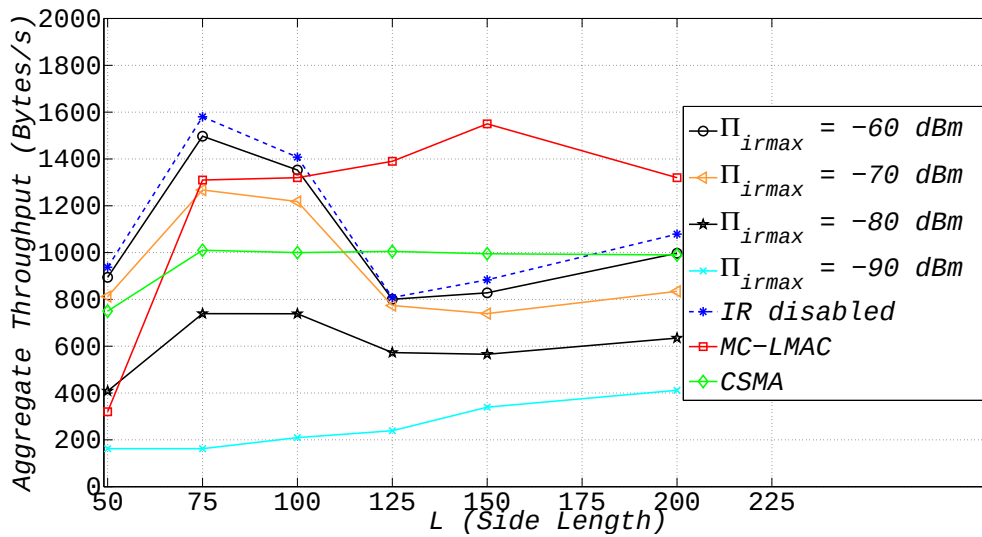


Figure 8.45: Aggregate throughput of MC-SCP-MAC, MC-LMAC and CSMA protocols with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) for different deployment scenario side lengths when IR enabled or disabled.

In Section J.6 from Appendix J results are presented for the aggregate throughput as a function of the side length for MC-SCP-MAC while considering a periodic traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

Figure 8.46 shows the variation of the aggregate throughput with the coverage distance for the MC-SCP when considering an **exponential traffic** profile with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$. The 95 % confidence intervals are also presented in this Figure. In this case the values obtained for the aggregate throughput are similar to the ones for periodic traffic from Figure 8.45. The MC-SCP-MAC presents high values for the aggregate throughput when the IR is enabled. Beyond a side length of 100 m, the aggregate throughput of MC-SCP-MAC starts to decrease. However, for a side length of 150 m, the aggregate throughput of MC-SCP-MAC starts to increase. If the IR is disabled the aggregate throughput of the MC-SCP-MAC protocol achieves its highest values. The values of aggregate throughput when the IR is enabled are always lower because of the

drop of redundant packets.

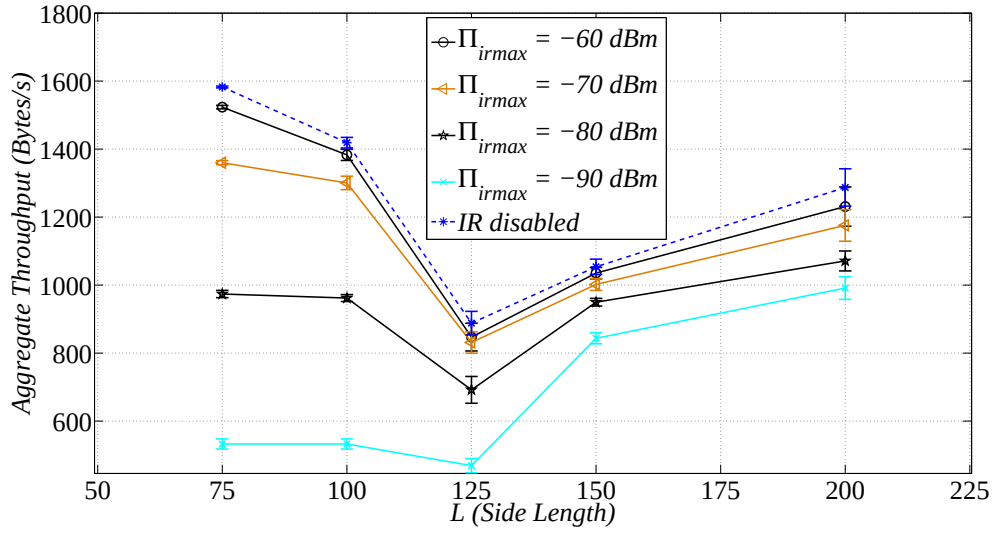


Figure 8.46: Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

In Section J.6 from Appendix J are presented results for the aggregate throughput of MC-SCP-MAC as a function of the side lengths when considering an exponential traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

Figure 8.47 shows the results for the delivery ratio as a function of the side length of the MC-SCP, MC-LMAC, and CSMA protocols, when considering a **periodic** traffic profile with a generation frequency of $\lambda = 1/2 \text{ s}^{-1}$. MC-SCP-MAC presents higher values of delivery ratio when the scenario deployment is denser for both the situations, i.e., when IR is enabled and disabled. Compared with the MC-LMAC protocol, MC-SCP-MAC achieves higher delivery ratios for side lengths that vary from 50 to 100 m. For longer side lengths, the delivery ratio of MC-SCP-MAC decreases sharply, while the MC-LMAC is maintained constant around 92 %. In Figure 8.47, an interesting behaviour of MC-SCP-MAC is the increase of the delivery ratio for side lengths longer than 125 m. For denser scenarios i.e., $L = 50$ m the MC-SCP-MAC achieves much higher delivery ratios than the considered MAC protocols.

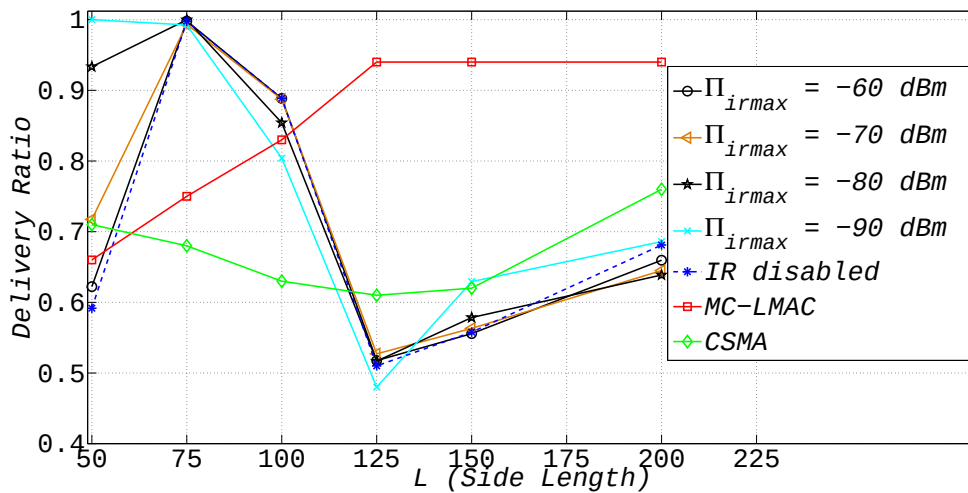


Figure 8.47: Delivery ratio of MC-SCP-MAC, MC-LMAC and CSMA as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

Section J.6 from Appendix J addresses the results for the delivery ratio as a function of the side length of the deployment scenario when considering a periodic traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

Figure 8.48 presents the delivery ratio of MC-SCP-MAC as a function of the side length of the deployment scenario whilst considering an **exponential** traffic profile with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$. The 95 % confidence intervals are also presented in this Figure. By comparing these results with the ones of the aggregated throughput from Figure 8.45, for side lengths that vary between 50 and 125 m, the delivery ratios are similar, whereas, for side lengths longer than 125 m, the delivery ratios in the **exponential** case are higher than in the periodic one. For all the considered values of the sensing range, Π_{irmax} , the delivery ratios are similar.

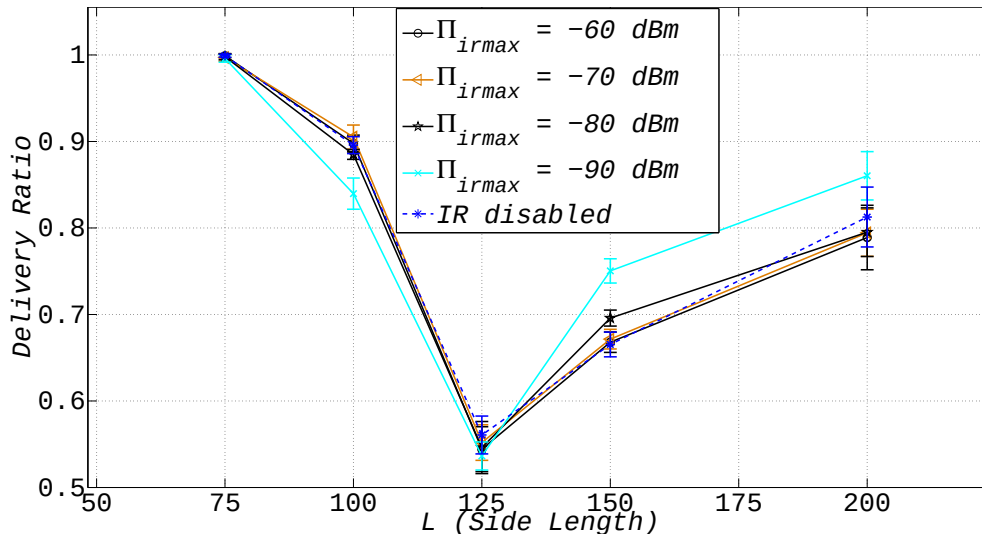


Figure 8.48: Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

Detailed results on the delivery ratio as a function of the side lengths of the deployment scenario for MC-SCP-MAC, for exponential traffic profile $\lambda = 1/10 \text{ s}^{-1}$, are presented in Section J.6 from Appendix J.

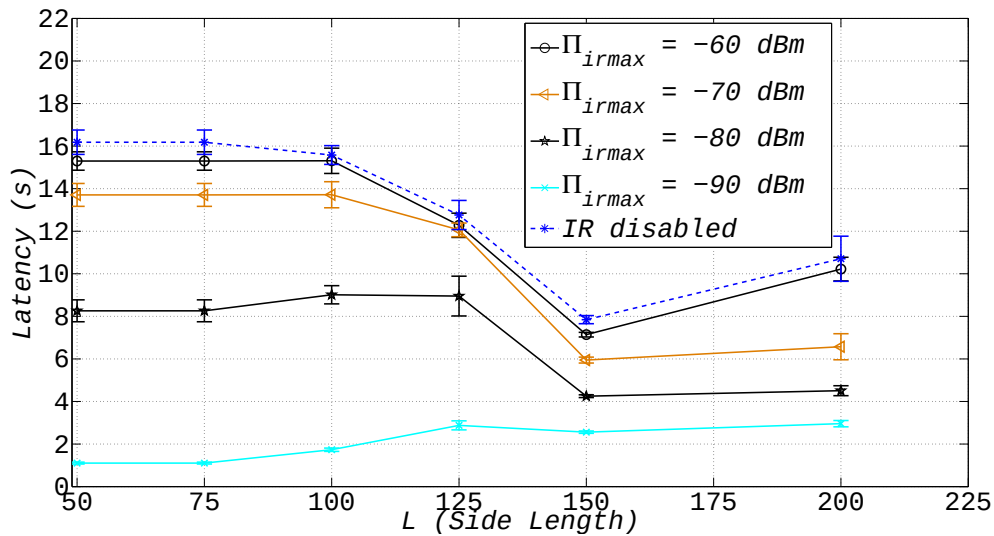


Figure 8.49: Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

Figure 8.49 presents the end-to-end latency of MC-SCP-MAC as a function of the side length of the deployment scenario for **periodic** traffic profile, with generation rate of $\lambda = 1/2 \text{ s}^{-1}$. The 95 % confidence intervals are also presented in this Figure. The MC-SCP-MAC presents shorter latency if IR is enabled for all the values of the sensing range, Π_{irmax} . As the value of sensing range, Π_{irmax} , increases, the latency also increases, for all the considered values for the side length. The short values for the latency if IR is enabled is due to the reduction of the redundant data packets waiting to be transmitted in the queue. As shown in Figure 8.45, the use of IR may reduce the aggregate throughput but the latency is considerably reduced, too, as shown in Figure 8.49. The longest latency is verified when the IR is disabled, while the case, $\Pi_{irmax} = -90 \text{ dBm}$ always presents the shortest latency. For side lengths that vary between 50 and 100 m the values are different for all the considered values of sensing range, Π_{irmax} , when the IR is enabled and disabled. The latency decreases between side lengths of 100 and 150 m, except for sensing range of $\Pi_{irmax} = -90 \text{ dBm}$. For side lengths longer than 150 m the values for the latency are relatively constant, except for IR disabled and IR enabled with sensing range $\Pi_{irmax} = -60 \text{ dBm}$, as shown in Figure 8.49. Section J.6 from Appendix J addresses the latency of MC-SCP-MAC for periodic traffic pattern with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

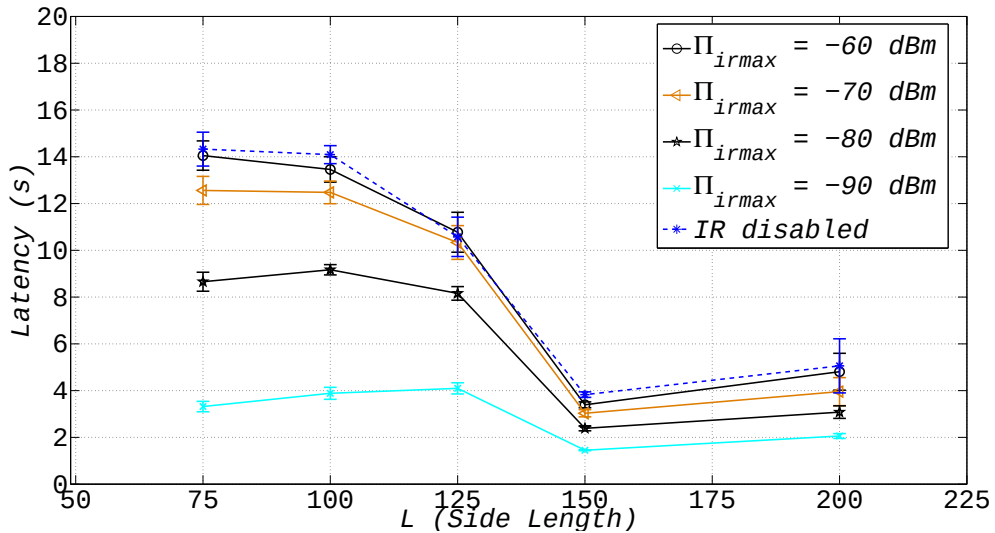


Figure 8.50: Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

Figure 8.50 presents the dependence of the end-to-end latency on the side lengths of the deployment scenario in MC-SCP-MAC for an **exponential** traffic pattern with a generation rate $\lambda = 1/2 \text{ s}^{-1}$. The MC-SCP-MAC presents short latency with IR enabled, for all the values of the sensing range, Π_{irmax} . As the value of sensing range, Π_{irmax} , increases, the latency also increases for all the considered side lengths. By comparing these results with the ones presented in Figure 8.49 all the values for the latency are similar in both results, except for the case with IR enabled and sensing range of $\Pi_{irmax} = -90 \text{ dBm}$, in which the exponential profile presents longer latency.

Section J.6 from Appendix J presents the results for the the latency of MC-SCP-MAC as a function of the side length of the deployment scenario whilst considering an exponential traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

Here, we evaluate the energy consumption of MC-SCP-MAC as a function of the side length whilst considering periodic traffic profile with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$, considering the cases where IR is enabled and disabled. These results are presented in Figure 8.51, where

the 95 % confidence intervals are also presented. As the value of the side length from the deployment scenario increases the energy consumption is pretty constant up to the value of 125 m for the side length. This is due to the high delivery ratio that MC-SCP-MAC presents in denser scenarios along with the consequent decrease of hidden terminals on the deployment. For side lengths larger than 125 m the MC-SCP-MAC presents high energy consumption. This is explained by the increase of the presence of more hidden terminals, which cause the MC-SCP-MAC to decrease the delivery ratio and, consequently suffer from an increase of the energy consumption. MC-SCP-MAC presents the highest values for the energy consumption when the IR is disabled. However, we can observe in Figure 8.51 that, by enabling the IR, the energy consumption slightly decreases. This is due to the slight increase of delivery ratio verified when the IR is enabled.

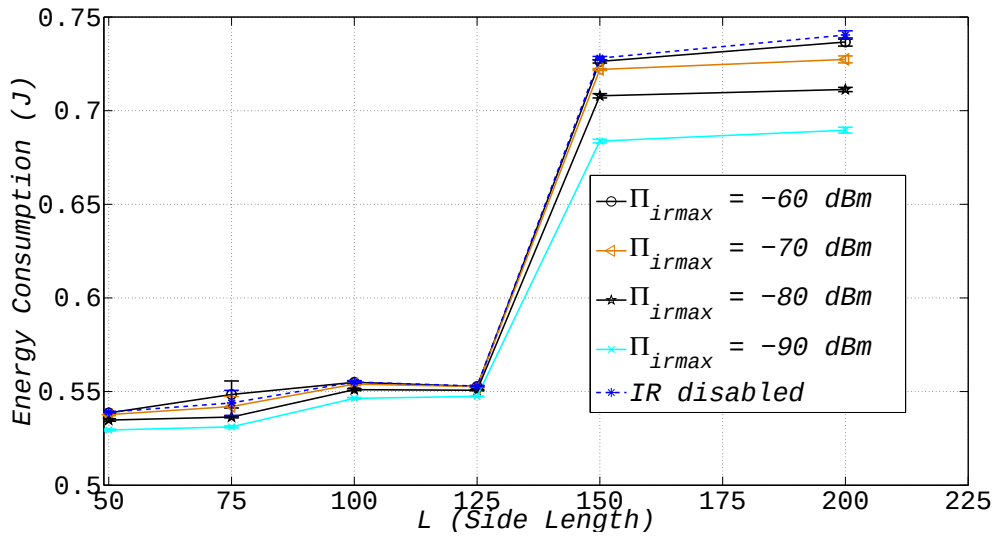


Figure 8.51: Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

Section J.6 from Appendix J presents the results for the energy consumption of MC-SCP-MAC as a function of the side lengths whilst considering **periodic** traffic profile with a generation frequency of $\lambda = 1/10 \text{ s}^{-1}$, when the IR is enabled and disabled.

Figure 8.52 shows the results for the energy consumption per node when an exponential traffic profile is considered with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$, when the IR is enabled and disabled. The 95 % confidence intervals are also presented in this Figure. For all the values of the side length, the values for the energy consumption are similar to the ones from periodic traffic presented in Figure 8.51. The differences are negligible for all the considered values of the sensing range.

Section J.6 from Appendix J also addresses the results for the energy spent by the MC-SCP-MAC as a function of the side lengths whilst considering exponential traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$, when the IR is enabled and disabled.

It is now worthwhile to evaluate the energy saving gains that can be achieved with the employment of the IR concept, as shown in Figure 8.53. The respective percentages of saving gain are shown as a function of the side lengths. It considers the **periodic** traffic profile with a generation rate of $\lambda = 1/2 \text{ s}^{-1}$. It is observable that the use of IR is only efficient for denser scenarios and for sensing values $\Pi_{irmax} \in \{-90; -80; -70\} \text{ dBm}$. For side lengths larger than 100 m, the saving gains are negligible.

Section J.6 from Appendix J also presents the results for the energy saving gains as a function of

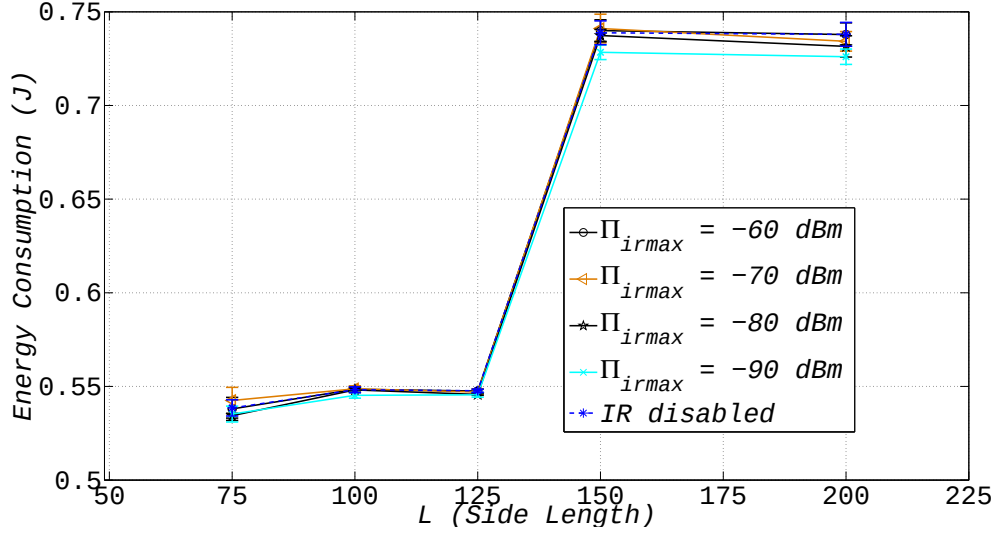


Figure 8.52: Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) when IR enabled or disabled.

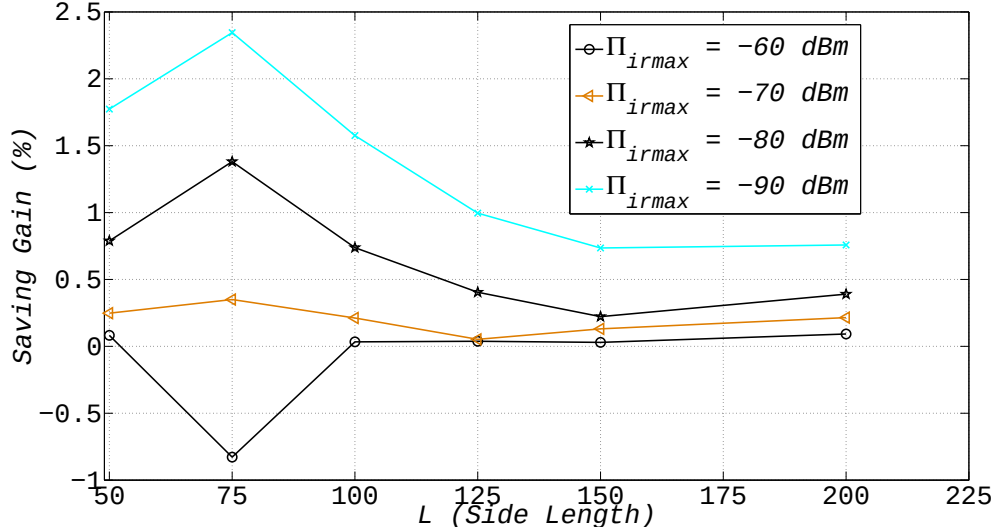


Figure 8.53: Saving gain percentage per node of MC-SCP-MAC as a function of the deployment scenarios side lengths when IR is enabled with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).

the side lengths that can be achieved with the employment of the IR concept whilst considering periodic traffic profile and a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

We can conclude that the employment of IR allows for achieving shorter latency values, higher delivery ratios and considerable energy consumption savings, at the expense of reduced aggregate throughput. Moreover, the denser scenarios allow for MC-SCP-MAC to achieve better overall performance.

8.5.8 Performance Analysis in the Cluster Topology

This set of tests aim to assess the impact of enabling the influential range concept and the dependence on the available number of slot channels for data exchange in the MC-SCP-MAC. Different traffic patterns and data generation rates are considered. We consider a heterogeneous sensor network, where nodes are hierarchically different, and mainly focus on the operation inside a cluster. Since MC-SCP-MAC is more robust and efficient in denser scenarios

(e.g., deployment scenario comprises sensor nodes in a forest or agricultural field), we consider that the performance evaluation in a cluster topology can be useful to extract insights. The main advantages of using heterogeneous sensor networks (i.e., clusters) is twofold:

- it has improved scalability than a flat network without hierarchies;
- the majority of nodes in the network, can be made very simple and inexpensive, which reduces the overall cost of the network.

Asymmetric communications is, however, a special and unique feature in clusters: The message sent by a cluster head can be received directly by all sensors in the cluster, whereas the message sent by a sensor node (Full Function Device (FFD) or Reduced Function Device (RFD)) may have to be relayed by other sensors, by multi-hop connections, to reach the cluster head. In heterogeneous sensor networks, the basic sensors can be randomly deployed as in homogeneous sensor networks. The cluster heads, on the other hand, should be more carefully deployed, to ensure that all basic sensors are covered, i.e., that each sensor node can sense and hear from at least one cluster head. Nevertheless, since the number of cluster heads is small, their best locations can be found within a reasonable amount of time. Besides, the cluster heads can even increase their transmitter power to cover remote sensors. For this set of tests we consider a deployment scenario of $300 \times 300 \text{ m}^2$. Four clusters have been deployed composed by 22 FFD's or RFD's in each cluster, four cluster heads, 4 FFD's and one PAN coordinator, illustrated in Figure 8.54.

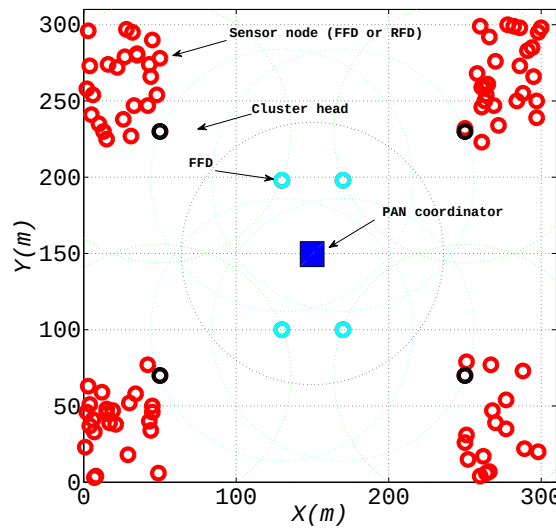


Figure 8.54: Network deployment in the cluster topology.

MC-SCP-MAC considers maximum contention window sizes of $CW_k^{max} = 80$, $k \in \{1, 2\}$. For this set of results we consider for the maximum transmitter power $P_{tx} = 0.8 \text{ mW}$, data packet size $L_{data} = 32 \text{ Bytes}$, a variable number of slot channels $N_{ch} \in \{4; 7; 15\}$ and that each node generates 600 packets. Here, the frame duration is $t_F = 1 \text{ s}$ for all the considered number of slot channels, while the values for the time allocated for each slot channel are $\Delta t_{SC} = 0.0625 \text{ s}$, $\Delta t_{SC} = 0.125 \text{ s}$ and $\Delta t_{SC} = 0.2 \text{ s}$, for $N_{ch} = 4$, $N_{ch} = 7$ and $N_{ch} = 15$, respectively. The objective of these tests is the analysis of the gains achieved when the IR is enabled for different values of $\Pi_{irmax} \in \{-90; -80; -70; -60\} \text{ dBm}$ while varying the number of slot channels, as shown in Figure 8.55 ($\lambda = 1/2 \text{ s}^{-1}$) and Figure 8.56 ($\lambda = 1 \text{ s}^{-1}$).

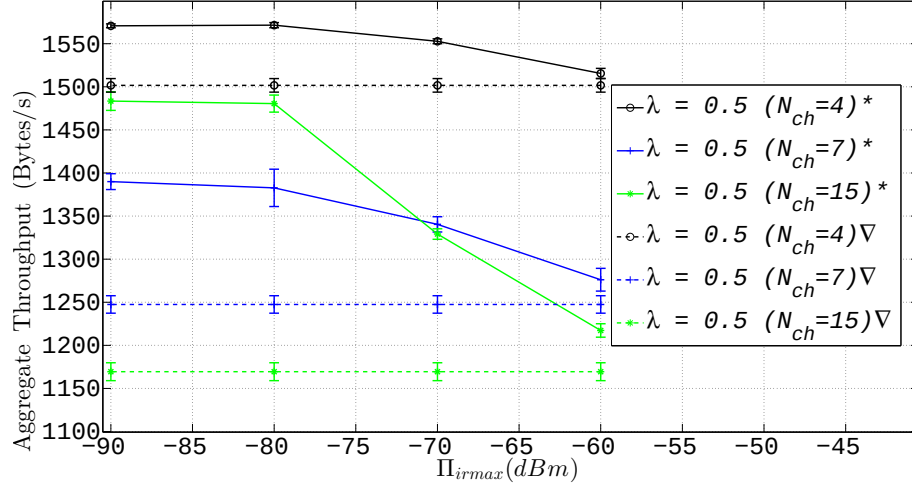


Figure 8.55: Aggregate throughput as a function of Π_{irma_max} for the MC-SCP-MAC protocol when IR enabled (*) or disabled (∇) while varying the number of slot channels, for periodic traffic generation ($\lambda = 1/2$ s⁻¹).

Figure 8.55 shows the aggregate throughput as a function of Π_{irma_max} for MC-SCP when IR is enabled and disabled as the number of slot channels as a parameter for a traffic generation rate $\lambda = 1/2$ s⁻¹ and **periodic** profile. The 95 % confidence intervals are also presented. Here the computation of the aggregate throughput takes into account the dropped packets due to the use of IR. By observing the results it is noticeable that the use of the IR allows to achieve a higher aggregate throughput since there are less packets to be transmitted by the sensor nodes from the nodes in the cluster to the cluster heads. The highest values of aggregate throughput occur when $\Pi_{irma\_max} = -90$ dBm, due to this sensing range that allows to overhear more packets and therefore increase the level of dropped packets. When the IR capability is disabled the achieved aggregated throughput is much lower than in the case the IR is enabled. This is due to the high contention between nodes that have a larger number of packet in queue to be transmitted while trying to win the access to the medium, in order to transmit their packets. As the value of the sensing range, Π_{irma_max} , increases the influential range decreases, which, in turn, causes the aggregate throughput to decrease. As the number of available slot channels increases the aggregate throughput decreases. This is justified by the slot channel duration. As the number of slot channels increases, the slot channel duration decreases, which lead to nodes have less time to dispatch their packets. The case that presents the highest values of aggregate throughput is the one with 4 slot channels but it also presents the highest value of slot channel duration (i.e., 0.2 s). Since it has longer time for each slot channel it can use this time to send more packets during a frame.

Figure 8.56 presents the aggregate throughput as function of the Π_{irma_max} for MC-SCP-MAC when IR is enabled or disabled with the number of slot channels as a parameter for a traffic generation rate of $\lambda = 1$ s⁻¹ and **periodic** profile. The 95 % confidence intervals are also presented. This analysis enables to understand how the MC-SCP-MAC behaves when the data generation rate is increased. As in Figure 8.55, the highest values for the aggregate throughput occur when $\Pi_{irma\_max} = -90$ dBm, due to the increased sensing range (that enables to overhear more packets). When IR is disabled, the achieved aggregated throughput is much lower than when the IR is enabled, as expected. As the value of the sensing range, Π_{irma_max} , increases the influential range decreases, which, in turn, causes the aggregate throughput to decrease. The number of available slot channels also play an important role in the aggregate throughput for higher traffic generation rates since, in Figure 8.56, the highest values of the aggregate throughput

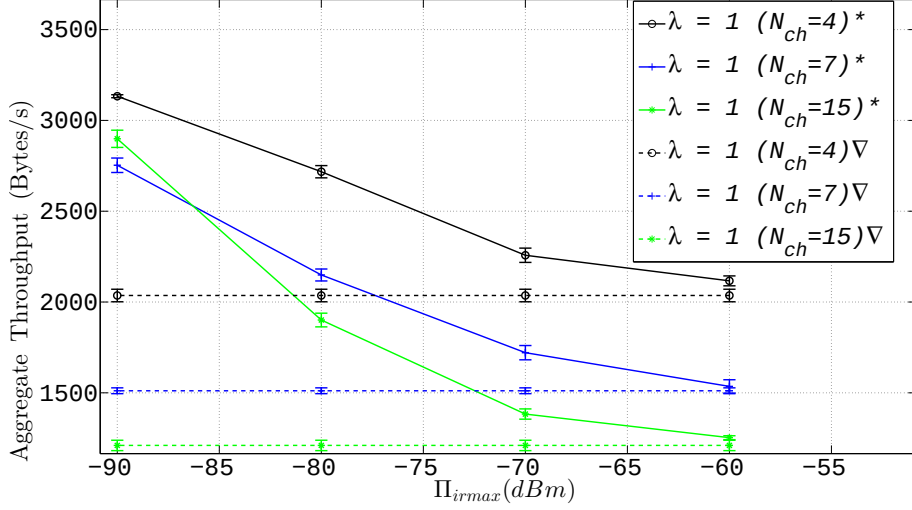


Figure 8.56: Aggregate throughput as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR enabled (*) or disabled (∇) while varying the number of slot channels, for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).

occur when there are 4 slot channels available. From these results, we are able to conclude that MC-SCP-MAC supports higher traffic generation rates in the cluster topology. Section J.5 from Appendix J presents results for the aggregate throughput as a function of Π_{irmax} when IR is disabled, with the number of slot channels as a parameter for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ whilst considering an exponential profile.

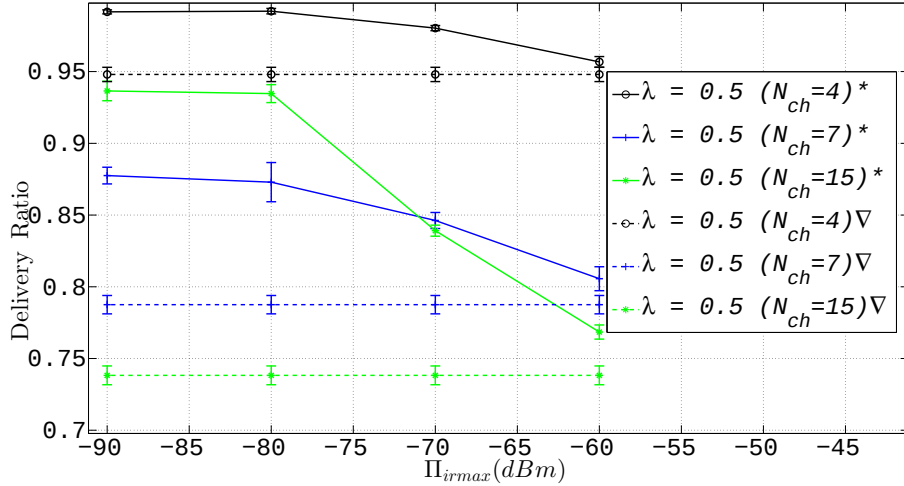


Figure 8.57: Delivery ratio as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).

Figure 8.57 shows the results for the delivery ratio as a function of the sensing range, Π_{irmax} , for the MC-SCP protocol considering the IR feature (enabled or disabled) with the number of slot channels as a parameter for a traffic generation rate $\lambda = 1/2 \text{ s}^{-1}$ and a periodic profile. The 95 % confidence intervals are also presented. When the IR is enabled, the high values for the delivery ratio verified in Figure 8.57 identifies the high aggregate throughput presented in Figure 8.55. The highest values of delivery ratio occur when $\Pi_{irmax} = -90 \text{ dBm}$, since it corresponds to the situation where more redundant data packets are dropped, due to the considered reduced value of IR sensing range, Π_{irmax} . As the value of the sensing range, Π_{irmax} , increases the influential range decreases which, in turn, causes the delivery ratio to decrease. As verified in Figure 8.55, when the number of available slot channels increases,

the aggregate throughput decreases and, therefore, the delivery ratio decreases. Figure 8.58 presents the delivery ratio as a function of the sensing range for the MC-SCP protocol when IR is enabled or disabled, with the number of slot channels as a parameter, for a traffic generation rate $\lambda = 1 \text{ s}^{-1}$ and a periodic profile. Similarly to the conclusions from Figure 8.57, the protocol presents the highest values of delivery ratio for a sensing value of $\Pi_{irmax} = -90 \text{ dBm}$. If the IR is disabled the achieved delivery ratio is much lower than when the IR is enabled, as expected. As the value of the sensing range, Π_{irmax} , increases the delivery ratio decreases and, consequently, the aggregated throughput decreases. The increase of the number of slot channels leads to a decrease of the achievable delivery ratio as the value of the sensing range Π_{irmax} increases (when IR is enabled or disabled).

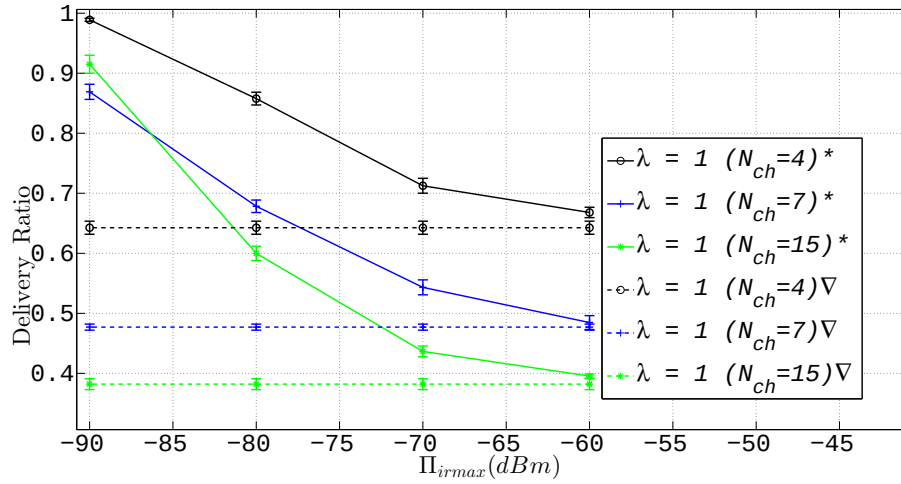


Figure 8.58: Delivery ratio as a function of Π_{irmax} for the MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).

Section J.5 from Appendix J presents the results of the delivery ratio as function of the sensing range, Π_{irmax} , while varying the number of slot channels for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ whilst considering an exponential profile. We intend to evaluate the energy consumption per node of MC-SCP-MAC when IR is enabled or disabled, for different number of slot channels, whilst considering a **periodic** traffic generation profile with $\lambda = 1/2 \text{ s}^{-1}$. Here the computation of the energy consumption does not take into account the energy spent by the PAN coordinator. However, it considers the energy consumed by the cluster heads and FFD nodes, placed between the cluster heads and the PAN coordinator. Since these nodes have to process and forward more packets than the ones located within the cluster, their energy consumption is higher than for the remaining ones inside the cluster. Therefore, the energy consumption presented in the following figures takes into account this difference. By analyzing the results from Figure 8.59 it is noticeable that the use of IR allows for achieving a lower energy consumption per node since there are less packets to be transmitted by the sensor nodes. The lowest values of energy consumption occur when $\Pi_{irmax} = -90 \text{ dBm}$. As the value of the sensing range, Π_{irmax} , increases the energy consumption also increases, up to the value of energy consumption that corresponds to disabled IR. It is worthwhile to note that, in Figure 8.59, the energy consumption presents lower values of energy consumption per node for a reduced number of slot channels. This is justified by the higher values for the delivery ratio from Figure 8.57. For the case of 4 slot channels a slot channel duration of 0.2 s allows for the nodes to transmit more packets in shorter time. Decreasing the active time to transmit all the packets consequently causes the reduction of the energy consumption per node.

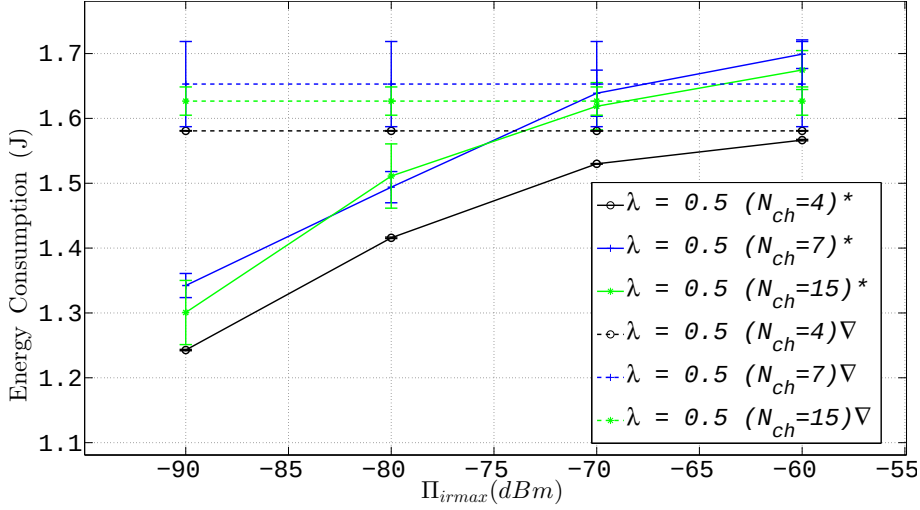


Figure 8.59: Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).

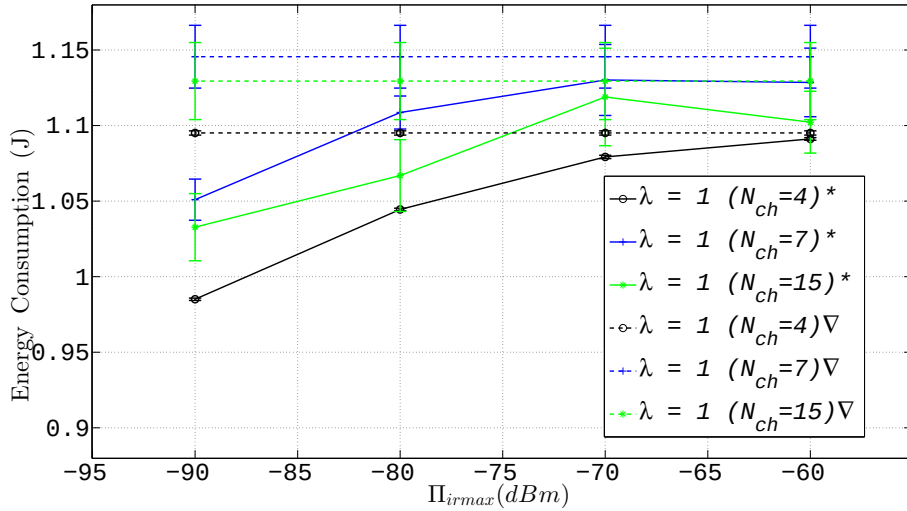


Figure 8.60: Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC protocol when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).

Figure 8.60 presents the results for the energy consumption per node when IR is enabled or disabled, as a function of the number of slot channels for a traffic generation rate of $\lambda = 1 \text{ s}^{-1}$ and **periodic** profile. The 95 % confidence intervals are also presented. Similarly to the conclusions for $\lambda = 1/2 \text{ s}^{-1}$ from Figure 8.59, the lowest values for the energy consumption occur when $\Pi_{irmax} = -90 \text{ dBm}$. As the value of sensing range, Π_{irmax} , increases the energy consumption also increases until it reaches the maximum value for the energy spent per node when the IR is not enabled. In terms of energy consumption, as the number of slot channels increases, similar conclusions relatively to the energy consumption per node from Figure 8.59 can be applied here. Here, the energy consumption also presents lower values of energy consumption per node for a reduced number of slot channels. By comparing Figures 8.59 and 8.60 it is noticeable that increasing the data generation frequency reduces the energy consumption when IR is enabled and disabled. This is due to the quick generation and transmission of the packet from the sensor nodes to the PAN coordinator, which leads to a significant reduction of active time needed to transmit and receive all the packets. This reduction of the active time

causes the decrease of the energy consumption per node. Section J.5 from Appendix J presents the results for the energy consumption per node when IR is disabled as a function of the number of slot channels for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ whilst considering an exponential profile.

It is worthwhile to evaluate the end-to-end latency of MC-SCP-MAC when IR is enabled and disabled, for different values of the number of slot channels, whilst considering a periodic traffic generation profile with $\lambda = 1/2 \text{ s}^{-1}$. The computation of the end-to-end latency considers in average 3 hops until the packet reaches the PAN coordinator. It is expected that the values for the latency when the IR is not enabled are going to be quite high. However, we expect that enabling IR helps to reduce the latency since it will reduce the redundant data packets and therefore avoiding high traffic loads.

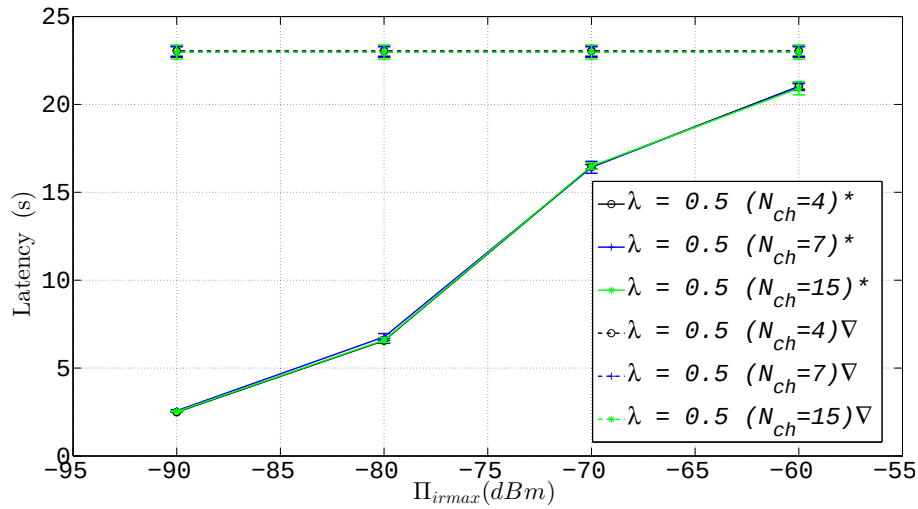


Figure 8.61: Latency for MC-SCP-MAC as a function of Π_{irmax} when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$).

By observing the results from Figure 8.61 it is evident that the use of the IR allows for obtaining a shorter latency since there are less packets in queue (to be transmitted by the sensor nodes). For a value of the sensing range of $\Pi_{irmax} = -90 \text{ dBm}$, the MC-SCP can achieve values for the latency around 2.8 s. It corresponds to a latency of around 0.933 s per hop, almost a frame time duration (per hop). As the values of the sensing range, Π_{irmax} , increases the latency also increases. This increase of the latency is due to the increase of the number of packets waiting in queue to be transmitted. When the IR is disabled, the value of the latency is around 23 s for all the considered number of slot channels. The same holds if the IR is enabled since for all the considered number of slot channels, the latency is similar and increases as the value of the sensing range increases.

Figure 8.62 shows the results for the end-to-end latency as a function of Π_{irmax} when IR is enabled or disabled with the number of slot channels as a parameter for a traffic generation rate $\lambda = 1 \text{ s}^{-1}$ and **periodic** profile. The 95 % confidence intervals are also presented. As in Figure 8.61 the shortest values for the latency are noticeable when the IR is enabled for different values of sensing range, Π_{irmax} . For a value of the sensing range $\Pi_{irmax} = -90 \text{ dBm}$, the MC-SCP achieves values for the latency around 4 s. By comparing these results with the ones obtained for the latency in Figure 8.61, this increase of the latency is due to the increase of the number of packets in the queue that are awaiting to be transmitted. As the value of the sensing range, Π_{irmax} , increases the latency also increases. When the IR is disabled, for all the considered values for the number of slot channels, the latency is around the 24 s. The same

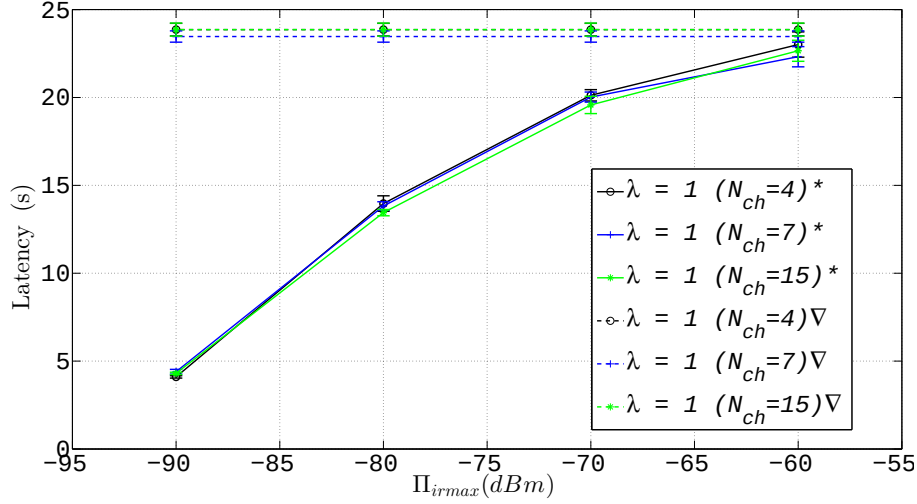


Figure 8.62: Latency for MC-SCP-MAC as a function of Π_{irmax} when IR is enabled (*) and disabled (∇) while varying the number of slot channels for periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$).

holds if the IR is enabled since for all the considered number of slot channels, the latency is similar and increases as the value of the sensing range increases. In Section J.5 from Appendix J, results are presented for the end-to-end latency as a function of the Π_{irmax} when IR is disabled, with the number of slot channels as a parameter for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ whilst considering an **exponential** traffic profile.

8.5.9 Performance Analysis in a Linear Chain Topology

The objective from this section is to compare the network performance metrics between the MC-SCP-MAC and SCP-MAC protocols in the linear chain topology from Figure 8.17. We analyze the end-to-end latency and delivery ratio of the MC-SCP-MAC protocol, while varying the number of slot channels and considering different durations for the slot channels and the frame. For this set of tests, the MC-SCP-MAC considers **periodic** and **exponential** traffic generation profile with $\lambda \in [1; 1/2] \text{ s}^{-1}$. In turn, for the SCP-MAC we only consider periodic traffic, with $\lambda = 1 \text{ s}^{-1}$. The 95 % confidence intervals are also presented in the following figures. The MC-SCP-MAC and SCP-MAC protocol consider maximum contention window sizes of $CW_k^{max} = 32$, $k \in \{1, 2\}$. For this set of results, we consider a maximum transmitter power for both MAC protocols of $P_{tx} = 1 \text{ mW}$ and data packet size $L_{data} = 50 \text{ Bytes}$. The SCP-MAC considers a frame duration of 1 s while the polling period $T_{poll} \in \{0.15; 1\} \text{ s}$. In these tests we consider for the MC-SCP-MAC different number of slot channels. The case of $N_{ch} = 3$ slot channels considers a slot channel duration of $\Delta t_{SC} = 0.25 \text{ s}$, $N_{ch} = 7$ slot channels considers a slot channel of $\Delta t_{SC} = 0.125 \text{ s}$ and for the case of $N_{ch} = 15$ slot channels is considered a slot channel duration of $\Delta t_{SC} = 0.0625 \text{ s}$. For all these slot channels configurations the frame is $t_F = 1 \text{ s}$. The remaining three configurations are the following ones:

- the first considers $N_{ch} = 4$ slot channels with a slot channel duration $\Delta t_{SC} = 0.17 \text{ s}$ and a frame duration $t_F = 0.85 \text{ s}$, and is identified in the graphs with the symbol (*);
- the second also considers $N_{ch} = 4$ slot channels with a slot channel duration $\Delta t_{SC} = 0.2 \text{ s}$ and a frame duration $t_F = 1 \text{ s}$;
- the third one considers $N_{ch} = 8$ slot channels, with a slot channel duration $\Delta t_{SC} = 0.17 \text{ s}$ and a frame duration $t_F = 1.53 \text{ s}$.

The SCP-MAC protocol comprises a single-channel for data. The deployment scenario for the MC-SCP-MAC comprises 10 sensor nodes and one PAN coordinator i.e., it considers 10-hops. The node located at the opposite edge of the PAN coordinator in the linear chain (node number 1) generates 600 packets. The remaining nodes have to forward the packets as quickly as possible, until they reach the PAN coordinator. Note however that, for the SCP-MAC protocol, the tests were performed with only 9-hops. Figure 8.63 presents the end-to-end latency for

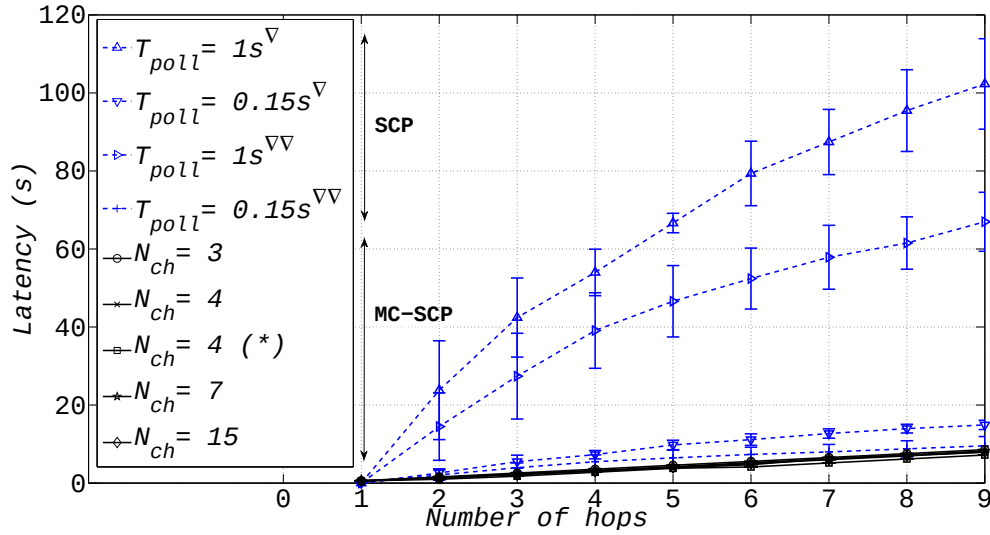


Figure 8.63: Latency as a function of the number of hops for the MC-SCP-MAC and SCP-MAC protocols, with ACK enabled (∇) or disabled ($\nabla\nabla$) with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in the linear chain topology, for the MC-SCP-MAC and with T_{poll} as a parameter for the SCP-MAC with the number of slot channels as a parameter.

the MC-SCP-MAC and SCP-MAC protocols with the number of hops in the linear chain as a parameter whilst considering a periodic traffic profile with a generation rate $\lambda = 1 \text{ s}^{-1}$. As the number of hops in the linear chain increases the latency of the packet increases. However, for the SCP-MAC protocol, the latency for all the presented values for T_{poll} (with and with no acknowledgements) is always larger than the values for the latency in MC-SCP-MAC. The use of the enhanced two-phase contention window mechanism along with multiple channels allows for the MC-SCP-MAC to transmit more packets concurrently in different slot channels, with no interference. Consequently the delivery ratio increases and the latency decreases.

Figure 8.64 presents the curves for the end-to-end latency of MC-SCP-MAC as a function of the number of hops in the linear chain. Periodic traffic with a generation rate $\lambda = 1 \text{ s}^{-1}$ is considered. In Figure 8.64 as the number of hops increases, the latency also increases, as expected. The longest values for the latency correspond to the case in which the number of slot channels is $N_{ch} = 3$ for all the number hops. The shortest values for the latency are verified when $N_{ch} = 4$ slot channels but with a frame duration $t_F = 0.85 \text{ s}$. For the frame duration $t_F = 1 \text{ s}$, the increase of the number of slot channels does not have a significant impact in the variation of the latency with the number of hops. We can conclude that, with a frame duration shorter than the traffic generation interval, the MC-SCP-MAC achieves a lower latency, since it can transmit the packets stored in the queue quicker. In average, the MC-SCP-MAC presents a mean latency per hop of 0.9 s . This value is shorter than the frame duration, in some cases. This is possible due to the deterministic choice of the slot channel given by the LCG generator, being able to dispatch the packets quicker or slower than the frame duration. Figure 8.65 presents the end-to-end latency of MC-SCP-MAC as the number of hops in the linear chain increases whilst considering a periodic traffic profile with a generation rate $\lambda = 1/2 \text{ s}^{-1}$. In Figure 8.65 as

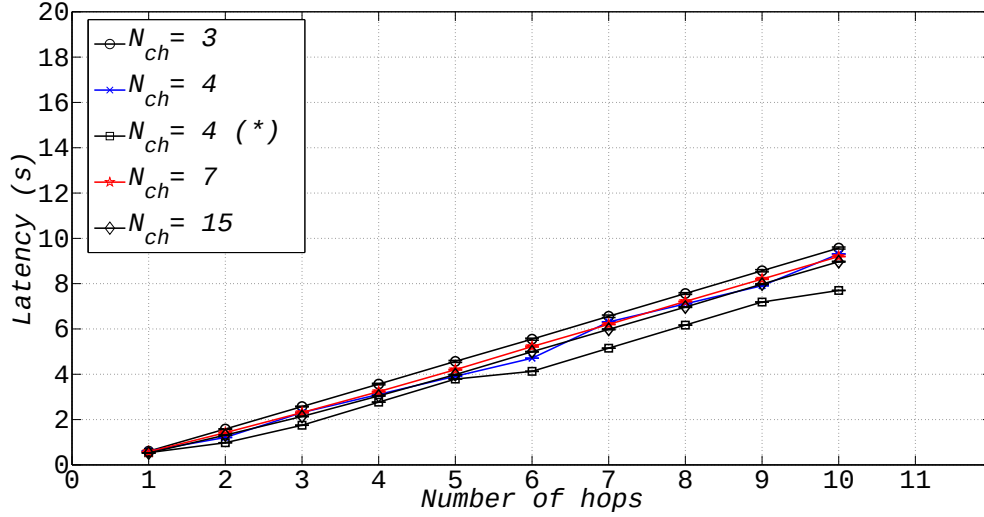


Figure 8.64: Latency of MC-SCP-MAC with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in linear chain topology for different number of slot channels.

the number of hops increases, the latency also increases, as expected. The longest values for the latency correspond to the case in which the number of slot channels is $N_{ch} = 8$ for all the number hops. This is justified by the value of the frame duration of $t_F = 1.53 \text{ s}$ that make the nodes to take more time to initiate the next transmission to forward the data packets. In turn, the case in which the values for the latency are shorter corresponds to $N_{ch} = 4$ slot channels but with a frame duration of $t_F = 0.85 \text{ s}$. If the frame duration is $t_F = 1 \text{ s}$, the increase of the number of slot channels does not have a significant impact in the variation of the latency with the number of hops. By comparing these results with the ones from Figure 8.64, we can conclude that the increase of the traffic generation interval frequency leads to an increase of the latency, as expected.

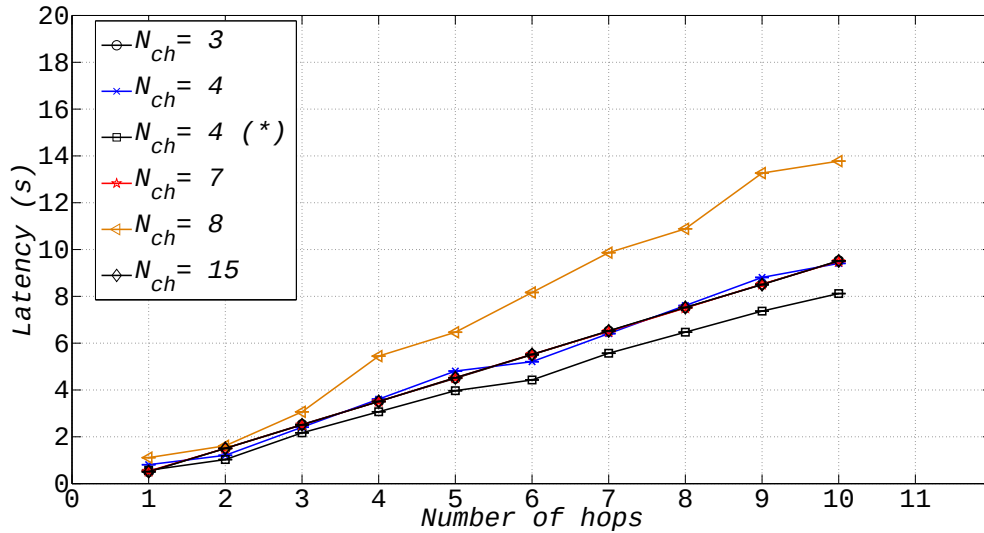


Figure 8.65: Latency as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.

Figure 8.66 presents the end-to-end latency of MC-SCP-MAC as a function of the number of hops in the linear chain topology whilst considering an **exponential** traffic profile with a generation rate $\lambda = 1/2 \text{ s}^{-1}$. As in Figure 8.65, the longest values for the latency correspond to the case in which the number of slot channels is $N_{ch} = 8$ for all the number hops. In turn, the case in which

the values for the latency are shorter correspond to the case $N_{ch}=4$ slot channels but with a frame duration of $t_F = 0.85$ s (as the number hops increases). By comparing these results with the ones from Figure 8.65, the values for the latency are similar for all the considered number of slot channels.

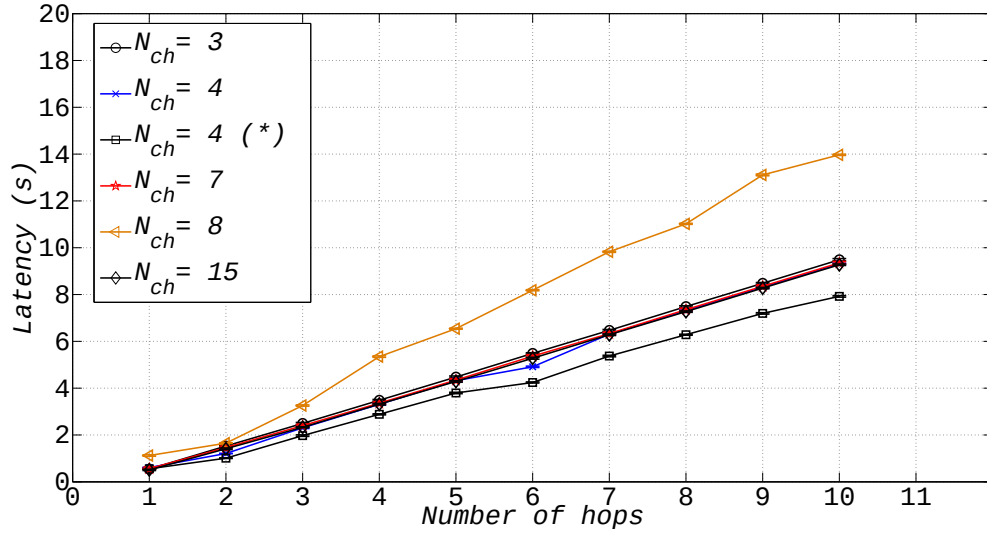


Figure 8.66: Latency as a function of the number of hops for MC-SCP-MAC protocol with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.

The objective of this part of the work consists in evaluating the delivery ratio of MC-SCP-MAC protocol as the number of hops in the linear chain increases, whilst considering a **periodic** traffic profile with a generation rate $\lambda = 1 \text{ s}^{-1}$. From the results presented in Figure 8.67 it is observable that the MC-SCP-MAC achieves the maximum value of delivery ratio when the number of slot channels is $N_{ch}=4$ for the cases $t_F = 0.85$ s and $t_F = 1$ s. For other values of the number of slot channels, as the number of hops increases the delivery ratio decreases. The case $N_{ch}=3$ slot channels corresponds to the lowest values of the delivery ratio in the linear chain (as the number of hops increases). For $N_{ch}=3$ slot channels, the low values for the delivery ratio are consistent with the long values for the latency presented in Figure 8.64.

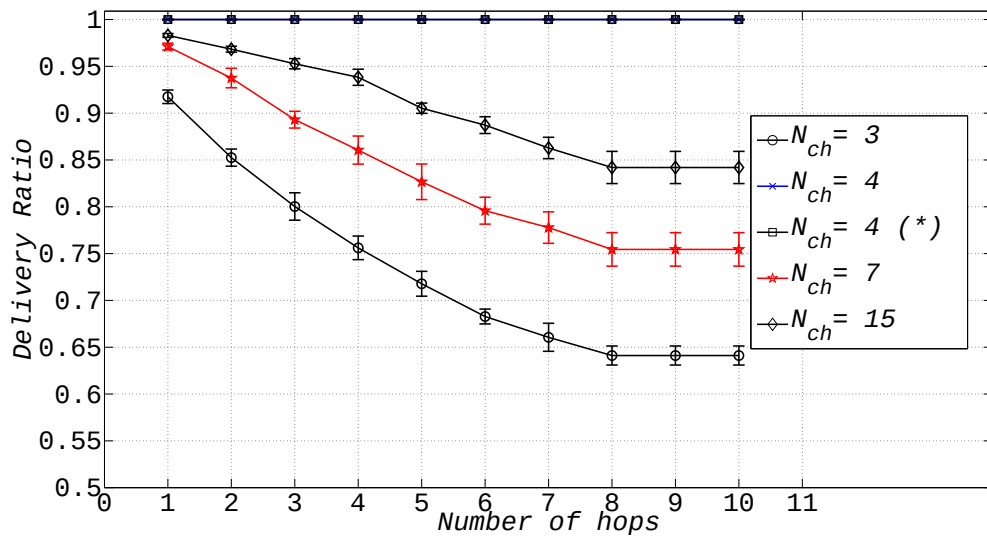


Figure 8.67: Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.

Figure 8.68 presents the delivery ratio for the MC-SCP-MAC protocol with the number of hops in the linear chain as a parameter, whilst considering a **periodic** traffic profile with a generation rate $\lambda = 1/2 \text{ s}^{-1}$. It is noticeable that the MC-SCP-MAC achieves the maximum value of delivery ratio when the number of slot channels is $N_{ch} \in \{4; 8\}$, for the cases $t_F = 0.85 \text{ s}$ and $t_F = 1 \text{ s}$. For the other values of the number of slot channels as the number of hops increases the delivery ratio decreases. The case $N_{ch} = 3$ slot channels corresponds to the lowest values of delivery ratio in the linear chain. By comparing these results with the ones from Figure 8.67, the delivery ratio for the **periodic** traffic generation with $\lambda = 1/2 \text{ s}^{-1}$ is lower than in the case with a traffic generation rate $\lambda = 1/2 \text{ s}^{-1}$.

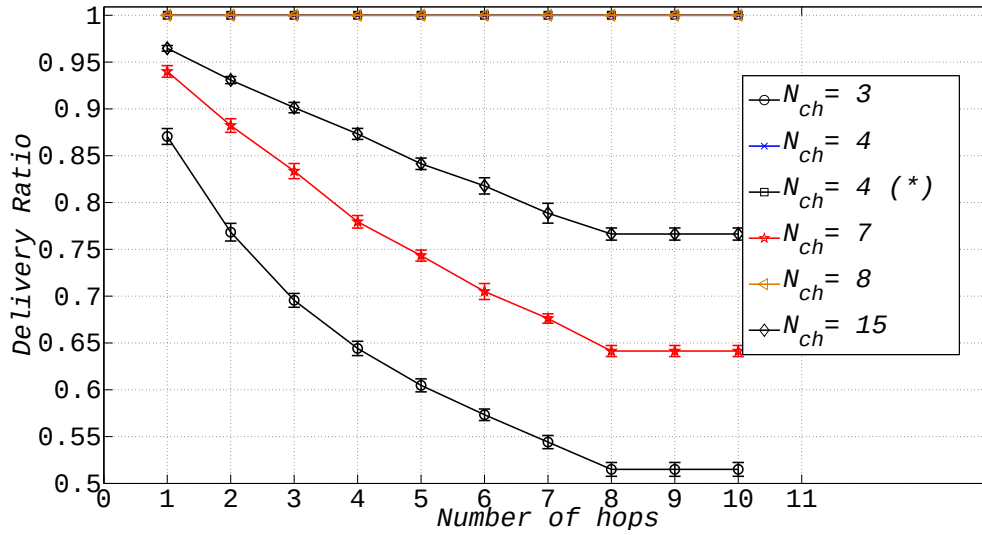


Figure 8.68: Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with periodic traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.

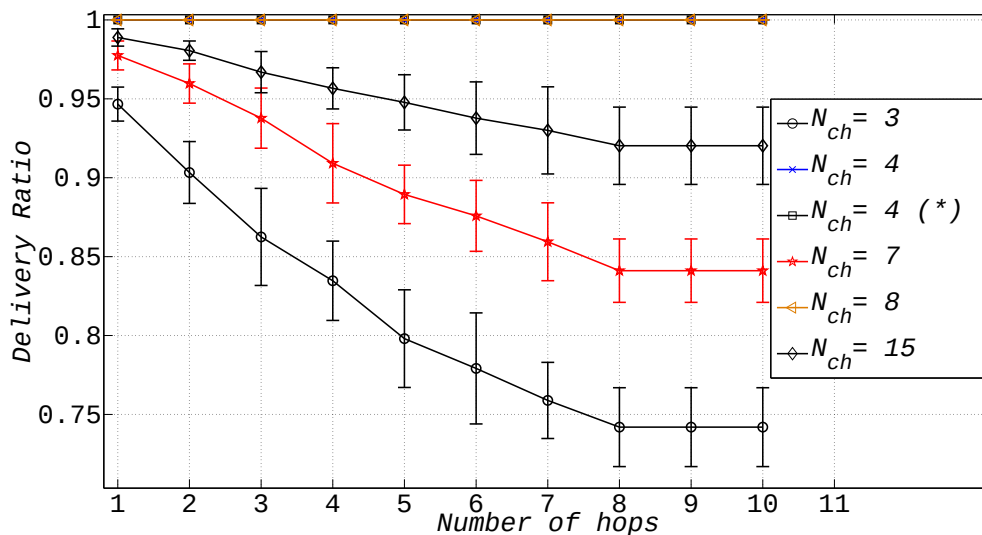


Figure 8.69: Delivery ratio as a function of the number of hops for MC-SCP-MAC protocol with exponential traffic generation ($\lambda = 1/2 \text{ s}^{-1}$) in the linear chain topology, with the number of slot channels as a parameter.

Figure 8.69 depicts the delivery ratio as a function of the number of hops for the MC-SCP-MAC protocol whilst considering an **exponential** traffic profile with a generation rate $\lambda = 1/2 \text{ s}^{-1}$. The delivery ratio achieves the maximum values when the number of slot channels is

$N_{ch} \in \{4; 8\}$ for the cases $t_F = 0.85$ s and $t_F = 1$ s, respectively. The case of $N_{ch} = 3$ slot channels corresponds to lowest values of delivery ratio. By comparing these results with the ones from Figure 8.68, the delivery ratio for the **exponential** traffic generation is higher than for the **periodic** traffic profile.

8.5.10 Fairness Index Evaluation for the Throughput

In this section we evaluate the throughput fairness index of the MC-SCP-MAC protocol for different network sizes and number of slot channels. The throughput fairness index follows the following definition [JDB99]:

$$\vartheta_{fi} = \frac{(\sum_{i=1}^n x_i)^2}{(n \sum_{i=1}^n (x_i)^2)} \quad (8.13)$$

where x_i represents the throughput of the node i . The closer the fairness index is to one, the fairer the system is. Fairness problems usually result from location dependent contention which is very common in multi-hop networks. The fairness problem is especially conspicuous when very few nodes are competing in a region. However, when n is larger, the fairness problem is less severe, as it is much more difficult for a node to win exclusive access to the shared channel from all the other competing nodes at the same time.

The fairness problems appear in MAC protocols that give more opportunities to win the shared medium to some nodes. One of cases is the BEB protocol. In slotted contention based protocols, like MC-SCP-MAC, if the system is not fair enough, a solution to provide better fairness is the increase of the maximum contention window size value when successful transmission happens. It causes an increase in fairness because it gives opportunities to others that cannot get access to the channel. This way provides fairness improvement.

Table 8.4: Correspondence between N_{ch} and Δt_{SC} for the throughput fairness index for the MC-SCP-MAC protocol.

t_F [s]	N_{ch}	Δt_{SC} [s]
1	3	0.25
	7	0.125
	9	0.1
	15	0.0625
1.53	8	0.17

In this simulation tests, we consider 10, 30 and 99 contending nodes and vary the simulation duration, in order to observe the short and long term fairness.

As the simulation duration gets longer, the fairness index indicates the long term fairness. Note that the duration is not the program running time, rather the time considered for the simulation. We consider a deployment scenario of 50×50 m², in which the transmitter power $P_{tx} = 0.8$ mW, the IR is disabled. It is considered a periodic traffic generation profile with $\lambda = 1/2$ s⁻¹. Each node can transmit a maximum of 3000 packets. However, depending on the simulation time considered, the node can transmit more or less packets. For each network size we consider four simulation scenarios: a) scenario A considers $t_{simulation} = 100$ s (short-term fairness); b) scenario B considers $t_{simulation} = 400$ s; c) scenario C considers $t_{simulation} = 1000$ s and d) scenario D considers $t_{simulation} = 3000$ s (long-term fairness). The throughput fairness index is evaluated

considering different number of slot channels. We consider the correspondence between N_{ch} and Δt_{SC} from Table 8.4.

Figure 8.70 shows the solution of the throughput fairness index of MC-SCP-MAC with the simulation duration for $n = 10$. We averaged 6 simulation runs, with different seeds for each point. The simulation results show that, for a low number of nodes, the short and long-term fairness index stays high for all the considered number of slot channels. Here, all nodes access the medium with the same probability.

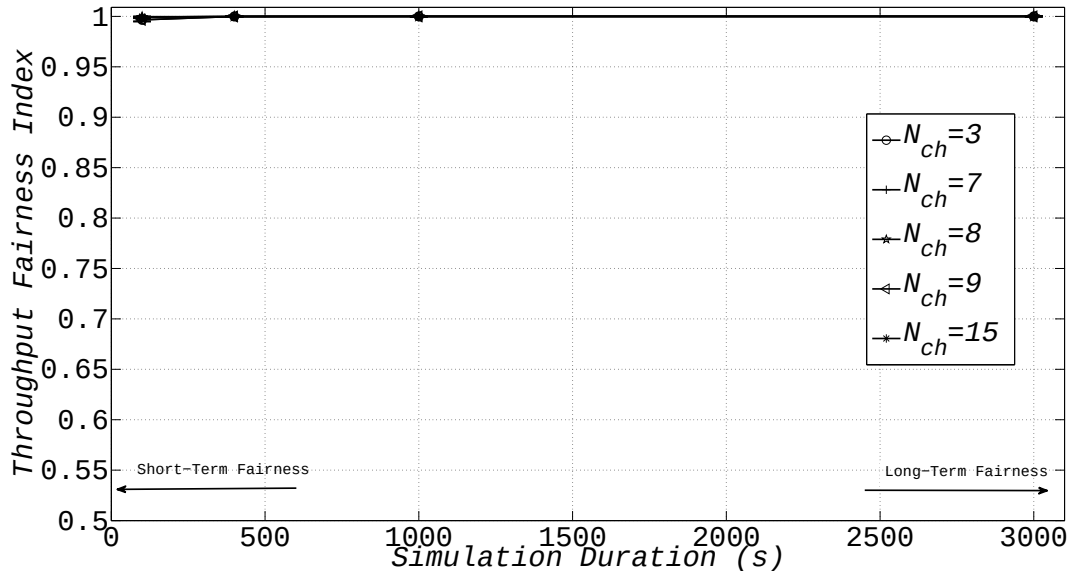


Figure 8.70: Throughput fairness index of MC-SCP-MAC for $n = 10$.

Figure 8.71 depicts the simulation results of the throughput fairness index for the MC-SCP-MAC for $n = 30$. The results shows that the increase of the number of slot channels improves the short-term fairness of MC-SCP-MAC. However, the long-term fairness stays high for all the considered number of slot channels.

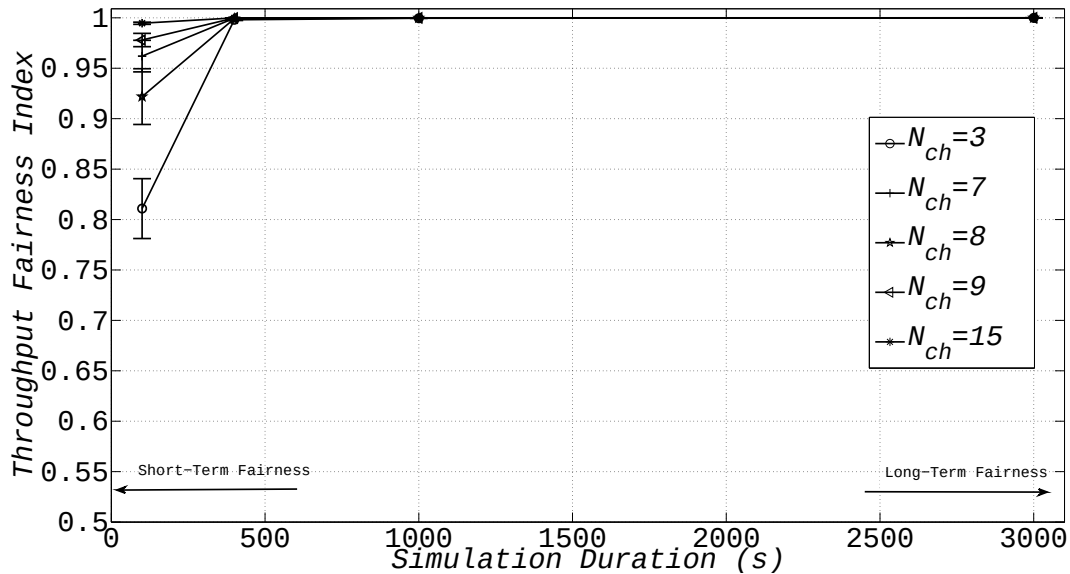


Figure 8.71: Throughput fairness index of MC-SCP-MAC for $n = 30$.

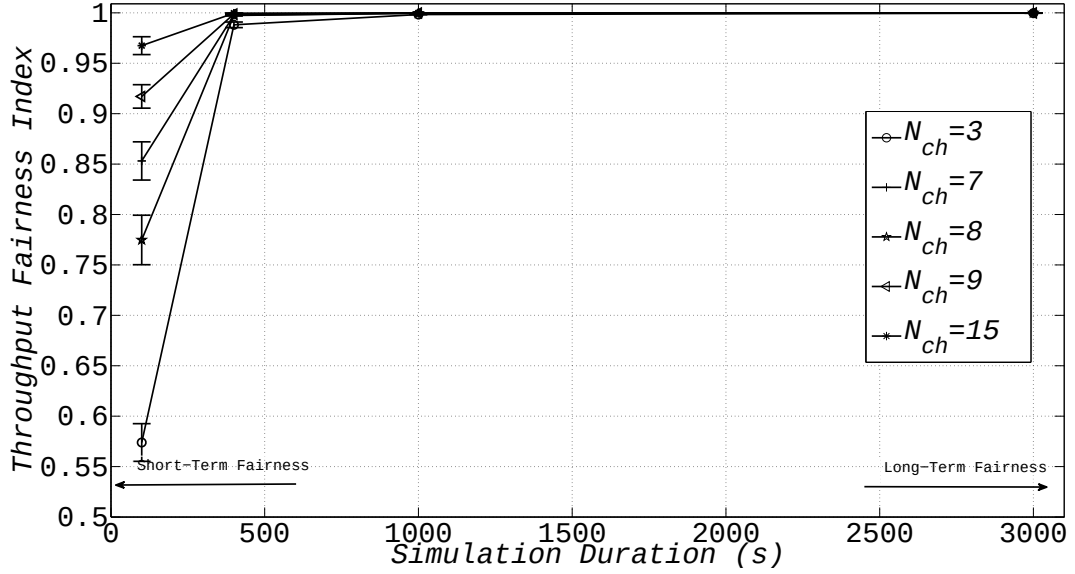


Figure 8.72: Throughput fairness index of MC-SCP-MAC for $n=99$.

Figure 8.72 shows the results of the throughput fairness index for $n=99$ nodes. This scenario considers a dense deployment scenario. The obtained results show that, as the number of slot channels increases, the short-term fairness improves. By comparing these results with the ones for $n=30$, the highest network sizes lead to a less fair behaviour for the short-term fairness among the nodes. The throughput fairness index is high for the long-term fairness index for all the network sizes.

8.6 Enhancements to be implemented in MC-SCP-MAC

In order to evaluate different performance metrics after performing all sort of tests with MC-SCP-MAC, some enhancements can be proposed and implemented in order to achieve better results.

The FFDs nodes possess two wake-up states. One wake-up state aims to sense the medium for any node that wants to send a data packet to the node. The other wake-up state is the one in which the node wakes-up to send the data packets stored in queue to its parent node (it can be the PAN coordinator or other FFD node).

To achieve better results in terms of latency, a solution is to suppress the first wake-up state from the RFDs nodes when, after some attempts, the node verifies that no neighbouring node wants to send packets to it. For example, by establishing a limit of 20 wake-ups without any packet reception in the first wake-up state, the disabling of this wake-up state can be triggered. As so, only one wake-up state can be used to switch to the same slot channel of its parent node, in order to send data packets to it. Other solution that aims to decrease the latency time is to decrease the frame size. However, decreasing the frame size may cause the decrease of the delivery ratio (to the sink). A fair tradeoff between the frame size, delivery ratio and latency needs therefore to be envisaged. It must not impair network performance or jeopardize network integrity.

Other improvement that can be proposed to the MC-SCP-MAC protocol is the inclusion of a second wake-up state to FFDs nodes that have the PAN coordinator as its parent node. In the current version of the MC-SCP-MAC, the nodes that have direct connection with the PAN only consider one wake-up state in which they perform the sensing of the channel for incoming data

packets (when the queue is empty) from neighbouring nodes, and transmit data packets to the PAN coordinator when the node has packets in queue to be transmitted. Since these border nodes consider only one wake-up state, in denser deployments this may limit the throughput performance and lead to the increase of the latency.

A solution to mitigate this limitation is the addition of a second wake-up state. Until now, these 1-hop nodes consider that the slot channel in which they wake-up and switch is given by their Linear Congruential Generator (LCG). The slot channel choice given by the LCG is used to wake-up and sense the medium, or to wake-up and send data packet to the PAN. The addition of a second wake-up state imposes special attention in the choice of the slot channel by these 1-hop nodes (to send the data packets to the PAN). Since the PAN coordinator is continuously hopping the slot channels, after a certain duration of time, the best solution for the slot channel choice of the 1-hop nodes (for the new wake-up state) is the addition of one unit to the slot channel choice, given by their LCG. If the LCG slot channel choice corresponds to the last slot channel available, the slot channel choice for the second wake-up state is the first lowest slot channel available for data packets transmission. The addition of this second wake-up state can significantly increase the delivery ratio and aggregate throughput, as well as decreasing the latency, due to the higher delivery ratio.

8.7 Summary and Conclusions

This Chapter addressed the proposal of the Multi-Channel-Scheduled Channel Polling (MC-SCP-MAC) protocol, a new MAC protocol based on the SCP-MAC protocol that envisages multi-channel features. The new protocol states, namely startup, synchronization, slot channel choice, discovery and addition to the network and medium access algorithm, packets structure, energy optimization techniques are described, as well as the transition from one state to the other. These techniques comprise the influential range concept, the proposal of the denial channel list technique which considers the degradation metric of each slot channel and other cognitive-based capabilities. In addition, the study of the capture effect in this new protocol is covered, as well as the extra resolution phase algorithm useful to mitigate packet losses. To better understand the development and implementation of the protocol a state transition diagram is proposed and described for MC-SCP-MAC, jointly with the associated table of the events and transitions between states.

The MC-SCP-MAC performance has been extensively investigated. For the first set of tests, the goal has been to evaluate the collision probability of MC-SCP-MAC and compare the results with the ones from SCP. It is observable that the curves for the MC-SCP-MAC protocol achieve much lower values for the CW_1 and CW_2 collision probabilities (in both regimes) for the MC-SCP-MAC are much lower than SCP-MAC. The improvement is due to the use of multi-channel jointly with an enhanced two-phase contention window mechanism to cope with the possible data packet collisions in MC-SCP-MAC. It causes an increase of the overall network performance at the expense of a small increase in the of complexity of the protocol algorithm.

In almost all the tests performed throughout this thesis the simulation results consider mostly the CC2420 radio transceiver. However, one set of experiments addresses the comparison between the energy consumption per packet (successfully delivered) between MC-SCP-MAC and SCP-MAC, for the CC2420 and AT86RF231 transceivers. With the AT86RF231 transceiver the MC-SCP-MAC protocol presents the lowest values for the energy spent per delivered packet, in comparison with the single-channel SCP-MAC protocol. The lowest values for the energy spent

per delivered packet are justified by the very high delivery rate, owing to the use of multiple channels, combined with the ultra-low power consumption features from the AT86RF231 transceiver (with low energy consumption, shorter duration to perform CS, shorter duration to perform channel switching). The same holds for the CC2420 transceiver, in which the MC-SCP-MAC protocol also presents lower values for the energy spent per delivered packet. Since MC-SCP-MAC is a multi-channel based protocol, we have shown how the collision probability varies with the number of slot channels, $N_{ch} \in \{3; 4; 7; 9; 15\}$. Here, SCP considers a single-channel for data ($N_{ch} = 1$). The network size considered in these tests is $n = 99$ nodes plus 1 PAN coordinator. The increase of the number of slot channels allows for nodes selecting different slot channels. Therefore, it decreases the probability of a node choosing the same slot channel to transmit their data packets.

The difference of the CW_1 collision probability between the MC-SCP and SCP protocols is more noticeable in the unsaturated regime. The curves for the CW_2 collision probability for the MC-SCP-MAC protocol decreases as the number of slot channels increases. In comparison with the SCP protocol, the CW_2 collision probability of the MC-SCP-MAC protocol is always lower. This is due to the low values of CW_1 collision probability that result from the multi-channel features, and lead to a low number of expected number of nodes that pass from CW_1 to CW_2 . There are two main conclusions arising from these tests: the number of slot channels increases along with the proposed enhanced two-phase contention window mechanism, allowing for achieving a much lower collision probability of the data packets.

The difference of the effective collision probability between the MC-SCP and SCP protocols is more notorious in the saturated case. Other tests have been performed to evaluate the energy efficiency with multiple slot channels and contention window sizes. The comparison of the energy efficiency is performed for the MC-LMAC and MC-SCP-MAC whilst considering equal deployment area and transmitter power.

This Chapter, also analyzes the adaptation of the IR concept to a multi-channel based protocol along with the impact in terms of energy performance of enabling of the IR concept in the MC-SCP-MAC. The objective of these tests is to analyze of the gains achieved when the IR concept is enabled, for different values of sensing range, $\Pi_{irmax} \in \{-90; -80; -70; -60\}$ dBm. By enabling the IR, the node that overhears a data packet and verifies that it has redundant data stored in the queue to send to the sink, it discards these redundant packets. The adapted IR concept implies improvements, providing significant reduction of the redundancy of data packets and, consequently, the reduction of the energy consumption per node. As the value of Π_{irmax} increases the influential range of each node decreases which leads to a decrease of the overhearing and the consequent diminishing in the dropping of redundant data packets.

An additional performance metric has also been defined: the energy consumption saving. This metric translates the energy that a node can save when applying the IR concept (for different values of Π_{irmax}). The energy consumption saving is larger if the nodes have to send 600 packets to the PAN (long-term evaluation), compared with the case when nodes have to send 50 packets (short-term evaluation). Moreover, larger network sizes present the largest energy consumption savings when $\Pi_{irmax} = -90$ dBm. For 99 nodes, there is a gain of 21.42 % while for 50 and 20 nodes the gain is 11.70 % and 7.07 %, respectively. These savings decrease as the value of Π_{irmax} increases. This is due to the reduction of the influential range area which, in turn, reduces the overhearing of data packets by the node (as there is a decrease of the level of data packet redundancy), leading to the increase of the energy consumption per node, i.e., there is a reduction of the energy consumption savings.

Additional tests have been conducted with variable number of slot channels to assess the ben-

efits gained from the use of the IR concept in a multi-channel MAC protocol. We conclude that if the number of slot channels used by the MC-SCP-MAC increases the energy consumption also increases. However, the employment of IR allows for reducing the energy consumption for low values of Π_{irmax} . As the value of sensing range, Π_{irmax} , increases the number of redundant packets increases. Therefore, more packets are going to be exchanged, leading to an increase of the energy consumption. The energy savings decrease as the value of the sensing range, Π_{irmax} , increases. In turn, these gains are higher as the number of available slot channels increases.

In WSNs, the most usual traffic pattern is the periodic one. In all the tests performed throughout the thesis, the periodic traffic pattern is always considered in the simulations. However, the impact of different traffic patterns in the MC-SCP-MAC performance is also addressed. MC-SCP-MAC supports longer traffic generation intervals than other multi-channel based MAC protocols (e.g., MC-LMAC). The results for sparser scenarios have shown that the aggregate throughput does not attain a desirable value. However, tests have been conducted considering a denser scenario for $\lambda = 1 \text{ s}^{-1}$ (under periodic and exponential traffic generation). An aggregate throughput was achieved close to the maximum. With these results we can conclude that the MC-SCP protocol presents a better performance in high density scenarios but the presence of hidden terminals may lead to a degradation of the aggregate throughput as the number of source nodes increases. A method that enables to decrease the impact of the hidden terminals problem is therefore imperative.

Another conclusion is that the increase of the traffic generation frequency is well supported by the MC-SCP-MAC in the scenarios that do not present the hidden terminals problem. In terms of latency, as the number of source nodes increases the values of the latency increase. However, in scenarios with larger density of nodes the values for the latency are longer than in scenarios with sparser nodes density. Since MC-SCP-MAC is more robust and efficient in denser scenarios (and the envisaged scenario for this protocol is a deployment of sensor nodes in a forest or an agricultural field), we have considered that the performance evaluation in a cluster topology is useful to extract insights for further improvements in the protocol. The objective has been to assess the impact of the IR concept enabling and the number of slot channels available for data exchange in MC-SCP-MAC, whilst considering different traffic patterns and data generation rates. In the cluster topology, the increase of the number of slot channels leads to a decrease of the aggregate throughput when the IR is disabled. This is due to the high contention between nodes that have a higher number of packets in queue to be transmitted and are trying to win the medium in order to transmit their packets. Enabling the IR concept allows for achieving the highest values of aggregate throughput when $\Pi_{irmax} \in \{-90; -80\}$ dBm. Higher values for the the sensing range, Π_{irmax} , allows for nodes to overhear higher number of packets and therefore increasing the number of discarded packets. Energy consumption per node increases as the number of slot channels increases, whereas the enabling of the IR concept allows for achieving lower values of energy consumption per node. As the sensing range, Π_{irmax} , increases the energy consumption also increases (up to the value of the energy consumption corresponding to the case when the IR is not enabled). The use of the IR allows for obtaining shorter latency, since there are less packets to be transmitted by the sensor nodes in the queue. For a sensing range values of $\Pi_{irmax} = -90$ dBm, the MC-SCP achieves values for the latency around 2.8 s. It corresponds to a latency around 0.933 s per hop, almost a frame time duration per hop. As the value for the sensing range, Π_{irmax} , increases, the latency also increases. This increase for the latency is due to increase of the number of packets waiting in queue to be transmitted. If the IR feature is disabled, the latency value is around 23 s for all the considered number of

slot channels. The same holds for the case when the IR is enabled since for all the considered number of slot channels, the latency is similar and increases as the value of the sensing range increases.

In order to test the scalability of the MC-SCP-MAC protocol, we have varied the density of nodes in a homogeneous network. The deployment scenario has been varied between $50 \times 50 \text{ m}^2$ and $200 \times 200 \text{ m}^2$. The objective of these tests has been to analyze the gains achieved when the IR is enabled for different values of $\Pi_{irmax} \in \{-90; -80; -70; -60\} \text{ dBm}$. Interesting results are presented for the performance metrics such as, the aggregate throughput, delivery ratio, latency, energy consumption and energy consumption savings when the MC-SCP-MAC is deployed in scenarios with side lengths larger than 125 m while varying the values for the sensing range, Π_{irmax} . As the MC-SCP-MAC protocol is based on the SCP-MAC protocol a performance analysis of MC-SCP-MAC in a linear chain topology is also presented in Section 8.3.6. The end-to-end latency and delivery ratio of the MC-SCP-MAC protocol has been analyzed, while varying the number of slot channels and considering different durations for the slot channels and frame. It is observable that as the number of hops in the linear chain increases, the packet latency also increases. However, for the SCP protocol for all the presented values of T_{poll} , with and without acknowledgements, the values for the latency are always longer than the ones of MC-SCP-MAC. The use of the enhanced two-phase contention window mechanism along with the multiple channels allows for the MC-SCP-MAC to transmit more packets concurrently in different slot channels with no interference. Consequently the delivery ratio increases and the latency decreases.

The shortest values of the latency are verified for the case of $N_{ch} = 4$ slot channels but with a frame duration $t_F = 0.85 \text{ s}$. For a frame duration $t_F = 1 \text{ s}$, the increase of the number of slot channels does not have higher impact in the values of the latency. We can conclude that, with a frame duration shorter than the traffic generation interval, the MC-SCP-MAC can achieve lower latency, since it can transmit quicker the packets stored in the queue. In average, the MC-SCP-MAC presents a mean latency per hop of 0.9 s. This value is shorter than the frame duration, in some cases. This is possible due to the deterministic choice of the slot channel given by the LCG generator, which can dispatch the packets quicker or slower than a frame duration. The MC-SCP-MAC attains the maximum values of the delivery ratio for an optimal value of four slot channels. The shortest duration of the frame allows for achieving low latency and high delivery ratio.

The throughput fairness index of MC-SCP-MAC has also been evaluated, for different network sizes and number of slot channels. This metric allows for verifying if the MC-SCP-MAC is fair in terms of opportunities to use the channel by all the nodes (in the network in order to transmit their packets). Fairness aspects are especially conspicuous when very few nodes are competing in a region. Short and long term fairness has been analyzed as a function of the number of slot channels for different sizes of networks. Results for network sizes $n = 10$ and 30 nodes shows that the increase of the number of slot channels improves the short-term fairness of MC-SCP-MAC. The long-term fairness stays high for all the considered values of the number of slot channels. Results for the throughput fairness index for $n = 99$ nodes consider a dense deployment scenario, and show that, as the number of slot channels increases, the short-term fairness improves. By comparing these results with the ones for $n = 30$, the highest network sizes lead to a less fair behaviour among the nodes for the short-term fairness. High values of throughput fairness index are presented for the long-term fairness index for all the network sizes. Finally, it is worth mentioning that the throughput fairness index is very important if the envisaged scenario of the MC-SCP-MAC considers QoS policies.

Chapter 9

Conclusions and Suggestions for Further Research

9.1 Conclusions

Nowadays, the user of WSNs is becoming more and more demanding in terms of choice and diversity of applications. As a consequence, as the diversity of applications continues to grow there is a need to identify and classify the set of characterization parameters. These characterization parameters should allow for understanding the differences or similarities, advantages or disadvantages of different WSN applications, facilitating the WSNs applications designer to have a complete insight about the possible application requirements or possible outcomes from a specific Wireless Sensor Network (WSN) application area.

In fact, the information available in the literature about WSN's application classification is very generalist and does not completely describe specific WSN applications. Therefore, nowadays, there is a lack of a taxonomy which gathers several characterization parameters to exhaustively characterize and classify a WSN application. For these reasons, one of the main contributions from this PhD thesis is a taxonomy for the characterization and classification of WSN applications that has been presented in Chapter 2. This taxonomy fills the gap in the WSN literature by describing the classification and characterization parameters (criteria), and that can be used by other researchers or WSN's applications designers as a tool to better understand the services and requirements of each application. A holistic overview of the WSN application taxonomy is performed in which the relations (links) between different groups of classification, with the same value for a certain set of characterization parameters has been pointed out. These inter- and intra-connections among the applications groups facilitate to understand how different WSN applications from different areas may share the same parameters values/attributes. Moreover, this holistic overview allows for understanding that other WSN applications which do not share the same parameters values are assumed as different among all the aforementioned WSN applications.

Based on the different inter- and intra-connections three new groups of applications characterization parameters can be defined. The first group is based on the time related constraints of the application (e.g., lifetime, scalability). The three possible categories are Long-Term Applications (LTA), Medium-Term Applications (MTA) and Short-Term Applications (STA). The second group considers the data stream related constraints of application, such as service components and bit rate. It can be classified as High Data Stream Applications (HDS), Medium Data Stream Applications (MDS) and Low Data Stream Applications (LDS). The third group is related to the delivery requirements and delay sensitivity of the applications (e.g., QoS, criticality, interactivity). It is sub-divided into Real Time & Sensitive Delay Demanding Applications (RT-SDD) and Non Real Time & non Sensitive Delay Demanding Applications (NRT-nSDD). To complete the WSN application taxonomy, a chronological comparison is presented for the existing projects in all the highlighted areas, along with the evolution path towards new WSN application areas and future trends. Based on the vast WSN applications fields as well as the considered taxonomy, the applications have been subdivided into three generations. The first generation is characterized by applications that are considered as isolated and self-contained systems with a sink

node. The second generation is characterized by heterogeneous WSNs, where sensor networks offer a more rich and more complex set of services and information to the end users. This new class of network traffic gives the ground to the third generation (3G) of WSN along with communication between *things*, and with traffic patterns different from the traditional human-centric communications. This is known as the Internet of *Things*. With 3G, new fields of applications are arising such as the interactive class application, cognitive aid WSN application, ubiquitous mobile WSN, “green radio communications”, harvesting WSN and WBAN applications as well, and participatory sensing. With the Internet of *Things*, tiny Ultra Low Power (ULP) transceivers allow for thousands of devices to communicate among them whilst increasing the usefulness of each device.

The development and implementation of instrumentation and sensor data dissemination solutions for real WSN applications and scenarios, namely for health case, structure monitoring and precision agriculture areas has been addressed in Chapter 3. Different prototype sensor belts have been produced within the Smart-Clothing Project, which aim at detecting the movements of the foetus in a pregnant woman, whilst considering a network based on the IEEE 802.15.4 standard on a hierarchical wireless network with a Wi-Fi layer on top of the WSN that allows for extra flexibility in data communication.

In the framework of the structure monitoring application, it has been addressed the development of an automatic measurement system allowing for monitoring the temperature and humidity within civil engineering structures. Contributions have been given in the context of the INSYSM project. A wireless sensor network has been developed based on the IEEE 802.15.4, allowing for the creation of a continuous monitoring system capable of sending data wirelessly. In the precision agriculture area a WSN capable of establishing all the network connections, in a automatic way, while measuring physical values from the surrounding environment in a vineyard and triggering devices that are attached to sensor nodes has been developed and tested in real-world scenario. Examples of sensed physical parameters are temperature, CO₂ level, moisture level and wind speed.

A large amount of MAC protocols have been proposed all over the years to mitigate or try to solve several energy waste problems, whilst optimizing some performance parameters. Chapter 4 addresses the classification of key MAC protocols throughout a taxonomy. This MAC protocol research can be categorized in many different ways. However for the purpose of this thesis the classification of the MAC protocols into different categories has been performed by the technique used by the MAC protocol to access the channel, along with the possibility of the MAC protocol use multiple techniques. Due to the large amount of work that has been produced over the past two decades on WSNs, many of those apply more than one technique in the MAC layer. Hence, this taxonomy classification extends the classification of WSN MAC protocols for the new ones that employ multiple techniques to achieve the purposed objective. Three main categories of MAC protocols stand out from the ones presented throughout this chapter: Unscheduled, Scheduled and Hybrid MAC protocols. Moreover, comparison tables for the considered MAC protocols have been presented. From this intensive MAC techniques and protocols analysis the most promising MAC protocol which was worthwhile to assume as a solid basis for the future development of our own MAC protocol was SCP-MAC. The main reasons to choose the SCP-MAC protocol are identified. These reasons are three-fold: i) employs two-contention windows to contend for the medium; ii) synchronized channel polling combined with reserver mechanism and iii) low power listening protocol.

Chapter 5 has provided a detailed description of the mechanisms employed in SCP, along with the lessons learned during our the experience trying to implement the SCP protocol in the Mobil-

ity and MiXiM Frameworks. In addition, the possible SCP state transition diagram offers to the user the chance to follow closely how the simulator changes between the different simulations states. In order to conduct diverse types of experiments regarding single and multi-hop topologies, different traffic patterns generated by the application layer (heavy and periodic), the need of sending acknowledgement packets as a response to successful reception of data packets, we implemented different modes of simulation in the simulator. The use and operation of these modes has been described throughout Chapter 5.

Chapter 6 has addressed the implementation of the SCP protocol in the simulator and describes its performance evaluation considering single and multi-hop scenarios in the MiXiM framework simulator. The tests involved the single hop scenario in which the power consumption has been evaluated considering the employment of the piggyback technique while varying the contention window sizes and the inter-arrival periods. The use of the piggybacking technique has shown improvements showing to be a truly efficient technique, since the power consumption with piggybacking achieves 10-30 % lower values than the ones with explicit SYNC packets (piggybacking is not enabled). In addition, has also been investigated how some values of the parameters from SCP may cause changes in the performance. One of the modified parameters is the size of the wake-up tone in which the setting of a fixed duration of the wake-up tone to 2 ms (minimum duration of the wake-up tone in SCP) leads to an effective decrease of the energy consumption. By comparing the power consumptions in the presence and absence of a fixed wake-up tone duration, the energy savings obtained with a fixed wake-up tone duration are adequate (approximately 0.005 mW). Besides the energy efficiency evaluation of the SCP, the throughput performance with heavy traffic load is also assessed. For the multi-hop scenarios it is presented the SCP energy performance for multi-hop networks in a linear chain topology. The results have shown that the cases with higher contention window sizes lead to a higher energy consumption per node. However, for the multi-hop scenario as the inter-arrival period increases the energy consumption behaviour is more or less stable.

In addition to the implementation of the SCP protocol in the simulator, and consequent performance evaluation in Chapter 6 it is also described a model for the lifetime of SCP-MAC protocol with piggyback enabled. It has been shown the effect of different application variables such as the contention window maximum sizes, inter-arrival periods, network density, and polling period in the overall energy consumption (which directly affects the lifetime of the network). The presented results for the lifetime consider two types of battery models: the ideal (does not considers battery recovery phenomena's) and the Peukert's (takes into account the rate capacity effect but does not take into account the recovery effect) battery models. Normally in sensor nodes the nominal operation voltage is around 1.8 V. Below this value it is considered that the node stops operating normally. In the lifetime analysis performed for SCP, the battery voltage discharge decreases sharply for shorter packet inter-arrival periods and for larger maximum contention window sizes. The high data packet generation jointly with the increase of the maximum contention window sizes leads to a more quick depletion of the battery. Therefore, the node that employs a higher maximum contention window size and/or higher data packet generation achieves the lowest collision probability (which leads to a higher delivery ratio) and shorter values of latency. In turn, the depletion of the battery occurs faster.

Chapter 6 also addresses another main contribution of this PhD work. It presents an analytical study on the collision probability in the first contention window (CW_1) and in the second one (CW_2) along with the expected number of nodes that pass from CW_1 to CW_2 (under saturated and unsaturated traffic loads). Simulation results verify the analytical models (individual slot

state analysis approach and combinatorics one). The collision probabilities of SCP two-phase contention mechanism are investigated whilst considering saturated and unsaturated traffic load regimes. It has been shown that the CW_2 collision probability is directly related to the expected number of nodes that pass to CW_2 . For the expected number of nodes that pass from CW_1 to CW_2 , simulation and analytical results are well fitted. The results from the model under the unsaturated regime present some deviation relatively to the simulation results, although they follow them for larger number of nodes. For $CW_k^{max} = 8, k \in \{1, 2\}$, the CW_2 collision probability analytical curves are similar to the simulation ones, except for $n \leq 20$ and $n \leq 70$, for the saturated and unsaturated regimes, respectively. For $CW_k^{max} = 16, k \in \{1, 2\}$ the analytical results match the simulation ones, except for $n \leq 40$ in the saturated regime. In the unsaturated case, some deviation from the simulated results occurs for larger number of contending nodes. The analytical model underestimates the simulated collision probability in CW_2 , presenting a maximum deviation of approximately 5 % from the simulated value. Once again, the observed deviations are due to the rounding operations of the expected number of nodes that pass from CW_1 to CW_2 . From our analytical model for the collision probability in the two-phase contention window mechanism the average MAC service time for a successful transmission and the achieved throughput has been derived. The average service time increases while the network throughput significantly decreases as the number of sensor nodes and the contention windows sizes increase. The average service time and throughput are bounded by an asymptotic value when the collision probability in the contention window CW_1 reaches the maximum value.

In the initial performance evaluation of the SCP presented we have considered the CC1100 radio transceiver, which is a non-compliant IEEE 802.15.4 standard. Since there are new radio transceivers, which are IEEE 802.15.4 compliant, we found necessary to perform tests considering IEEE 802.15.4 compliant radio transceivers (CC2420 and AT86RF231). In addition, the considered radio frequency propagation models (i.e., IEEE 802.15.4 standard indoor and outdoor propagation model) were implemented in the MiXiM simulation framework. The use of IEEE 802.15.4 compliant radio transceivers leads to a clear decrease in the energy consumption in the presence and absence of piggybacking. Considering a multi-hop linear chain of sensor nodes, the SCP energy consumption is stable as the inter-arrival time varies. However, only the AT86RF231 transceiver presents lower mean energy consumption compared with the radio transceiver that does not complies with the IEEE 802.15.4 standard. Besides, the values of the achieved throughput are similar for both types of transceiver. In terms of delay, all the three radio transceivers have presented the same data packet latency, since the transmission bit rate is the same and the specific time parameters of all these radio transceivers are similar. For the linear chain scenario (multi-hop topology) and by comparing the energy consumptions between the three radio transceivers, the one that presents the lowest mean energy consumption is the AT86RF231 one. The CC2420 and CC1100 radio transceivers present similar values for the energy consumption. For all the configurations the energy consumption behaviour is consistent as the inter-arrival time is increasing. In the linear chain scenario the importance of different durations of the frame and the enabling of ACK packets is also investigated. In terms of node latency we may conclude that the latency curve when SCP polls each second (with the ACK packets feature enabled) is the one that presents the longest delay, due to the data packets retransmissions. When the polling period is set to 0.15 s, the maximum data packet latency is less than 20 s, but the energy consumption increases due to the number of times the node wakes-up. With the ACK packets feature disabled (for all three radio transceivers), we observe that the maximum data packet latency is less than 70 s (at the end of the linear chain), when

polling each second. Moreover, when polling at each 0.15 s (with the ACK packets feature disabled), the latency is less than 10 s. The Data Packet Success Rate (DPSR) of SCP in a linear chain topology was also studied to assess the importance of selecting different durations of the frame and the enabling of ACK packets. With the ACK feature enabled for both polling periods, there is approximately 100 % packet delivery success for all the three radio transceivers. When the ACK feature is disabled for both polling periods, the packet delivery in both experiments varies approximately 75 and 89 % for all the considered radio transceivers. Regarding these results, the option of enabling the ACK packets feature results into an increase of data packet delivery. However, the tradeoff of this choice is the increase of the latency as well as the energy consumption. The latency, DPSR and energy consumption should be well balanced in order to fulfill the minimum requirements for the application.

Chapter 7 proposes the Enhanced Reliability Decision Algorithm in the physical layer, addressing the implementation of the Frame Capture (FC) effect feature in the IEEE 802.15.4 compliant physical layer from the MiXiM simulation framework as well. The proposed decision algorithm utilizes the Signal to Noise-plus-Interference Ratio (SNIR) and the size of the packet ($nBits$) to guarantee the delivery, to the MAC layer, of a packet received at the PHY layer with a certain reliability (δ). The frame capture effect implementation considers five situations of packets overlapping (Interference region 1 to 5), depending on the field of the target packet that is being overlapped by the interfering packet(s). The considered regions are the following ones:

- Interference region 1: the interfering packets overlap the data field from the target data packet;
- Interference region 2: the interfering packets overlap the data and synchronization fields from the target data packet;
- Interference region 3: the interfering packets overlap the entire target data packet;
- Interference region 4: the interfering packets overlap the preamble and synchronization fields from the target data packet;
- Interference region 5: the interfering packets overlap the preamble field from the target data packet.

It has been shown that enabling the frame capture effect leads to different delivery ratio gains (G_n) for each one of the regions. Interference region 1 or 4 attains $G_n = 17.43$ %, interference region 3 achieves values of $G_n = 11.33$ % while interference region 2 or 5 attains values of $G_n = 15.39$ % for a maximum number of eight interfering nodes. Region 3 is considered as the worst case possible (full frame overlapping) in which the frame capture is always advantageous. The probability of success (PS) (with and without FC enabled) for a reliability of $\delta_1 = 0.9$ is always higher than the case with $\delta_2 = 0.99$. With the increase of reliability parameter the minimum BER required to accept a packet is higher than in the case with lower value of reliability. For the SCP-MAC protocol, results are also presented when enabling the FC effect for different values of reliability. These results have shown that for $n \geq 2$ the achieved throughput for the cases with FC enabled increases around 10 % compared with the achieved throughput when the FC is not enabled. For the SCP-MAC protocol, since the nodes are all synchronized the only possible overlapping scenario is the interference region 3 (the interfering frame completely overlaps the desired signal). By comparing the gains achieved (when frame capture is enabled) with the gains presented in Table 7.7 for the interference region 3, the values are similar and

consistent. Other performance metric considered is the delivery ratio, which is deeply related with the throughput. The delivery ratio when FC is enabled (for both reliability values) is always higher when $n > 1$. For $n > 1$ the gains achieved presents a maximum value of approximately 75 % for $n = 3$, and a minimum value of approximately 42 % for $n = 5$. It is also observable that the delivery ratio gains decrease as the number of transmitters increases, but at a slower rate.

Chapter 8 addresses the proposal of a new MAC protocol based on the SCP-MAC protocol that envisages multi-channel features, refereed as the Multi-Channel-Scheduled Channel Polling (MC-SCP-MAC) protocol. The new protocol organization, namely the startup, synchronization, slot channel choice, discovery and addition to the network and medium access algorithm, packets structure, as well as energy optimization techniques are described. These techniques comprise the influential range concept, the proposal of the denial channel list technique which considers the degradation metric of each slot channel and other cognitive-based capabilities. In addition, the study of the capture effect in this new protocol is covered, as well as the extra resolution phase algorithm useful to mitigate packet losses. To better understand the development and implementation of the MC-SCP-MAC a state transition diagram for the MC-SCP-MAC protocol is proposed and described, jointly with the associated table of the events and transitions between states.

The MC-SCP-MAC performance has been extensively investigated. For the first set of tests the goal was to evaluate the collision probability of MC-SCP-MAC and compare the results with the ones from SCP. It is observable that the curves for the MC-SCP-MAC protocol achieve much lower values for the CW_1 and CW_2 collision probabilities (in both regimes) than the SCP one. This improvement is due to the use of multi-channel jointly with an enhanced two-phase contention window mechanism to cope with the possible data packet collisions. It increases the overall performance of the network at the expense of a small increase of complexity in terms of protocol algorithm.

In almost all the tests performed throughout this thesis the simulation results consider mostly the CC2420 radio transceiver. However, one of the sets of experiments presents the energy consumption per packet successfully delivered between MC-SCP-MAC and SCP-MAC, for the CC2420 and AT86RF231 transceivers. The MC-SCP-MAC protocol presents for the AT86RF231 transceiver the lowest values of energy spent per delivered packet in comparison with the single-channel SCP-MAC protocol. The lowest values of energy spent per delivered packet are justified by the very high delivery rate, owing to the use of multiple channels combined with the ultra-low power consumption features of the AT86RF231 transceiver (with low energy consumption, shorter duration to perform CS, shorter duration to perform channel switching). The same holds for the CC2420 transceiver in which the MC-SCP-MAC protocol also presents lower values of energy spent per delivered packet than the SCP-MAC protocol. Since MC-SCP-MAC is a multi-channel based protocol we demonstrated how the collision probability behaves as the number slot channels for data utilized as a function of the number of slot channels, $N_{ch} \in \{3; 4; 7; 9; 15\}$. Here, SCP-MAC considers a single-channel for data ($N_{ch} = 1$). The network size considered in these tests is $n=99$ nodes plus 1 PAN coordinator. The increase of the number of slot channels allows for nodes selecting different slot channels and therefore decreasing the probability of a node choosing the same slot channel to transmit their data packets. The difference of the CW_1 collision probability between the MC-SCP and SCP protocols is more noticeable in the unsaturated regime. The curves for the CW_2 collision probability for the MC-SCP-MAC protocol decrease as the number of slot channels increases. In comparison with the SCP protocol the CW_2 collision probability of the MC-SCP-MAC protocol is always lower. This is due to the low

values of CW_1 collision probability that arises from the multi-channel features and which leads to a low number of expected number of nodes that pass from CW_1 to CW_2 . From these tests the conclusions are twofold: the number of slot channels increases along with the proposed enhanced two-phase contention window mechanism allowing for achieving a much lower collision probability of the data packets; The difference of effective collision probability between the MC-SCP and SCP protocols is more notorious in the saturated case as the number of slot channels increases. Other tests were performed to evaluate the energy efficiency with multiple slot channels and contention window sizes. Energy efficiency comparison is performed for the MC-LMAC and MC-SCP-MAC whilst considering equal deployment area and transmission power.

In Chapter 8, it is shown the adaptation of the IR concept to a multi-channel based protocol along with the impact of the enabling of the IR concept in the MC-SCP-MAC in terms of energy performance. The objective of these tests is the analysis of the gains achieved when the IR concept is enabled for different values of sensing range, $\Pi_{irmax} \in \{-90; -80; -70; -60\}$ dBm. By enabling the IR, the node that overhears a data packet and verifies that it has redundant data in the queue to send to the sink it drops these redundant packets. The adapted IR concept has shown improvements, providing significant reduction of the redundancy of data packets and consequently, the reduction of energy consumption per node. As the value of Π_{irmax} increases the influential range of each node decreases which leads to a decrease of the overhearing and the consequent diminishing in the discarding of redundant data packets. An additional performance metric was defined, the energy consumption saving. This translates the difference in terms of energy that a node can save when applying the IR concept (for different values of Π_{irmax}). The energy consumption saving is higher if the nodes have to send 600 packets to the PAN (long-term evaluation). Moreover, larger network sizes present the highest energy consumption savings when $\Pi_{irmax} = -90$ dBm (for 99 nodes a gain of 21.42 %; for 50 nodes a gain of 11.70 %; for 20 nodes a gain of 7.07 %). These savings decrease as the value of Π_{irmax} increases. This is due to the reduction of the influential area which, in turn, reduces the overhearing of data packets by the node (decreases the level of data packet redundancy), leading to the increase of the energy consumption per node, i.e., there is a reduction in the energy consumption savings.

Additional tests with variable number of slot channels were conducted to assess the benefits gained from the use of the IR concept in a multi-channel MAC protocol. It was conclusive that if the number of slot channels used by the MC-SCP-MAC increases the energy consumption also increases. However, the employment of IR allows for reducing the energy consumption for low values of Π_{irmax} . As the value of sensing range, Π_{irmax} , increases the number of redundant packets increases. Therefore, more packets are going to be exchanged, leading to an increase of the energy consumption. The energy savings decrease as the value of the sensing range, Π_{irmax} , increases. In turn, these gains are higher as the number of available slot channels increases.

In WSNs the most usual traffic pattern is the periodic one. In all the tests performed throughout the thesis the periodic traffic pattern is always used in the simulations. However, for the MC-SCP-MAC performance evaluation the impact of different traffic patterns in the performance is also presented. MC-SCP-MAC supports higher traffic generation intervals than other multi-channel based MAC protocols (e.g., MC-LMAC). MC-SCP-MAC supports periodic and exponential traffic generation profiles with higher and lower traffic generation intervals. The results for sparser scenarios have shown that the aggregate throughput does not attain a desirable value. However, tests have been conducted considering a denser scenario for $\lambda = 1 \text{ s}^{-1}$ (under periodic and exponential traffic generation). An aggregate throughput was achieved close to

the maximum. With these results we can conclude that the MC-SCP protocol presents a better performance in higher density scenarios but the presence of hidden terminals may lead to a degradation of the aggregate throughput as the number of source nodes increases. A method that decreases the impact of the hidden terminals problem is imperative. Another conclusion is that the increase of the traffic generation rate is well supported by the MC-SCP-MAC in scenarios that do not present the hidden terminals problem. In terms of latency, as the number of source nodes increases the values of the latency are longer. However, in scenarios with larger nodes density the values for the latency are longer than the scenarios with sparser nodes density.

Since MC-SCP-MAC is more robust and efficient in denser scenarios and the envisaged scenario for this protocol is a deployment of sensor nodes in a forest or an agricultural field we consider that the performance evaluation in a cluster topology can be useful to extract insights for further improvements in the protocol. The objective is to assess the impact of the IR concept enabling and the number of slot channels available for data exchange in the MC-SCP-MAC, while considering different traffic patterns and data generation frequencies. In cluster topology the increase of the number of slot channels leads to a decrease of the aggregate throughput when the IR is disabled. This is due to the high contention between nodes that possess a higher number of packets in the queue to be transmitted and are trying to win the medium in order to transmit their packets. However, by enabling the IR concept it allows for achieving the highest values of aggregate throughput when $\Pi_{irmax} \in \{-90; -80\}$ dBm, due to the values of the sensing range that it allows nodes to overhear more packets and therefore increasing the level of discarded packets. Energy consumption per node increases as the number of slot channels increases, whereas the enabling of the IR concept allows for achieving lower values of energy consumption per node. As the sensing range value, Π_{irmax} , increases the energy consumption also increases. It increases up to the values of energy consumption when the IR is not enabled. In terms of latency value it is observable that the use of the IR allows for obtaining a shorter values for the latency since there are less packets in the queue to be transmitted by the sensor nodes. For sensing range values $\Pi_{irmax} = -90$ dBm, the MC-SCP achieves latency values around 2.8 s (3 hops in average). It corresponds to a latency of around 0.933 s per hop, almost a frame time duration per hop. As the sensing range value, Π_{irmax} , increases the latency becomes longer. This increase of latency is due to increase of the number of packets waiting in queue to be transmitted. If the IR feature is disabled for all the considered number of slot channels, the latency value is around 23 s. The same holds for the case when the IR is enabled, since for all the considered number of slot channels the latency is similar and becomes longer as the sensing range value increases.

In order to test the scalability of the MC-SCP-MAC protocol we vary the density of the node deployments in a homogeneous network. The deployment scenario is varied between 50×50 m² and 200×200 m². The objective of these tests is the analysis of the gains achieved when the IR is enabled for different values of $\Pi_{irmax} \in \{-90; -80; -70; -60\}$ dBm while deploying the same network size in different deployment areas. Interesting results are presented for the performance metrics such as, the aggregate throughput, delivery ratio, latency, energy consumption and energy consumption savings when the MC-SCP-MAC is deployed in scenarios with side lengths larger than 125 m and as the values of the sensing range Π_{irmax} vary. As the MC-SCP-MAC protocol is based on the SCP-MAC protocol a performance analysis of MC-SCP-MAC in a linear chain topology is also presented in Chapter 8. The end-to-end latency and delivery ratio of the MC-SCP-MAC protocol has been analyzed, while varying the number of slot channels and considering different durations for the slot channels and frame. It is observable that as the number of hops in the linear chain increases the latency of the packets becomes longer.

However, for the SCP-MAC protocol for all the values of T_{poll} with and with no acknowledgements the latency values are always longer than the ones of the MC-SCP-MAC. The use of the enhanced two-phase contention window mechanism along with the multiple channels allows for the MC-SCP-MAC to transmit more packets concurrently in different slot channels with no interference and consequently the delivery ratio increases and the latency decreases.

The shortest values of latency are verified for the case of $N_{ch} = 4$ slot channels but with a frame duration $t_F = 0.85$ s as the number hops increases. For the cases in which the frame duration is $t_F = 1$ s, the increase of the number of slot channels does not differ in much the latency values as the number of hops increases. We can conclude that the MC-SCP-MAC with a shorter frame duration than the traffic generation interval can achieve a shorter latency, since it can dispatch quicker the packets stored in the queue to be transmitted. In average, the MC-SCP-MAC presents a mean latency per hop of 0.9 s. This value is shorter than the frame duration in some cases. This is possible due to the deterministic choice of the slot channel given by the LCG generator that can dispatch the packets quicker or slower than a frame duration. In terms of delivery ratio the MC-SCP-MAC attains the maximum values for an optimal value of four slot channels. The smallest duration of the frame allows for achieving low latency and high delivery ratio.

To conclude, the throughput fairness index of MC-SCP-MAC has been evaluated for different network sizes and number of slot channels. This metric allows for verifying if the MC-SCP-MAC is being fair in terms of opportunity to use the channel by all the nodes in the network in order to transmit their packets. Fairness problems are especially conspicuous when very few nodes are competing in a region. Short and long-term fairness has been evaluated for different sizes of networks as a function of the number of slot channels.

The results for network sizes of $n = 10$ and 30 nodes shows that the increase of the number of slot channels improves the short-term fairness of MC-SCP-MAC. The long-term fairness stays high for all the number of slot channels considered. The results of the throughput fairness index for $n = 99$ nodes is considered as a dense deployment scenario. The results obtained show that as the number of slot channels increases the short-term fairness is improved. By comparing these results with the ones that consider $n = 30$, the largest network sizes lead to a less fair behaviour among the nodes for the short-term fairness. High values of throughput fairness index are presented for the long-term fairness index in all the network sizes. The throughput fairness index is very important if the envisaged scenario of the MC-SCP-MAC considers QoS policies.

The results presented in this thesis reveal the importance of an appropriate design MAC protocol for the desired WSN application. It is worthwhile to mention that, depending on the objective or mission of the WSN application, different protocols are required. Therefore, the overall performance of a WSN application heavily depends on the development and application of the appropriate protocols (MAC, routing, etc). Different techniques and algorithms are useful to increase the overall performance of the protocols and, consequently, to increase of the overall performance of the WSN application. This thesis has given innovative contributions on the following issues:

- A taxonomy for the characterization and classification of WSNs applications accomplished via an application-oriented approach;
- The development and implementation of instrumentation and sensor data dissemination solutions for real WSN applications and scenarios, namely for the health, structure monitoring and precision agriculture areas;

- The proposal of a MAC protocols taxonomy that distinguishes different protocols by the technique employed to access the channel, whilst considering that one MAC protocol may utilize multiple techniques;
- The implementation of the SCP-MAC protocol in the MiXiM framework simulator;
- A stochastic model for the collision probability in the collision avoidance mechanism with two contention windows utilized in the SCP protocol, whilst considering the saturated and unsaturated cases;
- A model for the computation of the average MAC service time for a successful transmission as well as the achieved throughput based on the proposed model for the collision probability;
- The proposal of a new physical layer packet reception decision algorithm based on a reliability, the Enhanced Reliability Decision algorithm. The formulation utilizes the SNIR and the size of the packet to guarantee the delivery, to the MAC layer, of a packet received at the PHY layer with a certain reliability;
- The incorporation of the frame capture effect feature in the IEEE 802.15.4 compliant physical layer for the MiXiM simulation framework;
- The proposal of an innovative efficient MAC protocol, based on the SCP-MAC protocol, which envisages multi-channel features, the so-called Multi-Channel Scheduled Channel Polling (MC-SCP-MAC) protocol.

9.2 Suggestions for Future Research

As future work, we propose to implement other types of wireless sensor communication systems that may work together with the existing ones. For example, by creating a webpage where healthcare professionals are able to scroll through all the data produced in real time while sharing the information with other medical institutions.

Another proposal is to implement algorithms for signal source separation, noise and motion artefact signal suppression, as well as to implement advanced algorithms for data treatment and aggregation. Further work is needed to upgrade the signal conditioning circuitry, the processing software (to accomplish a real time filtering) and statistical techniques to detect the foetal movements in the piezoelectric belt. The data collected from the belt contains signals from the mother and foetus. An alternative approach to distinguish the different signals detected with the belt may be based on a spectral analysis instead of time domain analysis, facilitating the separation of the different signals, such as the mother respiration, foetus movements, mother's heart beat and motion artifacts. Other techniques may be based on the Fast Fourier Transform (FFT), which detects a peak from a signal composed by signals with different frequencies, or blind source separation.

Another suggestion for further research is to investigate the collision probability model considering limited retransmissions and other queueing models, such as the $M/M/1/K$ Markov chain model, which assumes finite buffers. In addition, we plan to use the model in the routing layer of wireless sensor networks, in a real testbed, in order to use the model's output to decide whether to transmit a packet, depending on the number of neighbour nodes. It can also be suggested to analytically compare the advantages/disadvantages of using one or two

contention windows in slotted contention based MAC protocols. The idea is to apply the two phase contention window mechanism of the SCP-MAC protocol with the specifications of the IEEE 802.11 Distributed Coordination Function (DCF) access method. The objective is to derive the achieved throughput based on the different slot probabilities and find the optimal values of the contention windows sizes that maximize the throughput for a certain network size. In addition, a throughput comparison between the IEEE 802.11 DCF and the modified IEEE 802.11 DCF access methods is planned.

Deployment in MC-SCP-MAC can be performed by taking into account if the IDs from the neighbouring nodes are sequential or random.

Appendix A

Choice of the Simulator: Simulators Classification

A.1 Introduction

This appendix addresses a list of possible simulators that can give us several choices for simulating MAC and PHY layer, as well as cross-layer design issues and network aspects (e.g., routing).

A.2 Objectives

The main objective of this appendix is to provide a first approach of the different simulation tools for the WSNs and decide what tool we can use to validate the different layer protocols (e.g., MAC, network protocols) in the nodes before deploying them into the real-world. In addition, optimization procedures implemented in the simulator are foreseen in order to contribute to the minimization of the overall power consumption.

A.3 Simulation Tools

A.3.1 Introduction to Simulation Tools

A simulation is the imitation of the operation of a real-world process or system over time. This is performed whether by hand or by a computer. The simulation involves the generation of an artificial history of a system and the observation of that artificial history to draw inferences concerning the operating characteristics of the real system. The behaviour of a system as it evolves over time is studied by developing a simulation model. This model usually takes the form of a set of assumptions concerning the operation of the system. Thus, simulation modelling can be used both as an analysis tool for predicting the effect of changes to existing systems or as a design tool to predict the performance of new systems under varying sets of circumstances. However, many real-world systems are so complex that models of these systems are virtually impossible to solve mathematically. In these instances, numerical computer-based simulation can be used to imitate the behaviour of the system over time. Data is collected from the simulation as if a real-time system was being observed. This simulation-generated data is used to estimate the measures of performance of the system.

A.3.2 Comparing Simulation Tools

Our aim is to address WSN discrete event driven simulation tools, although time driven approaches can also be considered. Different simulation languages and tools are available; hence, a comparison among them is in order. This appendix addresses three WSNs simulators that can give us a theoretical approach of the several paradigms such as communication, networking protocols, middleware, security and management. With the ever increasing popularity of WSNs

and their potential to penetrate multiple aspects of our lives, this appendix is timely and addresses the needs of a growing community of engineers, networks professionals and managers, and educators. Sensor networks designs must be optimized in order to extend the network lifetime. The energy and bandwidth constraints and the potential large-scale deployment pose challenges to efficient resource allocation and sensor management.

The next section presents the OMNeT++, NetTopo and GTNetS simulators. We decided to choose these simulators because they present the following advantages:

- are developed for WSN or including packages for WSN;
- include the level of detail (nodes or even network details) that as appropriate;
- already include some of the protocols, e.g, IEEE 802.15.4 PHY and MAC protocol;
- the source code is public and free for academic or research purposes;
- the majority of these simulators present an user-friendly interface.

OMNeT++

OMNeT++ is a public-source, component-based, modular and open-architecture simulation environment with strong GUI support and an embeddable simulation kernel. Its primary application area is the simulation of communication networks because of its generic and flexible architecture; it has been successfully used in other areas like the simulation of IT systems, queuing networks, hardware architectures and business processes as well. OMNeT++ is rapidly becoming a popular simulation platform in the scientific community as well as in industrial settings. Several Open Source Simulation Models have been published, in the field of internet simulations (IP, IPv6, MPLS, etc), mobility and ad-hoc simulations and other areas.

The goal of this description is to bring together OMNeT++ users and their tools, applications and ideas. It intends to provide a forum for presentations of recent developments and novel ideas in a broad context of network simulation with focus on OMNeT++. It will bring together researchers to focus on the important topics of integrating simulation models, coupling different simulation tools, providing better modelling approaches, while contributing to the active modelling and simulation community. with respect to identifying some of the most promising candidate solution methods, architectures and techniques to address the various challenges of network simulation. The benefits are two-fold:

- OMNeT++ users get into direct discussion;
- The users can meet and discuss with the developers of the different framework developed for the OMNeT++; Furthermore, the developers can pick up ideas for the future development.

Topics of interest include, but are not limited to:

- Parallel simulation;
- Simulation control;
- Result interpretation and analysis;
- Debugging;
- Simulation in the loop;

- Modelling techniques;
- Coupling with other simulation/emulation tools;
- Integration of hardware-specific code;
- Cross-layer protocol design methodologies;
- Mobility models;
- Simulation of wireless and P2P networks;
- Industrial applications;
- Use of OMNeT++ in other domains.

The OMNeT++ model is a collection of hierarchically nested modules as shown in Figure A.1. The top-level module is also called the System Module or Network. This module contains one or more sub-modules each of which could contain other sub-modules. The modules can be nested to any depth and hence it is possible to capture complex system models in OMNeT++. Modules are distinguished as being either simple or compound. A simple module is associated with a C++ file that supplies the desired behaviours that encapsulate algorithms. Simple modules form the lowest level of the module hierarchy. Users implement simple modules in C++ using the OMNeT++ simulation class library. Compound modules are aggregates of simple modules and are not directly associated with a C++ file that supplies behaviours. Modules communicate by exchanging messages. Each message may be a complex data structure. Messages may be exchanged directly between simple modules (based on their unique ID) or via a series of gates and connections. Messages represent frames or packets in a computer network. The local simulation time advances when a module receives messages from another module or from itself. Self-messages are used by a module to schedule events at a later time. The structure and interface of the modules are specified using a network description language. They implement the underlying behaviours of simple modules. Simulation executions are easily configured via initialization files. It tracks the events generated and ensures that messages are delivered to the right modules at the right time [CLZ06].

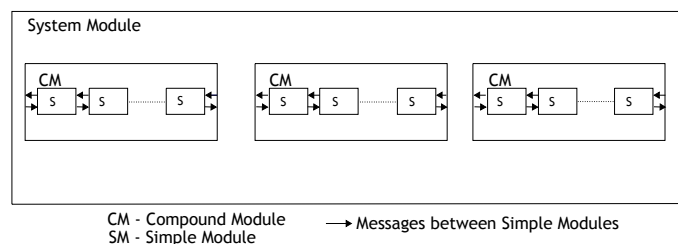


Figure A.1: Simple and compound modules in OMNeT++.

NetTopo

NetTopo is an open source research-oriented simulator and visualizer, designed to test and validate algorithms for wireless sensor networks. The goal of NetTopo is to build a sensor network simulation and visualization tool that gives users extraordinary flexibility to simulate their own algorithms and is a compelling replacement of commercial simulator focusing on visualization of the communication in the real wireless sensor network

testbed. NetTopo will help in the investigation of algorithms in WSNs [SWZ⁺08]. With respect to the simulation module, users can easily define a large number of on-demand initial parameters for sensor nodes, e.g. residential energy, transmission bandwidth, as well as radio radius. Users also can define and extend the internal processing behaviour of sensor nodes, such as energy consumption and bandwidth management. It allows for users to simulate extremely large scale heterogeneous WSNs. For the visualization module, it works as a plug-in component to visualize the testbed's connection status, topology or even the sensed data. These two modules paint the virtual sensor nodes and links on the same canvas which is an integration point for centralized visualization. Since the node attributes and internal operations are user definable, it guarantees the simulated virtual nodes to have the same properties with those of real nodes. The sensed data captured from the real sensor nodes can drive the simulation in a pre-deployed virtual WSN. Topology layouts and algorithms of virtual WSN are customizable and work as user defined plug-ins, both of which can easily match the corresponding topology and algorithms of real WSN testbed. As a major contribution of this research work, NetTopo is released as Open Source Software on the SourceForge. Currently, it has more than eighty Java classes and 11000 Java lines of source code. Users can freely download the latest version of NetTopo by accessing the NetTopo website. The friendly GUI makes it easy to use and the modular components enable it to be easily extended. Due to the algorithm-oriented design, NetTopo supports the simulation for an extremely large scale network. It is useful for the rapid prototyping of an algorithm. The visualization function uncovers the real device based WSN topology and displays the sensed data. Based on modular components design and common graphical resources, visualization process can drive the simulation. Generally, such integration takes the first step into the whole vision that applications can run partially in a simulation environment and partially in a physical WSN testbed and interact with each other to create an environment where algorithms can be much more accurately tested and validated. However, there still exist a few limitations on NetTopo and it needs a lot enhancements as follows:

- Integrate with GSN middleware. So far, NetTopo only support visualizing Crossbow WSN, although the framework can be easily extended to integrate new visualizers. GSN [WALW⁺06] is a sensor network middleware. It provides a large number of wrappers (currently there are more than 25 wrappers) for extracting data from heterogeneous sensor devices. This can help to reduce the workload to implement new wrappers for some GSN supported sensor devices;
- Simulation process controls the sensor device communication. Currently in NetTopo, visualization process can drive the simulation. However, if the driver of the sensor hardware provides API for controlling the sensors' actions such as route choosing, then our simulation result can be easily applied in the testbed for performance comparison;
- 3D visualization and localization. The basic 3D visualization model for the smart home/office scenario in NetTopo as shown in Figure A.2. As a future implementation work, we could further implement this 3D visualization model and integrate NetTopo with GPS to provide sensor nodes localization functions.

NetTopo consists of both simulation and visualization functions. These two functions need to interact with each other and access/manipulate some common resources. For focusing

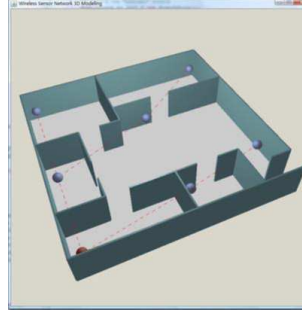


Figure A.2: A 3D visualization model

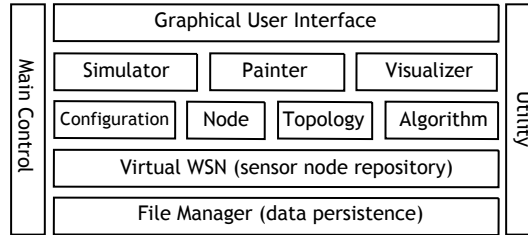


Figure A.3: NetTopo simulator components.

on the integration issues of them, we use component based NetTopo architecture, which is flexible enough for adding new components in the future. The basic architecture is illustrated in Figure A.3. The *Main Control* and *Utility* are two components involved in all layers. The *Main Control* is the core component working as a coordinator in charge of the interactions of other components. It can be regarded as an adaptor between input and output interfaces of other components and enables them to work smoothly. The *Utility* component provides some basic services, e.g., defined application exceptions, format verification, number transforms and dialogue wrappers. The *File Manager* is for the purpose of data persistence, e.g. log of the runtime information, recording statistical results as well as keeping references of virtual sensor nodes. Log information and statistical results are recorded as character streams into human readable format.

References of virtual sensor nodes are stored as serialized format for easy recovery and reuse. All these references are encapsulated in *Virtual WSN*, which works like a runtime sensor nodes repository and also declares interface to allow other components to add new virtual nodes, delete particular nodes, retrieve the same type of nodes and their derived children. In Figure A.3 the *Node*, *Topology* and *Algorithm* components are designed as highly extensible modules that can be regarded as plug-ins. The *Node* represents a virtual sensor node. Virtual sensor nodes do not have fixed properties or structures. For example, sensor nodes can have very different sensing attributes: temperature, humidity, vibration, as well as pressure. To allow users to create their own virtual sensor nodes, an abstract interface named *VNode* is declared to define several basic methods representing actions of a real sensor node. Any user that wishes to run on the simulator must implement the *VNode* interface. The *Topology* stands for the topology to be deployed in *Virtual WSN*. Network topology can assume various shapes, e.g., line, circle, triangle or tree. Users can flexibly implement any needed network topology. The *Algorithm* represents an algorithm to be applied in the *Virtual WSN*. The algorithm can be any routing, clustering, scheduling or even a controlling algorithm. Users can freely implement their needed algorithms for their specific studies.

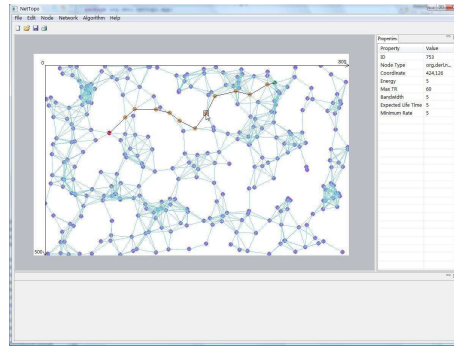


Figure A.4: NetTopo graphical user interface.

The Graphical User Interface (GUI) in Figure A.4 consists of three major components: a display canvas (on the upper left), which can be dragged in case of viewing a large scale WSN, a property tab for displaying node properties (on the upper right), and a display console for logging and debugging information. The *Painter* is separated from the main *GUI* due to the frequent painting tasks. The painter is also designed as an abstract interface for various painting requirements, e.g., 2D or 3D. The specific painter used in Figure A.3 is *Painter_2D*. Additionally, the painter encapsulates the lower painting API, interacts with the *Virtual WSN* and main *GUI* and provides advanced painting methods, e.g. it can paint a link between any two nodes by just using their ID information.

GTNetS

The Georgia Tech Network Simulator (GTNetS) is a full-featured network simulation environment that allows for researchers in computer networks to study the behaviour of moderate to large scale networks, under a variety of conditions. The design philosophy of GTNetS is to create a simulation environment that is structured much like actual networks. For example, in GTNetS, there is clear and distinct separation of protocol stack layers. The packets in GTNetS consist of a list of Protocol Data Units (PDUs) that are appended and removed from the packet as it moves down and up the protocol stack. Simulation objects representing network nodes have one or more Interfaces, each of which can have an associated IP address and an associated link. The objects in GTNetS are bound to ports, in a fashion nearly identical to the binding to ports in real network protocols. Connections between protocol objects at the transport layer are specified using a source IP, source port, destination IP, and destination port just like actual TCP connections. The interface between applications and transport protocols uses the familiar connect, listen, send, and send to calls much like the ubiquitous sockets API in Unix environments. Applications in GTNetS can have one or more associated protocol objects, and can simulate the flow of data (including actual data contents) between applications. To simulate WSNs we need to use GTSNetS [OAVRH07] that is an extension of GTNetS. The GTNetS is an C++ open-source free event-driven simulator developed by George Riley at Georgia Tech, Atlanta, USA. It enables researchers world-wide to easily model and simulate computer networks both wired and wire-less. GTNetS has been developed aiming at scalability. GTSNetS has extended GTNetS with wireless sensor network capabilities. It has been developed by George Riley and his students, especially by El-Moustapha Ould Ahmed Vall. Main contributions are the battery and mobility models. When added to the scalability, we consider that GTSNetS is particularly suitable for modelling and simulating large scale energy constrained and possibly mobile wireless sensor networks.

A.4 Conclusions

After analyzing the three simulators individually we conclude that the best simulator that ensures to our simulation needs for WSNs is OMNeT++, because it presents a public-source code, is component-based, modular and open-architecture simulation with a strong graphical user interface support as well as an embeddable simulation kernel. Other advantage of using OMNeT++ is that OMNeT++ is rapidly becoming popular in the scientific community as well as in the industrial community, in which several models have been published. Hence, the fact that there is a strong community and a forum where can be exchanged information with other people working with WSNs can be useful in the future for debugging and solve problems that overcome from the implementation or simulations. Besides, by comparing not only OMNeT++ with the other two simulators but also it with another well know simulator such as ns-2, we conclude that the OMNeT++ simulator is faster than ns-2 and uses memory more efficiently than ns-2. OMNeT++ as the advantage of supporting two types of simulation modes, the event-based and the process-oriented ones, while GTNetS only supports discrete event processing. NetTopo is developed using the JavaTM platform and OMNeT++ uses the C++ platform. As a consequence, the NetTopo does not always provide full access to the all features and the performance of the platform that the OMNeT++ runs on, C++ is more powerfull than JavaTM. In addition, C++ language often outperforms Java in arithmetic and trigonometric operations. Finally, we conclude that OMNeT++ is fully programmable and modular, and it is designed to support modelling for large scale networks. All these features make OMNeT++ a good candidate for both simulation and research purposes.

Appendix B

WSN Applications Tables for Characterization and Classification Taxonomies

B.1 Applications areas-description for Category 1 and 2 WSNs

After gathering the characteristics and classes above described, it is easier to build up a WSN taxonomy based on these characteristics and classes in order to better understand which type of applications belong to a certain group with specific characteristics.

Table B.1: WSN applications areas description for Category 1 WSNs.

Area	Description
Sensor and Robots	- Some researchers expect that mobile robotics will use WSNs to achieve ubiquitous computing environments; - For example, Intel envisions mobile robots acting as gateways into wireless sensor networks, such as into the Smart Dust networks of wireless motes. These robots embody sensing, actuation, and basic robotics functions; - Examples of projects: [DRS⁺05].
Reconfigurable Sensor Networks	- Military applications require support for tactical and surveillance arrangements that employ reconfigurable WSNs that are capable of forming networks on the fly, assembling themselves without central control, and being deployed incrementally; - Reconfigurable “smart” WSNs are self-aware, self-configurable, and autonomous; - Self-organizing WSNs utilize mechanisms that allow newly deployed WSNs to establish connectivity instinctively. In addition, these networks have mechanisms for managing WSN mobility (if any), WSN reconfiguration, and WSN failure (when that happens). - Examples of projects: [HKWW06].
Metropolitan operations - Highway Monitoring	- Transportation (traffic flow) is a sector that is expected to benefit from increased monitoring and surveillance; - Traffic Pulse Technology is an example. The goal of this system is to collect data through a sensor network, process and store the data in a data centre, and distribute those data through a variety of applications; - The system collects key traffic information, including vehicle speeds, counts (volume), and roadway density, transmitting the data over a wireless network to a data centre every 60 seconds. Each center produces the information through a wide range of methods: video, aircraft, mobile units, and monitoring of emergency and maintenance services frequencies; - Examples of projects: [CV07, MYT⁺06].

Table B.2: WSN applications areas description for Category 1 WSNs (cont.).

Area	Description
Condition-Based Monitoring	- These WSNs are designed for monitoring complex machinery and their correspondent processes. The evolution in machinery maintenance suffered an evolution no maintenance, to scheduled maintenance (e.g., change oil every three months) or to condition-based maintenance (CBM). All three techniques are in current use; - WSNs are positioned to minimize costs and, in particular, to eliminate the staffing costs, which often are the largest; - The primary challenge faced by WSNs in machinery and process monitoring is related to the quality of the information produced by both the individual sensors and the distributed sensor network. Nodes located on individual components must not only be able to provide information on the present state of the component (e.g., a bearing or gearbox), but also provide an indicator of the remaining useful life of the component. - Examples of projects: [JR07].
Military Surveillance	- These WSNs are used for military theater monitoring and can replace single high-cost sensor assets with large arrays of distributed sensors for both security and surveillance applications; - It is a need that these networks should be robust and self-organizing making WSNs deployable by untrained troops in essentially any situation; - Special characteristics are imposed in which distributed sensing provides redundant and hence highly reliable information on threats as well as the ability to localize threats by both coherent and incoherent processing among the distributed sensor nodes; - For the urban terrain, WSNs should offer troop safety as they clear and monitor intersections, buildings, and rooftops by providing continuous vigilance for unknown troop and vehicle activity; - The primary challenge for WSNs is accurate identification of the signal being sensed and low-power algorithms to classify a detected event as an impulsive event is also needed; - Examples of projects: [GM05].
Border Monitoring	- These WSNs are installed in borders to detect events. These events can include the detection of people that crosses the border, the removal of a piece of fence or attacks to the border; - It is essential to develop state-of-the-art vibration, acoustic and magnetic signal classification algorithms to accomplish this goal. Currently, WSNs run vibration detection algorithms based on energy thresholding, although this is a simple technique, it is subject to false alarms, leading to the search of new algorithms; - Examples of projects: [SBI].
Signal Blocking Devices	- These jamming devices are installed in sensor nodes from a WSN. Then these sensor nodes are scattered by the conflict area, in order to the enemy be incapable of establishing communications, but not interfering with the communications from troops that deployed the WSN.
Structural Integrity Monitoring (SIM)	- Research has been under way in recent years to develop sensor technology that is applicable for buildings, bridges, and other structures. The goal is to develop "smart structures" that are able to self-diagnose potential problems and self-prioritize requisite repairs; - Up to the present, wired seismic accelerometers have been used, however, these devices are expensive and are difficult to install; - Therefore, some projects used Smart Dust motes as a device for structure monitoring; - Data from the Smart Dust motes is expected to increase the accuracy of finite element analyses, a method of computer modelling where mathematical equations represent a structure's behaviour under given conditions; - Examples of projects: [BEOiRTUE07].

Table B.3: WSN applications areas description for Category 1 WSNs (cont.).

Area	Description
Monitoring Volcanic Eruptions WSN (MVE-WSN)	- MVE-WSN is a wireless sensor network to monitor volcanic eruptions with low-frequency acoustic sensors. This WSN was deployed in at the volcano Tungurahua, an active volcano in central Ecuador. The network collected infrasonic (low-frequency acoustic) signals at 102 Hz, transmitting data over a 9 km wireless link to a remote base station; - During the deployment, over 54 hours of continuous data have been collected, which included at least nine large explosions. Nodes were time-synchronized using a separate global positioning system (GPS) receiver, and the data was later correlated with that acquired at a nearby wired sensor array. In addition to continuous sampling, a distributed event detector that automatically triggers data transmission when a well-correlated signal is received by multiple nodes has been developed; - MVE-WSN has a wide range of goals related to both scientific studies and hazard monitoring. Another use of seismic networks is the imaging of the internal structure of a volcano through tomography inversion. Earthquakes recorded by spatially-distributed seismometers provide information about propagation velocities between a particular source and receiver; - Examples of projects: [WALJ⁺06].
Habitat Monitoring	- These WSNs monitor the microclimates in and around nesting burrows; - The goal was to develop a habitat-monitoring kit that enables researchers worldwide to engage in nonintrusive and no disruptive monitoring of sensitive wildlife and habitats; - For habitat, monitoring the planner needed sensors that can take readings for temperature, humidity, barometric pressure, and midrange infrared. Motes sample and relay their sensor readings periodically to computer base stations on the island; - Examples of projects: [MCP⁺02].
Water Monitoring	- These WSNs monitor the condition of the water that is then sent to be consumed by humans at their houses; - The sensor nodes should have sensors that identifies poisons or others pathogenic agents. Besides the monitoring of water quality, these WSNs should be capable of introducing biological agents to eliminate pathogenic agents or if there is poisons in the water should shutdown the main valve of the water supply; - Other example related with water monitoring is the Flood detection example; - Examples of projects: [Aqu, dLGLM⁺07].
Precision Agriculture	- These WSNs are scattered around by an agriculture field and in the machines (mobile or static) that are present in the agricultural facility; - The sensor nodes have several sensors attached to monitor temperature, moisture (soil or air), wind speed, pH (soil or water), rainfall quantity, solar intensity and global position system (GPS) device; - Besides the sensors, it is a necessary to actuate in certain machines/devices such as water motors or electro valves. The sensor nodes should send the data to the base station where is computed so that decisions should be taken and sent to the sensor nodes attached to the machines; - Examples of projects: [BDO⁺05, MID04].

Table B.4: WSN applications areas description for Category 1 WSNs (cont.).

Area	Description
Weather Monitoring	- These type of WSNs are used sensors from the traditional weather stations, but in this case the data communication is done wireless, using WSNs. These WSNs should be easy to deploy; - Glacsweb is a project with the aim of monitoring glacier behaviour via different sensors and linking them together into an intelligent web of resources; - Glacsweb aims at the development of a low-power wireless sensor network node capable of surviving for several years, which gathers the data autonomously into a web-accessible database. Probes are placed on and under glaciers and data collected from them by a case station on the surface; - Measurements include temperature, pressure and sub glacial movement; - The aim is to understand what happens beneath glaciers and how they are affected by climate. The data gathered is important in understanding the dynamics of glaciers as well as global warming; - Examples of projects: [JM06].
Crop Monitoring	- Other type of WSNs application is the crop monitoring such as corn and vineyard; - The main purpose of these WSNs is the scattering of these sensor by the crop field to monitor the microclimate in each zone monitored by the sensor node; - Other function of these WSNs is the detection of fungi or crop diseases; - The data are sent to a base station that monitors these microclimates and keeps all the data in a database while keeping the crop values for each microclimate; - Besides the sensor devices installed in the motes, it is necessary to actuate devices installed in the crops.
Nanosopic Sensor Applications	- There is enthusiastic interest in WSNs for biological sensing. In particular, there is interest in the "labs on a chip" concept, including new methodologies supported by nanotechniques; - Using this technology, one can detect biowarfare pathogens and can use it as a diagnostic tool in medicine. This work is expected to lead to the development of a very sensitive wristwatch biomonitor that soldiers can wear, through a wireless radio link, physicians can then keep tabs on each soldier's physiology on a cellular and molecular level and can identify any substance that a person might encounter.
Forest Fire Detection	- In recent years, Portugal has had serious problems with forest fires; - In these cases, a WSN could be deployed to detect a forest fire in its early stage. For this purposes a number of nodes need to be pre-deployed in a forest; - Each node could gather different types of information from sensors, such as temperature, humidity, pressure and position. All sensing data is sent by multi-hop communication to the control centre via a number of gateway devices distributed throughout the forest; - The gateways will be connected to mobile networks e.g., Universal Mobile Telecommunications System (UMTS), and will be positioned to reduce the number of hops from the source of fire detection to the control centre; - The gateways will also reduce network congestion in large-scale deployments by extracting data from the network at pre-determined points; - Operators in the control centre can judge if it is a false alarm by either using the data collected from other sensors or dispatching a team to check the situation locally. Then, both fire fighters and helicopters can be sent to put out the fire before it grows to a severe forest fire; - Examples of projects: [ASSDGC08, ASSdGC06].

Table B.5: WSN applications areas description for Category 1 WSNs (cont.).

Area	Description
Target tracking	- The aim of this application scenario is the monitoring of trolleys for baggage in a railway station; - The trolleys are located in some fixed locations distributed in the area. When they are used by passengers and not replaced in the appropriate locations, in general they are distributed over the whole area; - Moreover, some trolleys could be taken outside the railway station. To know if some of them are taken outside the station the trolley is equipped with an active RFID tag and each fixed location and entrance or exit with a sensor node equipped with an RFID reader; - Sensors periodically collect the position information coming from the RFID tags, organize themselves in a WSN and transmit all the information to the final user, the master of the network, located, for example, in an office of the station; - Examples of projects: [HKL⁺06, DHJ⁺06].
Warehouse tracking	- This type of scenario for WSNs is used for stock monitoring in a warehouse; The warehouse manager and the handling department can take into account that when the stock of one particular product increases, it has to be stored out of its corresponding area; - Thanks to wireless (sensor) ID tags, each container has an electronic reconfigurable identifier, able to transmit the product code, date of production, date of storage and a number of other pieces of information useful to the warehouse manager; - In addition, it can monitors the changes in the products location (time of moves, location, position, etc.) and the consumers (profile, time spent in the area or in front of a product, products they are interested in, etc.). Besides, the managing of the products, in real time he observes the way the products impact on the consumer behaviour, adapting his strategy and product display according to shopper behaviour; - In addition, the producer packaging (path, duration of transport and intermediary storage, incidents in cold chain) informs the manager about the history of the enclosed products. With the geo-positioning function, the manager can locate the right container to be sent in order to ensure a logical flow of containers and avoid unintentional long-term storage (first-in first-out). Thanks to a direct access to her database, the manager gets in real time and accurately the inventory levels of the stocks; - Examples of projects: [EHK⁺07].
Immersive Roam Application	- The LEMe room is an intelligent environment with a multi-projection display called LEMeWall, which is designed to support the research on innovative 2D/3D mixed reality interaction; - The LEMeWall is a tiled display system compound of twelve and is complemented by a network of five cameras for body gesture tracking and microphones for voice interaction. Sensors and actuators can play an important role in the interaction capabilities with the LEMeWall, and one of the first implementations is focused on tracking the position of users within the room so that position-dependent-user interaction with the system may be possible; - The users are supposed to move freely within the room while they interact with the system. To do so, tracking user position is important to identify how and which users are interacting through speech or gesture commands; - Examples of projects: [LEM].
Real-time relative positioning system	- People or object localization is important in a given number of scenarios and applications technologies using GPS have existed from some time now but most of the solutions only work in outdoor scenarios; - Localization indoors involves many more difficulties and represents an unsolved problem in many cases, especially when relative positioning to others and to objects is required while in movement; - This WSN could do measures regarding the distance between team members and a calculation of their relative positions could be achieved; - Examples of projects: [JKLK08].

Table B.6: WSN applications areas description for Category 1 WSNs (cont.).

Area	Description
Wild life monitoring	- Hogthrob application aims at monitoring sensor-wearing sows. A new law requires pregnant sows to move freely in a large pen; - Sows are nowadays equipped with RFID tags. The farmer needs to use a tag reader (possibly physically applied to the RFID tag) to identify the sows; - This solution is not practical in large agricultural facilities. A sensor node with an integrated radio placed on each sow could transmit the sow identification to the farmer's handheld PC, thus alleviating the need for a tag reader; - Software running on the sensor nodes could also alert the farmer to a sow entering its heat period; - Examples of projects: [JOW⁺02, Hog, Lor04].
Transportation Applications	- WSN applications for this class aim to provide people with more comfortable and safer transportation conditions; - The nature of transportation system starts from being ad hoc, hence infrastructure-less and mobile. One vital issue for those mobile components is localization; - These applications are highly required to run in real time, therefore, the synchronization of the components and the end-to-end delay of the whole system is quite critical for such systems; - The Smart Roads project is a traffic project which aims to the implementation of an intelligent communication infrastructure based on WSNs; - This WSN would provide to all vehicles, persons and other objects located on or near a road, the necessary information needed to make traffic safer; - In addition, all road users should be provided with an accurate positioning device; - CORTEX project is a system that automatically select the optimal route according to desired time for reaching the destination, distance, current and predicted traffic, weather conditions, and any other information that will be necessary for the purpose; - In this WSN, cars cooperate with each other to move safely on the road, reducing traffic conditions and reach their destinations. Cars control their speed if there are some obstacles or if they are approaching other cars, and speed up if there are no cars or obstacles; - Cars automatically obey traffic lights. The main purpose of this application scenario is to present the sentient object paradigm for real-time and ad hoc environments. It needs decentralized (distributed) algorithms; - Examples of projects:[Mar04, Ast, ESVS⁺09, SBF⁺04].

Table B.7: WSN applications areas description for Category 2 WSNs.

Area	Description
Home Control	- Home control applications using WSNs provide control, conservation, convenience, and safety, as follows; - Sensing applications facilitate flexible management of lighting, heating, and cooling systems from anywhere in the home, as well as automate control of multiple home systems to improve conservation, convenience, and safety and can capture highly detailed electric, water, and gas utility usage data; - Besides, using embedded intelligence will allow for optimizing the consumption of natural resources; - The use of specific sensors enables the monitoring of a wide variety of conditions. The installation, upgrading, and networking of a home control system without wires will enable one to configure and run multiple systems from a single remote control; - Body-worn medical sensors e.g., heartbeat sensors, are also emerging. Home-resident elderly or people with other medical conditions could wear this kind of sensors; - Examples of projects:[FFR09].
Building Automation	- Wireless lighting control can easily be accomplished with C2WSNs in general, e.g., dimmable ballasts, controllable light switches, customizable lighting schemes, energy savings on bright days; - Energy is a major operating expense for a hotel, and centralized Heating, Ventilating, and Air Conditioning (HVAC) management allow hotel operators to make sure that empty rooms are not cooled. Quality management and building automation applications are another application for C2WSNs which provide control, conservation, flexibility, and safety, as follows; - Sensing applications automate control of multiple systems to improve conservation, flexibility, and security. Sensing applications enable one to network and integrate data from multiple access control points and in some situations will enable one to deploy wireless monitoring networks to enhance perimeter protection; - A WSN used for building energy monitoring and control can improve living conditions for the building's occupants, resulting in improved thermal comfort, improved air quality, health, safety, and productivity; at the same time, it can reduce the energy budget needed to conditioning the space; - Examples of projects:[PWVW08].
Commercial Spaces Application	- This type of WSN application is very useful for a person that wants to go shopping and as this customer enters in the store the intelligent shopping application starts; - The shopping list she made during the previous days is uploaded and displayed on the terminal; - The system guides the customer through the store and helps to locate the products. The check out and payment are automatic, therefore avoiding the lengthy queues at the checkout point; - Examples of projects: [TIB11].

Table B.8: WSN applications areas description for Category 2 WSNs (cont.).

Area	Description
Smart Factory Application	- Industrial automation applications provide control, conservation, efficiency, and safety; - Using WSNs in industry will extend existing manufacturing and process control systems reliably, improve asset management by continuous monitoring of critical equipment and reduce energy costs through optimized manufacturing processes; - Besides, it will help identify inefficient operation or poorly performing equipment, help automate data acquisition from remote sensors in order to reduce user intervention and help deploy monitoring networks to enhance employee and public safety; - In a smart factory application the maintenance of equipment and quality control in a factory is performed by using WSNs; - The sensors are installed on the machines and take data about temperature, humidity, vibrations, lubrication, moisture sensors and other relevant parameters of the machines; - Each sensor node is able to communicate its observations through other nodes to the gateway destination where data from the network is gathered and processed. The remote monitoring, remote control, and data exchange is also enabled. In this kind of factories many alerts could be sent to the factory manager even if he (or she) is not present at the factory, sending all the necessary information to his (or her) PDA; - Examples of projects:[WLH⁺08].
Pre-Hospitalar Application (Emergency response)	- These WSNs are applied in the patients composing a WBAN; - This WBAN, connects to a gateway installed for example in the ambulance and this gateway is connected to the nearest hospital using other type of communication, e.g. UMTS; - An example of this type of WSN application is the CodeBlue project; - All the data collected by the WBAN is sent to the gateway and the gateway forward the data to the nearest hospital in order to the medical personal knows what is the condition of the patient that is being delivered to the hospital; - Other practical example is the acute patient monitoring, where a patient is sent to home but it is monitored by a system composed by a mobile phone and various physiological sensors; - The sensors from the WBAN are able to communicate attained data to the phone and the phone will process this sensor information; - In case of a dangerous change in echocardiogram (ECG) or breathing rate, an alarm will be sent to the hospital and from there to the on-duty physician's handheld device, and the hospital will get back to the patient by phone to make sure it is not a false alarm; - Examples of projects:[LMFJ⁺04].
In-Hospital Emergency (Care Application)	- In this type of application, these WSNs are applied in patients that are in the hospital by the way of Body Area Network (BAN); - These WBANs communicate with gateways installed in the hospital, sending the data from the personal WBAN to the gateway. The patient data sent is recorded in database and this information can be seen by the medical personal, using for example a PDA or a laptop, accessing to the clinical history of the patient or interfacing directly with the personal WBAN of a patient with a PDA; - The sensors used are the same as in the pre-hospitalar application; - The patient data from the BAN should be sent in real time and with a secure communication. The sensors could be programmed to process the vital signs, and for example triggering an alert signal when a physiological sign goes out of normal scale. This alert can be sent do the PDA from the medical personnel; - Examples of projects:[KLC⁺10].

Table B.9: WSN applications areas description for Category 2 WSNs (cont.).

Area	Description
Patient (Tele)Rehabilitation Application	- Previous efforts on telemedicine management have focused on medical care for rural populations, however urban communities will benefit significantly from advances in wireless network design and management; - Within the domain of occupational and physical therapy, known as “telerehabilitation”, expected active benefits to urban communities include greater adherence to rehabilitation protocol due to ease of use and removal of the travel requirement for multiple weekly trips to clinical site and clinical appointments; - Often, these systems provide video-conferencing to rural patients, who permit patients to receive the attention of occupational therapists and medical specialists, which might not otherwise be available; - Wireless sensing network can be used in the form of a therapeutic cover on the injured limb, with Velcro closures to hold the cover in place on the rehabilitation patient body. As the patient executes the recommended series of movements, which are prescribed to be repeated from three to four days a week, up to four times a day, for a series of repetitions, data from the sensors as to the commencement of movement, the angle of movement, which can be calculated in relation to other sensors, and the duration of the movement, can be reported and recorded for later review by the rehabilitation specialist. - This data, collected through active sensor monitoring, would provide a better understanding of the rehabilitation patient adherence to the rehabilitation protocol and the effectiveness of the prescribed treatment; - Examples of projects:[IKKV08].
Telemedicine Application	- Telemedicine refers to “the use of medical information exchanged from one site to another via electronic communications for the health and education of the patient or health care provider and for the purpose of improving patient care”; - The integration of telemedicine with medical micro sensor technology Mobile Sensor Networks for Telemedicine (MSNT) applications provides a promising approach to improve the quality of people’s lives; - This type of network can truly implement the goal of providing health-care services anytime and anywhere. Telemedicine application using WSNs leads to the utilization of different assets independent of their geographical location, multidisciplinary collaboration, facilitates the dissemination of medical knowledge to practicing doctors and medical students and allows doctors in remote and rural areas to consult with specialists in urban areas; - There are two broad categories of healthcare applications. There are those that are specific to medical data and those of general purpose, but used in a medical environment, also known as healthcare informatics; - Medical data healthcare applications are usually specific to the medical device that collects or generates medical data. such has blood pressure, temperature and infusion devices; - Patient records, Internet access, and other administration information are considered healthcare informatics, since they are similar to general applications such as database manipulation; - However, in some of these cases, there may be additional application requirements, such as whether the remote control was used during a critical operation or for the delivery of the dosage of a medication; - One of the main advantages of using wireless technologies in healthcare environments is to enable devices to move; - But there is the need for careful analysis of the trade-offs associated with using wireless networks in healthcare environments. The obvious benefits introduced by wireless technologies in terms of eliminating cumbersome wires, enabling mobility, and facilitating cheaper deployment should always be evaluated against potential side effects, including interference and deployment management; - Examples of projects:[ZC05].

Table B.10: WSN applications areas description for Category 2 WSNs (cont.).

Area	Description
Personal Coaching Application	- Personal coaching addresses self-improvement; - The application of WSNs to this kind of application enables the users to get information and advice about the subconscious aspects of his/her own behaviour; - The physiological parameters and gestures are monitored constantly. Then these data are loaded up to a server and stored there together with his time schedule information and all data are analyzed and mapped to make inferences concerning unwanted behaviour during certain situations; - At the end of each week, the system provides with a report to the person that requested the service. This way he can see how his behaviour and mood varies with the situation or people involved; - Other scenario is the danger warning application where alert messages are sent to the required service providers when the user feels he/she is in a dangerous and urgent situation in order to ensure a mobile security monitoring; - A good situation to see these type of WSNs in action is when a person is alone in the train and in one of the stops enters a frightening person that starts shouting and behaving erratically. The person is so terrified that she cannot use her phone to ring somebody, but the Body Sensor Network (BSN) detects her fear and instructs her mobile phone (acting as a gateway) to send a message to the security officers located at the next train stop; - Examples of projects:[e-S].
Entertainment Applications	- WSNs applied to the entertainment provides a wide range of heterogeneous services for leisure activities in order to improve the respective situations for the users; - In this scenario, the application enables the manager of entertainment establishments to promptly adapt the ambiance and animation according to the permanent monitoring of the audience mood; - Personalized additional services are offered to the persons that are using the space based on the person's experiences. Other ambient adjustments to room temperature and noise level can be made automatically by the space system, based on current user perception; - In the gaming applications the BSN enables the user to project himself into the virtual world of the game and to meet virtual characters that are also animated by online friends; - Their virtual experience corresponds accurately to their gesture and mood variations. She has created a character named Elea who evolves in a virtual world in this role-playing game; - Examples of projects:[MGN⁺05].
Smart Office Applications	- In this type of WSN application, it is considered an area covered by some indoor UMTS stations, and the employees are working in the offices carrying UMTS mobile devices also equipped with ZigBee air interfaces. These mobile terminals can interact with ZigBee-enabled small devices distributed over the corridors and inside the offices; - These devices might provide localization and logistic information, and are able to detect the presence in the neighbourhood of objects such as laptops, printers, pieces of equipment; - The use of ZigBee technology in these devices, allow to the devices communicate with the nodes distributed in the environment, being more easy to interact with all the electronic equipments present in the office; - In this scenario, every employee can scan the environment to get the information on the localization of movable objects. This can also be done through web services implemented in the intranet serving the building; - Examples of projects:[RML05].
Sports Application	- In this type of applications the main objective is the sports activity monitoring of the athletes in indoor and outdoor environments. Moreover, the design and development of support instrumentation to clinical interventions for rehabilitations of neuro-muscular and muscular-skeletal functions due to traumatic injuries happened during some sports activity or due to cardiac stroke, or even from the neurologic forum is also envisaged by some recent projects; - Besides the vital signs monitoring other objective of these type of applications is the biomechanical analysis of the human movement. Since the methods normally used are still limited due to the laboratory conditions (imposed by the amplitude and freedom of the movements and by the portability of the systems), the use of WSNs in this cases is beneficial; - Examples of projects:[KGG⁺09].

B.2 Tables for WSN applications taxonomy

The remaining taxonomy tables for the militar, civil engineering, environmental monitoring, logistics, position & animals tracking, transportation, automobile, sensor & robots, reconfigurable WSN, industrial automation, health and mood-based services, entertainment and smart office applications are presented in this section of Appendix B.

Table B.11: Service, traffic, communication, service components, network and node characteristics of metropolitan operation applications.

	Parameters			Applications	
				Sensys's Project	Traffic Dot
Service	Delivery requirements			RT & NRT	RT & NRT
	Directionality			Bid	Bid
	Communication symmetry			Sym	Sym
	End-to-end connection			Non end-to-end	Non end-to-end
	Interactivity			Interactive	Interactive
	Delay tolerance			Non delay tolerant	Non delay tolerant
	Criticality			Mission critical	Mission critical
Traffic	QoS			Collective QoS (Event-driven)	Collective QoS (Event-driven)
	Bit rate (kbps)			250	40-50
	Latency			T_{min} =125 ms (48 nodes) T_{max} =6 s (2340 nodes)	T_{min} =1 s (20 nodes) T_{max} =2 s (60 nodes)
Commun.	Synchronization			Sync	Sync
	Class of service			ISO&RT-VBR	ISO&RT-VBR
	Traffic classes			RT&LT&Data	RT&LT&Data
	Modulation			FSK(DSSS)	FSK(DSSS)
	Communication direction			Half-duplex	Half-duplex
Serv. comp.	Service components	Voice	VOI	—	—
			AMB	—	—
		Video	STV	✓	—
		Data	LOD	✓	N.A.
			MED	✓	N.A.
		HID	✓	N.A.	
	Acquisition & dissemination classes			Event-driven	Event-driven
Packet delivery failure ratio			1%	5%	
Network	Lifetime (h)			70090-96360	26400-28800
	Scalability			2340 nodes	60 nodes
	Density			N.A.	N.A.
	Sensing range			3.24 m ²	N.A.
	Self-organization			Entire	Entire
	Security			Low	Low
	Addressing			Address-centric: MAC address	Address-centric: MAC address
	Programmability			Not programmable	Not programmable
	Maintainability			Maintainable	Maintainable
	Homogeneity			Heterogeneous	Heterogeneous
	Mobility support			No support	No support
Node	Microprocessor			Coldfire	ATMEL (ATMega 128L)
	Transceiver			CC2420	CC1000
	Overall energy consumption			60 μ A	0.01044 A
	Sampling rate			128 Hz	128 Hz
	Type of function			Sensor & Sink	Sensor & Sink
	Communication range			6.1-7.3 (freeway) 3.1-3.7m (arterial)	5.5 m
	Power supply			Battery	Battery

Table B.12: Service, traffic, communication, service components, network and node characteristics of military applications.

	Parameters			Applications		
				Border monitoring	Surveillance shooter	Condition based monitoring
Service	Delivery requirements	RT			RT& NRT	NRT
	Directionality	Bid			Bid	Bid
	Communication symmetry	Sym			Sym	Sym
	End-to-end connection	End-To-End			End-To-End	End-To-End
	Interactivity	Interactive			Interactive	Interactive
	Delay tolerance	Non-Delay Tolerant			Delay tolerant & Non-delay tolerant	Delay tolerant
	Criticality	Mission critical			Mission critical	Non mission critical
Traffic	QoS	Collective QoS (Event-driven)			Collective QoS (continuous mode)	Collective QoS (Event-driven)
	Bit rate (kbps)	19.2			38.4	35
	Latency	$T_{min} = -$ $T_{max} = 8 \text{ ms}$			$T_{max} = -$ $T_{max} = 2 \text{ s (60 nodes)}$	$T_{max} = -$ $T_{max} = 2.76 \text{ s (318 pkt)}$
Commun.	Synchronization	Sync			Sync	Sync
	Class of service	ISO&RT-VBR			ISO&CBR	ISO&CBR
	Traffic classes	RT&LT&Data			DT&LI&Data	DT&LT&Data
	Modulation	FSK(DSSS)			FSK(DSSS)	DSSS-O-QPSK
	Communication direction	Half-duplex			Half-duplex	Half-duplex
Serv. Comp.	Service components	Voice	VOI	—	—	—
			AMB	—	—	—
		Video	STV	—	—	—
			LOD	✓	N.A.	N.A.
		Data	MED	✓	N.A.	—
			HID	✓	N.A.	—
	Acquisition & dissemination classes	Event-driven			Event-driven	Event-driven
Network	Packet delivery failure ratio	11%			8%	9%
	Lifetime (h)	72000			72 (continuous mode)	1220
	Scalability	1200 nodes			60 nodes	5 nodes
	Density	389 km ²			4 km ²	-
	Sensing range	12 m ²			9 m ²	local
	Self-organization	Partial part of network			Entire	Entire
	Security	Medium			Medium	Low or none
	Addressing	Address-centric: MAC address			Address-centric: MAC address	Address-centric: MAC address
	Programmability	Programmable			Not programmable	Not programmable
	Maintainability	Maintainable			Maintainable	Maintainable
	Homogeneity	Heterogeneous			Heterogeneous	Heterogeneous
	Mobility support	No support			Support	No support
Node	Microprocessor	ATMEL ATMega 128L			ATMEL (ATMega 128L)	TI (MSP430F1611)
	Transceiver	CC1000			CC1000	CC2420
	Overall energy consumption	21.3 mA			110 mA	61.2 mA
	Sampling rate	32 Hz			1 MHz	20 kHz
	Type of function	Sensor & Sink			Sensor & Sink	Sensor & Sink
	Communication range	8 m			10 m	10 m
	Power supply	Battery			Battery	Battery

Table B.13: Service, traffic, communication, service components, network and node characteristics of civil engineering applications.

	Parameters			Applications Structural Integrity monitoring	
Service	Delivery requirements			RT	
	Directionality			Bid	
	Communication symmetry			Sym	
	End-to-end connection			Non end-to-end	
	Interactivity			Interactive	
	Delay tolerance			Delay tolerant	
	Criticality			Mission critical	
Traffic	QoS			Collective QoS (Event-driven)	
	Bit rate (kbps)			25	
	Latency			T _{min} =400 ms	
				T _{max} =1500 ms	
Commun.	Synchronization			Async	
	Class of service			ISO&RT-VBR	
	Traffic classes			RT&LT&Data	
	Modulation			FSK(DSSS)	
	Communication direction			Half-duplex	
	Serv. Comp.	Service components	Voice	VOI	—
AMB				—	
Video			STV	—	
			LOD	-	
Data			MED	-	
			HID	✓	
Acquisition & dissemination classes			Event-driven & Time-driven		
Packet delivery failure ratio			-		
Network	Lifetime (h)			26280	
	Scalability			-	
	Density			-	
	Sensing range			10 - 52 m ²	
	Self-organization			Entire	
	Security			Low	
	Addressing			Address-centric: MAC address	
	Programmability			Programmable	
	Maintainability			Maintainable	
	Homogeneity			Heterogeneous	
	Mobility support			No support	
Node	Microprocessor			TI DSP 8-bit processor	
	Transceiver			CC2420	
	Overall energy consumption			53.167 mA	
	Sampling rate			2 - 100 kHz	
	Type of function			Sensor & Sink	
	Communication range			10 - 30m	
	Power supply			Battery	

Table B.14: Service, traffic, communication, service components of environmental monitoring applications.

Parameters		Applications				
		Monitoring volcanic eruptions	Habitat monitoring	Water monitoring	Weather monitoring	Precision agriculture
Service	Delivery requirements	RT	RT	NRT	NRT	RT
	Directionality	Bid	Bid	Bid	Bid	Bid
	Communication symmetry	Sym	Sym	Asym	Sym	Asym
	End-to-end connection	Non end-to-end	End-to-end	Non end-to-end & end-to-end	Non end-to-end	Non end-to-end
	Interactivity	Interactive	Interactive	Non interactive	Interactive	Interactive
	Delay tolerance	Non delay tolerant	Delay tolerant	Delay tolerant	Delay tolerant	Delay tolerant
Traffic	Criticality	Mission critical	Mission critical	Mission critical	Mission critical	Mission critical
	QoS	Collective QoS (Event-driven)	Collective QoS (Event-driven) or Hybrid	Collective QoS (QoS driven)	Collective QoS (Query driven)	Collective QoS (Query driven & Event driven)
	Bit rate (kbps)	< 34	40	250	5	50
	Latency	$T_{max}=63$ s (per radio hop)	$T_{min}=-$	$T_{min}=-$	$T_{min}=-$	$T_{min}=-$
	Synchronization	Sync	Sync	Sync	Sync	Sync
	Class of service	ISO&CBR	ISO&CBR	ISO&CBR	ISO&CBR	ISO&CBR
Comm. Comp.	Traffic classes	DT&LT&Data	DT&LT&Data	DT&LT&Data	DT&LT&Data	DT&LT&Data
	Modulation	FSK	On-off keying/ASK	FSK	FSK	FSK
	Communication direction	Half-duplex	Half-duplex	Half-duplex	Half-duplex	Half-duplex
	Service components	VOI	-	-	-	-
		AMB	-	-	-	-
		STV	-	-	-	-
		LOD	-	✓	✓	✓
		MED	-	-	-	-
Serv. Comp.	Acquisition & dissemination classes	✓	✓	-	-	-
	Packet delivery failure ratio	Demand-driven & Event-driven 1.46 - 4.96%	Demand-driven & Time-driven	Time-driven	Time-driven	Demand-driven & Time-driven 5.2%
			-	-	-	-

Table B. 15: Network and node characteristics of environmental monitoring applications

Parameters	Applications					
	Monitoring volcanic eruptions	Habitat monitoring	Water monitoring	Weather monitoring	Precision agriculture	Forest fire detection
Network	Lifetime (h)	168	5208	168	1680	-
	Scalability	11 nodes	33 nodes	65 nodes	9 nodes	11 nodes
	Density	3 Km ²	8250 m ²	1 Km ²	1256.6 m ²	N.A.
	Sensing range	-	-	local	local	1 m ²
	Self-organization	Entire	No self-organization	Entire	No self-organization	Entire
	Security	Low	Low or none	Low	None	None
	Addressing	Address-centric: MAC address	Address-centric: MAC address	Address-centric: MAC address	Address-centric: node ID	Address-centric: node ID
	Programmability	Not programmable	Not programmable	Programmable	Programmable	Programmable
	Maintainability	Maintainable	Maintainable	Maintainable	Maintainable	Maintainable
	Homogeneity	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous
Node	Mobility support	No support	No support	No support	Support	No support
	Microprocessor	ATMEL (ATMega 128L)	ATMEL (AT91RM9200)	MICROCHIP (PIC16LF876A)	ATMEL (ATMega 128L)	ATMEL (ATMega 128L)
	Transceiver	CC1000	TR1000	Radiometrix BiM2, Tx14	nRF2401	CC1000
	Overall energy consumption	36 mA	0.002976 A	160 mA	30 mA	36 mA
	Sampling rate	102.4 Hz	2-2000 Hz	0.0011 Hz	0.0011 Hz	0.4 Hz
	Type of function	Sensor & Sink	Sensor & Sink	Sensor & Sink	Sensor & Sink & Actuator	Sensor
	Communication range	10.7 m	360 m	N.A.	300 m	Sink + Gateway
	Power supply	Battery	Battery	Solar panel	Solar panel	N.A.
				Battery		Battery
				Solar panel		

Table B.16: Service, traffic, communication, service components, network and node characteristics of logistics applications.

	Parameters		Applications	
			Target Tracking	Warehouse Tracking
Service	Delivery requirements		RT & NRT	RT
	Directionality		Bid	Bid
	Communication symmetry		Sym	Asym
	End-to-end connection		Non end-to-end	Non end-to-end
	Interactivity		Interactive	Interactive
	Delay tolerance		Non delay tolerant	Non delay tolerant
	Criticality		Mission critical	Mission critical
Traffic	QoS		Collective QoS (Event driven)	Collective QoS (Continuous mode)
	Bit rate (kbps)		250	50
	Latency		$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = 10 \text{ ms}$
Commun.	Synchronization		Sync	Sync
	Class of service		ISO&RT-VBR	ISO&CBR
	Traffic classes		RT&LI&Data	DT&LI&Data
	Modulation		DSSS-O-QPSK	GFSK
	Communication direction		Half-duplex	Half-duplex
Serv. Comp.	Service components	Voice	VOI	-
			AMB	-
		Video	STV	-
			LOD	✓
		Data	MED	-
			HID	-
	Acquisition & dissemination classes		Event-driven	Event-driven
Network	Packet delivery failure ratio		1%	5%
	Lifetime (h)		2640	N.A.
	Scalability		564 nodes	21 nodes
	Density		50 Km ²	100 m ²
	Sensing range		200 m ²	N.A.
	Self-organization		Entire	Entire
	Security		None	High
	Addressing		Address-centric: MAC address	Address-centric: Node ID
	Programmability		Programmable	Programmable
	Maintainability		Maintainable	Maintainable
	Homogeneity		Heterogeneous	Heterogeneous
	Mobility support		No support	Support
Node	Microprocessor		TI (MSP430)	TI (MSP430F1611)
	Transceiver		CC2420	nRF905
	Overall energy consumption		35.1 mA	21.5 mA
	Sampling rate		0.001 Hz	0.1 Hz
	Type of function		Sensor & Sink + Gateway	Sensor & Sink
	Communication range		125 m	300 m
	Power supply		Battery Solar panel	Battery

Table B.17: Service, traffic, communication, service components, network and node characteristics of position & animals tracking applications.

	Parameters			Applications		
				Immersive Roam	Real-time relative positioning system	Wild-life tracking
Service	Delivery requirements			RT	RT	RT & NRT
	Directionality			Bid	Bid	Bid
	Communication symmetry			Asym	N.A.	Asym
	End-to-end connection			Non End-To-End	Non End-To-End	End-To-End
	Interactivity			Interactive	Interactive	Interactive
	Delay tolerance			Non-Delay Tolerant	Non-Delay tolerant & Delay tolerant	Delay tolerant
	Criticality			Mission critical	Mission critical	Non mission critical
Traffic	QoS			Collective QoS (Event-driven)	Collective QoS (Query-driven)	Collective QoS (Event-driven)
	Bit rate (kbps)			38.4	250	1000
	Latency			$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = 3 \text{ s}$	$T_{min} = -$ $T_{max} = 3 \text{ ms}$
Commun.	Synchronization			Sync	Sync	Async
	Class of service			ISO&RT-VBR	ISO&RT-VBR	NISO&ABR
	Traffic classes			RT&LI&Data	DT&LI&Data	-
	Modulation			FSK (DSSS)	DSSS-O-QPSK	GSFK
	Communication direction			Half-duplex	Half-duplex	Half-duplex
Serv. Comp.	Service components	Voice	VOI	-	-	-
			AMB	-	-	-
		Video	STV	-	-	-
			LOD	-	-	✓
		Data	MED	-	-	-
			HID	✓	✓	-
	Acquisition & dissemination classes			Event-driven Demand-driven	Time-driven Demand-driven	Event-driven
Packet delivery failure ratio			-	-	-	
Network	Lifetime (h)			744	-	179
	Scalability			51 nodes	4 nodes	3 nodes
	Density			450 m ²	7 m ²	-
	Sensing range			2 m	1 m	local
	Self-organization			Entire	Entire	Entire
	Security			Medium	Medium	Low or none
	Addressing			Address-centric: Node ID	Address-centric: Output TAG	Address-centric: MAC address
	Programmability			Programmable	Not programmable	Not programmable
	Maintainability			Not Maintainable	Maintainable	Maintainable
Node	Homogeneity			Heterogeneous	Heterogeneous	Heterogeneous
	Mobility support			Support	Support	Support
	Microprocessor			ATMEL ATMega 128L	ATMEL (ATMega 128L)	ATMEL (ATMega 128L)
	Transceiver			CC1000	CC2420	nRF2401
	Overall energy consumption			0.0526A	0.05512 A	38 mA
	Sampling rate			16 KHz	0.2 Hz	10 KHz
	Type of function			Sensor & Sink	Sensor & Sink	Sensor & Sink
Communication range			305 m	75-100 m	220 m	
Power supply			Battery	Battery	Battery	

Table B.18: Service, traffic, communication, service components, network and node characteristics of transportation applications.

	Parameters		Applications
			Smart Roads
Service	Delivery requirements		RT & NRT
	Directionality		Bid
	Communication symmetry		Sym
	End-to-end connection		Non end-to-end
	Interactivity		Interactive
	Delay tolerance		Non delay tolerant
	Criticality		Mission critical
Traffic	QoS	Collective QoS (continuous) & Individual specific	
	Bit rate (kbps)	38.4	
	Latency	$T_{min} = -$ $T_{max} = 130289.73 \text{ ms}$	
Communication	Synchronization	Sync	
	Class of service	ISO&RT-VBR	
	Traffic classes	RT&LT&Data	
	Modulation	FSK(DSSS)	
	Communication direction	Half-duplex	
Serv. Comp.	Service components	Voice	VOI
			AMB
		Video	STV
			LOD
		Data	MED
			HID
	Acquisition & dissemination classes	Event-driven	
Network	Packet delivery failure ratio	0.1%	
	Lifetime (h)	N.A.	
	Scalability	50 nodes	
	Density	N.A.	
	Sensing range	N.A.	
	Self-organization	Entire	
	Security	None	
	Addressing	Address-centric: Node ID	
	Programmability	Programmable	
	Maintainability	Maintainable	
	Homogeneity	Heterogeneous	
	Mobility support	No support	
Node	Microprocessor	ATMEL (ATMega 128L)	
	Transceiver	CC1000	
	Overall energy consumption	0.045 mA	
	Sampling rate	N.A.	
	Type of function	Sensor & Sink & Actuator	
	Communication range	305 m	
	Power supply	Battery	

Table B.19: Service, traffic, communication, service components, network and node characteristics of automobile, sensor & robots, reconfigurable WSN applications.

	Parameters			Applications		
				Automobile	Sensor & Robots	Reconfigurable WSN
Service	Delivery requirements			RT	NRT	NRT
	Directionality			Bid	Bid	Bid
	Communication symmetry			Sym	Sym	N.A.
	End-to-end connection			Non End-To-End	Non End-To-End	End-To-End
	Interactivity			Non Interactive	Interactive	Interactive
	Delay tolerance			Delay Tolerant	Delay tolerant	Delay tolerant
	Criticality			Mission critical	Non Mission critical	Mission critical
Traffic	QoS			Hybrid model	Collective QoS (Event-driven)	Collective QoS (Query-driven)
	Bit rate (kbps)			38.4	19.2	64
	Latency			$T_{min} = -$ $T_{max} = 2.9 \text{ s}$	$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = -$
Commun.	Synchronization			Sync	Sync	Sync
	Class of service			ISO&CBR	NISO&UBR	ISO&CBR
	Traffic classes			DT&LI&Data	-	DT&LT&Data
	Modulation			FSK (DSSS)	On-Off keying/ASK	FSK
	Communication direction			Half-duplex	Half-duplex	Half-duplex
Serv. Comp.	Service components	Voice	VOI	-	-	-
			AMB	-	-	-
		Video	STV	-	-	-
			LOD	✓	-	-
		Data	MED	-	✓	-
			HID	-	-	✓
	Acquisition & dissemination classes			Event-driven Time-driven	Event-driven Demand-driven	Time-driven Demand-driven
Packet delivery failure ratio			4 %	-	-	
Network	Lifetime (h)			60	15.1	N.A.
	Scalability			9 nodes	21 nodes	200 nodes
	Density			0.17023 m ²	2.9768 m ²	1500 m ²
	Sensing range			1 m	1 m	-
	Self-organization			Entire	Entire	None
	Security			None	None	None
	Addressing			Localized or geographic addressing scheme	Address-centric: Node ID	Address-centric: Node ID
	Programmability			Not programmable	Not programmable	Not programmable
	Maintainability			Maintainable	Maintainable	Not Maintainable
	Homogeneity			Heterogeneous	Heterogeneous	Heterogeneous
	Mobility support			Support	Support	No support
Node	Microprocessor			ATMEL ATMega 128L	ATMEL (ATMega 163 and 8535)	TI (MSP430F1611)
	Transceiver			CC1000	TR1000	TDA5250 & CC2420
	Overall energy consumption			0.0346 A	0.056973 A	19 mA
	Sampling rate			N.A.	40 KHz	$1.11 \times 10^{-3} \text{ Hz}$
	Type of function			Sensor & Sink	Sensor & Sink & Actuator	Sensor & Sink + Gateway
	Communication range			140 m	0.85 m	-
	Power supply			Battery	Battery	Battery

Table B.20: Service, traffic, communication, service components, network and node characteristics of industrial automation applications.

		Parameters	Applications
			Smart Factory
Service	Delivery requirements		RT
	Directionality		Bid
	Communication symmetry		Sym
	End-to-end connection		End-to-end
	Interactivity		Interactive
	Delay tolerance		Delay tolerant
	Criticality		Mission critical
Traffic	QoS		Collective QoS (Event-driven & Query-driven)
	Bit rate (kbps)		4.8
	Latency		$T_{min}=80$ ms $T_{max}=250$ ms
Commun.	Synchronization		Sync
	Class of service		ISO&CBR
	Traffic classes		DT&LI&Data
	Modulation		GFSK or MSK/OOK
	Communication direction		Half-duplex
Serv. Comp.	Service components	Voice	VOI
			AMB
		Video	STV
			-
		Data	LOD
			MED
			HID
	Acquisition & dissemination classes		Event-driven & Time-driven
Network	Packet delivery failure ratio		10%
	Lifetime (h)		30000
	Scalability		407 nodes
	Density		3000 m ²
	Sensing range		1 m
	Self-organization		Entire
	Security		None
	Addressing		Address-centric: Node ID, group ID, cluster ID
	Programmability		Not Programmable
	Maintainability		Maintainable
	Homogeneity		Heterogeneous
	Mobility support		No support
Node	Microprocessor		ATMEL (ATMega 128L)
	Transceiver		CC1000
	Overall energy consumption		0.072503 A
	Sampling rate		200 Hz
	Type of function		Sensor & Sink & Gateway
	Communication range		400 m
	Power supply		Battery

Table B.21: Service, traffic, communication, service components of health and mood-based services applications.

Parameters	Applications			
	Pre-Hospitalar	In-Hospitalar Emergency Care	Telemedicine	(Tele)Rehabilitation
Service	Delivery requirements	RT	RT	RT
	Directionality	Bid	Bid	Bid
	Communication symmetry	Asym	Sym	Sym
	End-to-end connection	End-to-end & Non end-to-end	End-to-end & Non end-to-end	End-to-end
	Interactivity	Interactive	Interactive	Interactive
	Delay tolerance	Non delay tolerant	Non delay tolerant	Non delay tolerant
Traffic	Criticality	Mission critical	Mission critical	Mission critical
	QoS	Collective QoS (Query-driven)	Collective QoS (Event-driven)	Collective QoS (Query driven & Event driven)
	Bit rate (kbps)	120	250	250
	Latency	$T_{min} = 15$ ms	$T_{min} = 7-8$ ms	$T_{min} = 19$ ms
		$T_{max} = 15$ ms	$T_{max} = 7-8$ ms	$T_{max} = 19$ ms
		$T_{min} = 15$ ms	$T_{min} = 7-8$ ms	$T_{min} = 19$ ms
Commun.	Synchronization	Sync	Sync	Sync
	Class of service	ISO&RT-VBR	ISO&CBR	ISO&RT-VBR
	Traffic classes	RT&LL&Data	DT&LL&Data	RT&LL&Data
	Modulation	FSK	DSSS	DSSS-Q-PSK
	Communication direction	Half-duplex	Half-duplex	Half-duplex
Serv. Comp.	VOI	–	–	–
	AMB	–	–	–
	Video	–	–	–
	STV	–	–	–
	LOD	–	–	–
	MED	–	–	–
Acquisition & dissemination classes	HID	–	–	–
		✓	✓	✓
Packet delivery failure ratio	Demand-driven & Event-driven	Demand-driven & Time-driven	Event-driven	Time-driven
	17%	17%	6.3%	55%
				N.A.

Table B.22: Network and node characteristics of health and mood-based services applications.

Parameters	Applications				
	Pre-Hospitalar	In-Hospital Emergency Care	Telemedicine	(Tele)Rehabilitation	Personal Coaching
Lifetime (h)	5	5	N.A.	168	600
Scalability	31 nodes	31 nodes	4 nodes	8 nodes	N.A.
Density	3 hospital floors	3 hospital floors	N.A.	2 m ²	Area house
Sensing range	1 m	1 m	local	1 m	1 m
Self-organization	Entire	Entire	Entire	No self-organization	Entire
Security	None	None	None	None	Medium
Addressing	Address-centric: Node ID	Address-centric: Node ID	Address-centric: Address number	Address-centric: Node ID	Address-centric: User ID & Sensor ID
Programmability	Programmable	Programmable	Not programmable	Not programmable	Not programmable
Maintainability	Not maintainable	Not maintainable	Not maintainable	Maintainable	Maintainable
Homogeneity	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous
Mobility support	Support	Support	Support	No support	Support
Microprocessor	TI (MSP430F1611)	TI (MSP430F1611)	TI (TMS320VC5509A)	TI (MSP430)	ATMEL (ATMega 128L)
Transceiver	CC2420	CC2420	UZ2400	ANTFTR2282	CC2420
Overall energy consumption	31.6 mA	31.6 mA	40.955 mA	1 mA	38 mA
Sampling rate	100-120 Hz	100-120 Hz	256 Hz	16 Hz	4 Hz
Type of function	Sensor & Sink	Sensor & Sink	Sensor & Sink	Sensor & Sink	Sensor & Sink + Gateway
Communication range	20-30m (indoor) 75-100m (outdoor)	20-30m (indoor) 75-100m (outdoor)	100 m	> 5 m	20-30 m
Power supply	Battery	Battery	Battery	Battery	Battery

Table B.23: Service, traffic, communication, service components, network and node characteristics of entertainment applications.

	Parameters			Applications		
				Dynamic Spaces	Gamming	Gesture / body tracking
Service	Delivery requirements			RT	RT	RT
	Directionality			Bid	Bid	Bid
	Communication symmetry			Asym	Sym	Sym
	End-to-end connection			Non End-To-End	End-To-End	End-To-End
	Interactivity			Interactive	Interactive	Interactive
	Delay tolerance			Non-Delay Tolerant	Non-delay tolerant	Non-delay tolerant
	Criticality			Mission critical	Mission critical	Mission critical
Traffic	QoS			Collective QoS (Event-driven)	Collective QoS (Event-driven)	Collective QoS (Query-driven)
	Bit rate (kbps)			1000	76.8	400
	Latency			T_{min} = 200 ms T_{max} = 1000 ms	T_{min} =- T_{max} = -	T_{min} =- T_{max} =-
Commun.	Synchronization			Sync	Async	Sync
	Class of service			ISO&RT-VBR	ISO&RT-VBR	ISO&RT-VBR
	Traffic classes			RT&LT&Data	RT&LT&Data	RT&LT&Data
	Modulation			DSSS-O-QPSK	FSK (DSSS)	GFSK
	Communication direction			Half-duplex	Half-duplex	Half-duplex
Serv. Comp.	Service components	Voice	VOI	—	—	—
			AMB	—	—	—
		Video	STV	√	—	—
			LOD	-	-	-
		Data	MED	-	√	-
			HID	√	-	√
	Acquisition & dissemination classes			Event-driven	Event-driven	Demand-driven
Packet delivery failure ratio			0 %	-	-	
Network	Lifetime (h)			17520	12648	4
	Scalability			43 nodes	11 nodes	13 nodes
	Density			8 story campus building	room area	-
	Sensing range			1 m	1 m	0.16 m ²
	Self-organization			Entire	Ad hoc	Entire
	Security			None	None	None
	Addressing			Address-centric: Node ID	Address-centric: Node ID	Address-centric: Node ID
	Programmability			Not programmable	Not programmable	Not programmable
	Maintainability			Maintainable	Maintainable	Not Maintainable
	Homogeneity			Heterogeneous	Homogeneous	Homogeneous
	Mobility support			Support	Support	Support
Node	Microprocessor			ATMEL ATMega 128L	ATMEL (ATMega 163 and 8535)	TI (MSP430F14x)
	Transceiver			CC2420	CC1000	nRF2401
	Overall energy consumption			0.0432 A	0.0356 A	0.041842 A
	Sampling rate			400 Hz	0.017 - 1.67 Hz	100 Hz
	Type of function			Sensor & Sink	Sensor & Sink	Sensor & Sink
	Communication range			10-12 m	305 m	15 m
	Power supply			Battery	Battery	Battery

Table B.24: Service, traffic, communication, service components of Smart office applications.

	Parameters	Applications			
		Smart Office	Sports	Building Automation	Home Control
Service	Delivery requirements	RT	RT	NRT	RT
	Directionality	Bid	Bid	Bid	Bid
	Communication symmetry	Asym	Asym	Sym	Asym
	End-to-end connection	Non End-To-End	Non End-To-End	Non End-To-End	End-To-End
	Interactivity	Non Interactive	Interactive	Non Interactive	Interactive
Traffic	Delay tolerance	Non delay tolerant	Non delay tolerant	Delay tolerant	Delay tolerant
	Criticality	Mission critical	Non Mission critical	Mission critical	Mission critical
	QoS	Collective QoS (Event-driven)	Collective QoS (Event-driven)	Collective QoS (Event-driven)	Collective QoS (Event driven & Demand-driven)
	Bit rate (kbps)	38.4	1000	100	250
	Latency	$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = -$	$T_{min} = -$ $T_{max} = -$
Commun.	Synchronization	Async	Sync or Async	Sync	Sync
	Class of service	ISO&RT-VBR	ISO&RT-VBR	ISO&CBR	ISO&RT-VBR
	Traffic classes	RT&LT&Data	RT&LT&Data	RT&LT&Data	RT&LT&Data
	Modulation	FSK	DSSS-O-QPS	FSK	DSSS-O-QPSK
	Communication direction	Half-duplex	Half-duplex	Half-duplex	Half-duplex
Serv. Comp.	VOI	-	-	-	✓
	AMB	-	-	-	-
	Video	✓	-	-	✓
	LOD	-	-	-	-
	MED	✓	-	-	-
Acquisition & dissemination classes	HID	-	✓	✓	✓
	Acquisition & dissemination classes	Event-driven	Event-driven	Event-driven Time-driven	Event-driven & Demand-driven
	Packet delivery failure ratio	-	-	6.6%	-

Table B.25: Network and node characteristics of Smart office applications

Parameters	Applications			
	Smart Office	Sports	Building Automation	Home Control
Lifetime (h)	8760	N.A.	N.A.	irrelevant
Scalability	8 nodes	41 nodes	31 nodes	13 nodes
Density	office area	room area	1840 m ²	house
Sensing range	1 m	1 m	1 m	1 m
Self-organization	Entire	Entire	Entire	Entire
Security	None	None	None	None
Addressing	Address-centric: Node ID	Address-centric: Node ID + Serial number	Address-centric: Node ID	Address-centric: Node ID
Programmability	Not programmable	Programmable	Not programmable	Not programmable
Maintainability	Not maintainable	Maintainable	Maintainable	Maintainable
Homogeneity	Heterogeneous	Heterogeneous	Heterogeneous	Heterogeneous
Mobility support	Support	Support	Support	No support
Microprocessor	ATMEL (ATmega 128L)	ATMEL (ATmega 8)	ATMEL (ATmega 1281)	ATMEL (ATmega 128L)
Transceiver	CC1000	CC2420	proprietary	CC2420
Overall energy consumption	61.111 mA	28.9 mA	31 μ Ah	N.A.
Sampling rate	1 Hz	0.5-100 Hz	3.33×10^{-3} Hz	N.A.
Type of function	Sensor & Sink + Gateway	Sensor & Sink	Sensor & Sink & Actuator	Sensor & Sink & Actuator & Gateway
Communication range	305 m	10 m	1300 m	20-30m (indoor) 75-100m (outdoor)
Power supply	Battery	Battery	Battery Solar panel	Battery

Appendix C

Smart-Clothing Description - Other applied solutions

Another belt is based on pressure sensors. It was built up with conductive and semi-conductive fabrics. The pressure sensor belt shown in Figure C.1 is made with two different types of conductive fabrics: one is conductive in the entire surface while the other is conductive only in some zones.

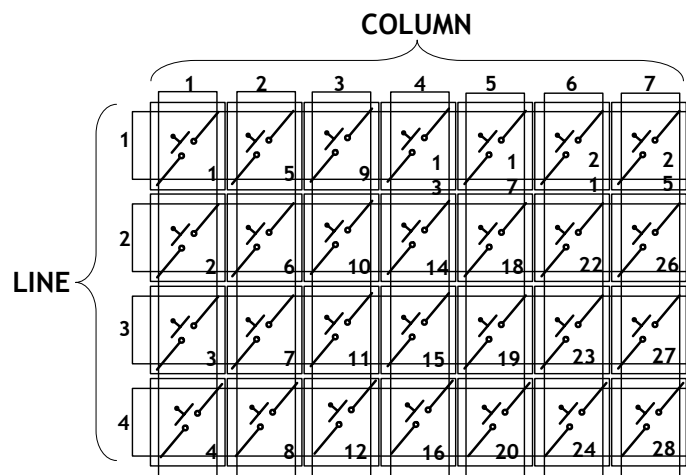


Figure C.1: Smart-Clothing On-Off belt with fabric pressure sensor.

Fabrics are deployed in layers so that the fabric (with square shaped conductive areas) stays between the other layers. This will act as a switch when the outer fabric layers are pressed, letting the current traverse from one to the other, according to the value of its resistance. By observing Figure C.1, while the horizontal stripes are conductive fabric, the vertical stripes are the semi-conductive fabric which forms the switch. The system diagram is presented in Figure C.2, where the lines and columns from the belt are connected to MSP430 based acquisition module.

As presented in Figure C.1 and C.2, the Smart-Clothing On-Off sensor belt is based on a matrix of 28 fabric squares. Each of these fabric square acts like a switch that closes the circuit if it is pressed and leave the circuit open if it is not pressed. Besides the Conductive Fabrics based belt, a button (or a patient counter) was incorporated into the system, to be pressed by the pregnant woman when she feels or detects the foetus moving. These events will be very useful for comparison purposes, as they enable a comparison with the movements detected automatically by the belt. One idea was to connect each individual fabric square (a switch) to the power supply and the other connector of the switch to a port in the acquisition module and detect if there was any signal entering in the port of the microcontroller. This possibility was abandoned due to hardware restrictions. To further develop this idea, twenty eight inputs of the acquisition module would be needed but the chosen microcontroller did not have so many inputs available. To overcome this

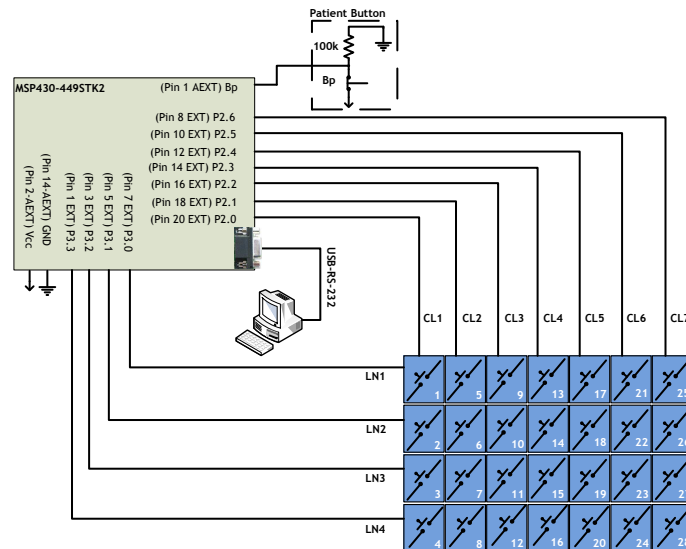


Figure C.2: System diagram for the Conductive Fabrics based belt.

difficulty, the final and definitive proposal to read the switches was to connect the seven columns and the four lines to input/output ports.

The algorithm to scan all the switches uses only eleven ports and has the following sequence:

1. It places a signal at the first column and reads if there is any signal at the first line;
2. It places a signal at the first line and reads the first column to detect any signal;
3. It puts a signal at the first column and reads if there is any signal at the second line;
4. It feeds a signal at the second line and reads if there is any signal at the first column;
5. A signal is applied at the first column and the algorithm reads if there is any signal at the third line;
6. It places a signal at the third line and reads if there is any signal at the first column;
7. It places a signal at the first column and reads if there is any signal at the fourth line;
8. It puts a signal at the fourth line and read if there is any signal at the first column.

When it reaches the last line verification for a column it checks if the patient pressed the button. The procedure for the other columns is the same. The data packet is built and sent to the computer when these iterations are finished for all the switches from the last column.

Some tests have been made with this belt in a pregnant woman and the results have shown that the belt was too sensitive to allow for a discrimination of movements. The belt detected some foetal movements but it was quite difficult to understand if the detection was due to a foetus movement or to the woman movement.

Note that the conductive fabrics from the Conductive Fabrics based belt may be washed after disconnecting all the electronics associated to the belt.

Appendix D

Description of the INSYSM Project

The authors from [CDLNL06] studied the performance of a fibre-optic sensor for monitoring cracks of concrete, masonry and bituminous elements. The proposed sensor does not require prior knowledge of the locations of cracks, which is significantly advanced over existing crack monitoring techniques. Moreover, according to the authors, several cracks can be detected, located and monitored using a single fibre. In [DF09] the authors developed an integrated cost-effective sensor system to monitor the state of reinforced concrete structures from the corrosion point of view. The sensor provides measurements of the open circuit potential of rebars, corrosion current density of rebars, electrical resistivity of concrete, availability of oxygen, chloride ions concentration in the concrete, and temperature inside the structure [DF09]. Insertion of small sensors inside or at the surface of the concrete can be considered as one of the most promising development in order to monitor the long-term behaviour of concrete structures. Corrosion monitoring is possible using different sensors and methods that can work in the alkaline media of concrete for several years. Recorded data for corrosion potential and electrical concrete resistance obtained in real structures exposed to the environment can be used to determine the corrosion rate that corresponds to the concrete structure [MA09]. Embedded sensors in the concrete near the surface (depth of 50 mm) enable measurements of the spatial and temporal distribution of the electrical characteristics within the cover-zone. Thereby it allows for an integrated assessment of its performance. Regular monitoring can enable cover-zone response to different ambient environments, namely changes in the temperature [MCS⁺10]. Advances in the study of concrete deterioration can be achieved if concrete technologists cooperate with scientists in the relevant sensor sciences, to take advantage of the development of wireless low power smart sensor nodes capable of measuring behaviour, filtering, sharing and combining readings from a large variety of sensors. Key issues are calibration of embedded sensors, robustness of sensors cast into concrete elements and durability of sensors in relation to the long life required for the structures [Bue11]. Resulting from cross-disciplinary research between civil engineering and automatic control engineering, a new measurement technique was recently developed that enables direct, real-time measurements and continuous monitoring of concrete internal temperature and humidity via wireless signal transmission. The results are very promising with temperature/humidity sensors which monitor the internal temperature and humidity of concrete wirelessly, directly, in real-time, and continuously. However, several limitations need to be overcome when embedding electronic components into concrete, such as the continuity and stability of signal transmission, protection of electronic components, as well as the design of encapsulation boxes [CH12]. In most of the works the temperature and moisture are important parameters. Temperature is an important parameter during the curing and hardening of the concrete, since the concrete cannot be too cold or too hot. When the temperature decreases, the hydration reaction slows down. Hence, if the concrete temperature increases the reaction accelerates, creating an exothermic reaction (which produces heat), causing temperature differentials

within the concrete. This temperature gradient can lead to cracking. Moreover, during the initial phase of the life of the concrete, it is essential to avoid cracking caused by the rapid drying due to increased temperature and the on-going hydration reaction. Both moisture and temperature at specific operational conditions promote concrete deterioration processes namely, occurrence of undesirable cracks, corrosion of the reinforcing steel, ingress of carbon dioxide and other chemical processes. The properties of civil structures involve a significant amount of uncertainties in several parameters, caused by the effects from environmental factors, e.g., temperature and humidity. The deterioration process of the underlying structure is caused by these variations. At earlier ages, temperature and moisture plays an important role during the curing and hardening of the concrete, and can have long-term consequences.

D.1 Negative Temperature Thermistor Specification and Results

The first set of tests consisted of measuring the temperature with a Negative Temperature Coefficient (NTC) temperature sensor inside a concrete cube (common strength class C25/30, 10 cm length size), as shown in Figure D.1.



Figure D.1: On-going measurement of temperature with wireless sensors inside a concrete cube.

The acquisition system consists of a Sensor Board and an IRIS mote, facilitating the creation of an IEEE 802.15.4 network whose primary function is to remotely collect the data from the NTC sensor inside the concrete cube.

The first experimental approach for reading temperature inside a concrete cube involves the use of a NTC thermistor and an IRIS mote. This setup foresees an automatic wireless monitoring system.

The temperatures inside the concrete cube and environment have been compared. Figure D.2 presents the values obtained for the temperature by the probe and calibrated sensors.

As shown in Figure D.2, there is a difference of 5 °C between the actual and measured temperatures. This is due to some failures during the calibration of the sensor, resulting in inaccurate values. Based on this fact, we can conclude that using a NTC sensor with an “unknown” behaviour is not the most adequate approach to the problem. Besides, this kind of sensor is not able to simultaneously measure temperature and humidity inside the concrete structures.

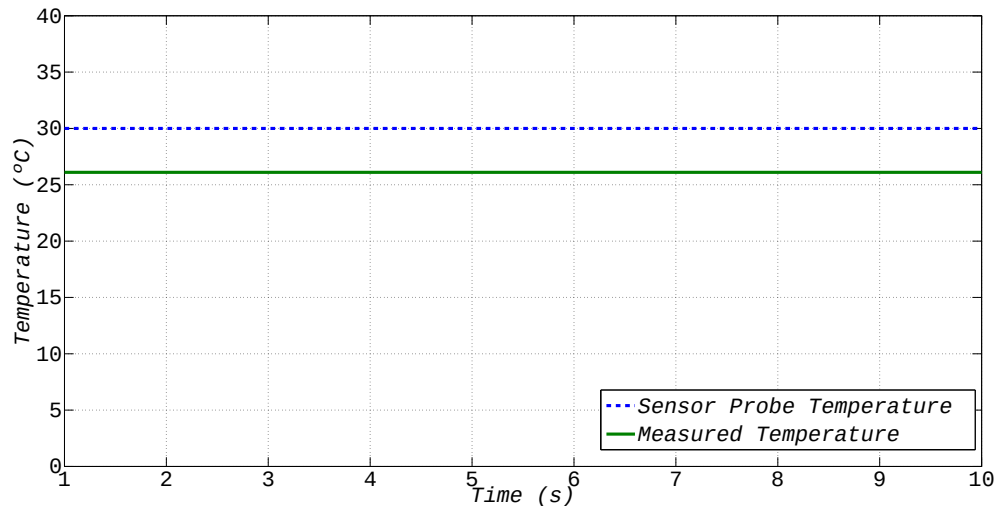


Figure D.2: Verification of the sensor probe and measured temperatures inside the concrete cube by using an NTC temperature sensor.

D.2 SHT21S - Humidity and Temperature Sensor characteristics

The sensor used is the SHT21S [SHT10b] which presents the following features:

- Measurement range: 0-100 % RH;
- Output: SDM/analog Volt interface;
- Temperature operating range: -40 to +125 °C;
- Temperature accuracy: +/- 0.3 °C @ 25 °C;
- Humidity accuracy: +/- 2 % @ 25 °C;
- RH response time: 8 s;
- Energy consumption: 3.2 μ W (at 8 bit, 1 measurement/s).

The SHT21S sensor could be supplied with a maximum voltage of 5 V. The supply voltage of SHT21S must be in the range of 2.1 - 3.6 V (recommended supply voltage is 3.0 V). The interface specifications of SHT21S are described in Table D.1.

Table D.1: SHT21S pin assignment.

Pin	Name	Comment
1	SDA	Data bit-stream
2	VSS	Ground
5	VDD	Supply Voltage
6	SCL	Selector for humidity or temperature
3, 4	NC	Not connected

Power supply pins Supply Voltage (VDD) and Ground (VSS) must be decoupled with a 100 nF capacitor (should be placed closer to the sensor). The SCL is used to select the humidity or the temperature output. When SCL is set as high it yields humidity output, while when SCL is set as low it yields temperature output. The SDA pin provides the Sigma Delta

Modulation (SDM) output. The signal carries humidity or temperature data, depending on SCL being high or low, respectively. SDM is a bit-stream of pulses. The more high pulses the higher the value we obtain in the full measurement range, as presented in Figure D.3.

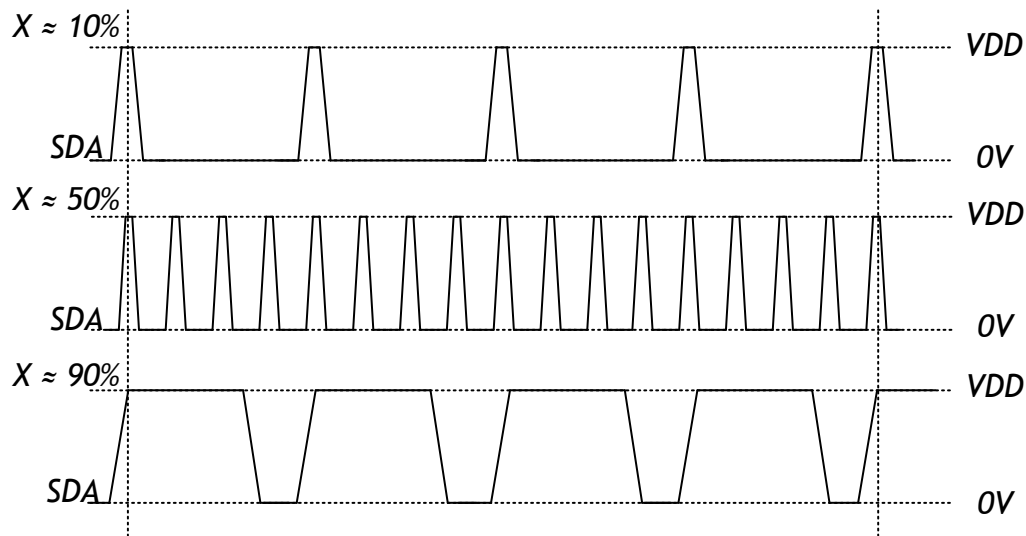


Figure D.3: Schematic principle of SDM signal. X represents either RH or T at different levels of sensor output.

D.3 eZ430-RF2500 kit

The eZ430-RF2500 kit is a complete wireless development tool for the MSP430 and CC2500 that includes all the hardware and software required in order to develop an entire wireless project with the MSP430 in a USB stick. The tool includes a USB-powered emulator to program and debug your application in-system and two 2.4-GHz wireless target boards featuring the highly integrated MSP430F2274 ultra-low-power microcontroller. All the required software is included such as a complete Integrated Development Environment and SimpliciTI, a propriety low-power star network stack. The eZ430-RF2500 is a development kit that leverages the ultra-low power MSP430F2274 microcontroller to control the 2.4GHz CC2500 radio to establish basic wireless networks with minimal power requirements. The two IC's interface via SPI and there is an antenna on-board which allows connectivity with no additional hardware components required. The eZ430-RF2500 uses the SimpliciTI protocol stack, which is aimed at small RF networks. Such networks typically contain battery operated devices which require long battery life, low data rate and low duty cycle and have a limited number of nodes talking directly to each other or through an access point or range extenders. Access point and range extenders are not required but provide extra functionality such as store and forward messages. With SimpliciTI, Texas Instruments claims that the MCU resource requirements are minimal which results in the low system cost. In our work we modified the packet frame of the temperature example source code, which runs in the eZ430-RF2500 modules, in order to send the values for the temperature and humidity.

D.3.1 SHT21S eZ430-RF2500 Acquisition System

We defined has Access Point (AP) the eZ430-RF2500 module that is connected to the computer and the End Device (ED) as the one where the SHT21S sensor is connected. As stated before we modified the packet frame of the temperature example source code in order to include the values of the temperature and humidity of the SHT21S sensor.

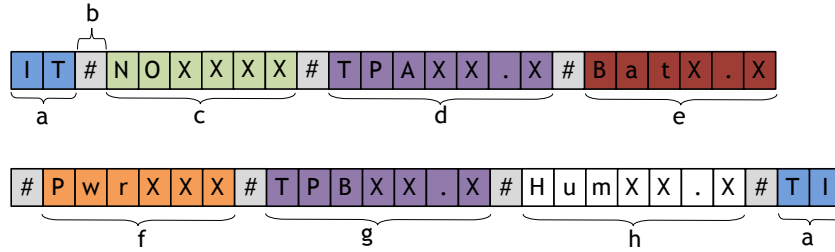


Figure D.4: Frame sent by the ED.

The AP receives the frame and the information is decoded, as presented in Figure D.4. In Figure D.4 the field 'a' represent the initializer and the finalizer of the frame; the field 'b' is the separator character between different fields; field 'c' is the node number; field 'd' is the temperature value of the built in sensor of the microcontroller; field 'e' is the battery voltage; field 'f' is the signal power; field 'g' is the temperature value of the SHT21S sensor; and field 'h' is the humidity value of the SHT21S sensor.

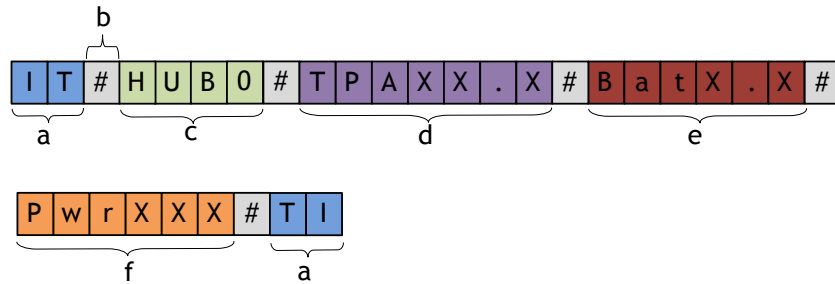


Figure D.5: Frame sent by the AP.

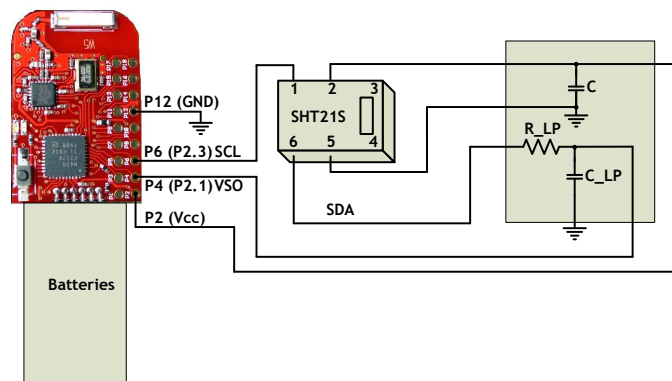


Figure D.6: SHT21S eZ430-RF2500 version acquisition system.

Besides the frame received by the AP from the ED, the AP also generates a frame to be sent by USB to the computer jointly with the frame received from the ED. The frame sent by the AP is presented in Figure D.5. The fields from this frame have all the same meaning as the ones presented in the ED frame, but since our network follows a star-topology, the

AP is unique and therefore it must have an unique ID in the network. Therefore, the frame sent by the AP has the name 'HUB0' in the field 'c'. In Figure D.6 is presented the acquisition system used to read the signal from the SHT21S sensor, compute the values for the temperature and humidity and send them wirelessly to the AP. The ED reports values each minute to the AP, but it can be changed by the user.

Appendix E

Modelling Radio Frequency Propagation in MiXiM Framework

E.1 Mixed Simulator (MiXiM)

The MiXiM [WSKW09] framework is an extension for wireless and mobile networks from the discrete event OMNeT++ [Var10] simulator. This framework is different from the most popular simulators, since it is not limited to a single frequency and a single antenna system. These characteristics, together with a physical layer that offers flexibility to the user, it is very efficient. It can consider single- or multi-frequencies, multiple channels, variable bit rates, Orthogonal Frequency Division Multiplexing (OFDM) systems (e.g., IEEE 802.11a) and Multiple Input Multiple Output (MIMO). Besides all these features, several models can be considered for modelling the wireless channels or even to easily implement new ones. There are path loss models that characterize the variation of the received power with the distance, or models that account for shadowing effects, due to the presence of obstacles such as the log-normal fading. Models that rely on fast fading due to the mobility of nodes, like Rice and Rayleigh fading, are also possible to be used.

E.2 Environmental Models

In MiXiM, the environment of the simulation, where objects and nodes are displaced, is called the playground (it can be either 2 or 3-dimensional) in the simulations. While nodes are the entities with communication capabilities, the objects are entities without any communication capabilities. The objects only affect the signal propagation through the medium where the nodes are placed. Nodes have a position and can be either static or mobile (different mobility patterns can be enabled in MiXiM).

The *ObjectManager* and *ConnectionManager* modules are responsible for the management of all the entities within the playground. The first one manages the objects and their locations within the playground, and can be called to see if a certain connection between two nodes is affected by an object in the middle. The second one, manages and updates all the connectivity information, in terms of the interference range of the nodes. If the *ConnectionManager* module informs that the nodes are mutually interfering with each other, then there is a connection between two nodes. However, it does not mean that they are able to communicate. If the *ObjectManager* module states that the nodes are not connected, then they will not interfere with each other. Therefore, if a node wants to receive a packet from a neighbouring node, it will receive all interfering signals that are in the interfering range and can decide whether it receives (or not) correctly the desired packet, based on the interference level and SNR.

E.3 Propagation Models

The electromagnetic wave propagation is related with several factors that affect it, such as the refraction, diffraction, and scattering. Since the radio frequency communication among sensor nodes requires access to the wireless channel, we must be capable to model the channel by means of a numerical analysis. By modelling and understanding the wireless channel we will be able to design, simulate and implement better WSNs.

Propagation models are proposed for a specific environment and protocol, and are generally obtained from empirical results. These models are used to predict the average received signal strength at a given distance from the transmitter node, as well as the signal strength variability for closer distances [Rap01]. Moreover, it is possible to estimate the radio coverage area of a sensor node by using these prediction models.

In the signal propagation through a wireless channel, there is a decrease in the power as the distance increases, referred as *path loss*. The *path loss* (in dB) is defined as the difference between the effective transmitted and received powers. The effect of the antenna gains may or not be included. The *path loss* is defined as in Equation E.1:

$$PL(d) = P_{tx} - P_{rx}(d) \quad (\text{E.1})$$

where PL is the *path loss*, P_{tx} [dB] is the transmitted power, P_{rx} [dB] is the received power, and d [m] is the distance separation between the transmitter and receiver. In the context of logarithmic units, the decibel values can be assumed as “relative” or “absolute”. The path loss is a “relative” decibel value, where the ratio between the transmission and reception powers is specified. An “absolute” decibel value is the one relative to a fixed reference. The values for the transmission and reception powers are referred as “absolute” decibel values, because the power is specified relatively to a reference power of 1 mW (or 1 W). When an “absolute” decibel value is referred to a reference power in mW, the unit is dBm (dBW). A mathematic relation between W and dBW can be achieved by using Equation E.2 or Equation E.3, depending what conversion we envisage.

$$P_{[dBW]} = 10 \times \log_{10}(P_{[W]}) \quad (\text{E.2})$$

$$P_{[W]} = e^{P_{[dB]}/10} \quad (\text{E.3})$$

The *path loss* is associated with the maximum distance between the transmitter and receiver nodes, which is limited by the maximum transmitter power of the sensor node, and by the minimum reception power that can be successfully received and decoded by the sensor node. The maximum transmission power of a wireless device is limited by a hardware parameter that is established by the radio transceiver manufacturer, as well as by the regulatory bodies in each country which guarantee the wireless communication system integrity, product performance, and control the associated health risks.

In Europe, this regulation is performed by the Conference of Postal and Telecommuni-

cations Administrations (CEPT). CEPT provides a high degree of standardization on lower-power radio equipment, while specifying the maximum output power and maximum active duty cycle for different frequency bands [Far08]. Other two parameters related with the *path loss* are the sensitivity and the saturation power in the receiver node. The first one is defined as the lowest received signal power that yields a Packet Error Rate (PER). The second one is defined as the largest signal strength that can be received by the receiver node to achieve a specific performance, with an acceptable BER. By combining the values defined for the maximum output power and receiver sensitivity and by employing the correct equation for the path loss model equation from an appropriate radio frequency propagation model, it is possible to calculate the maximum distance between two sensor nodes.

E.3.1 Friis Free Space Path Loss Model

The Friis free-space propagation equation is derived from Maxwell's equations and describes the receiver power at a distance of $d \geq d_0$ (between the transmitter and receiver nodes). The Friis free-space propagation equation assumes LoS propagation, but it does not consider reflection and obstruction propagation effects [Rap01, KW05]. The Friis free-space propagation equation is given by Equation E.4, in linear units:

$$P_{rx}[W] = \frac{P_{tx}G_{tx}G_{rx}}{L_s} \cdot \left(\frac{\lambda}{4\pi d} \right)^2 \quad (\text{E.4})$$

where G_{tx} and G_{rx} are the transmitter and receiver antenna gains respectively, L_s is the system loss factor (represents losses in the radio transceiver electronics), which is always greater than or equal to unity. By using a 2.4 GHz carrier frequency, L_s is assumed to be equal to unity. The wavelength is given by Equation E.5:

$$\lambda = \frac{c}{f_b} \quad (\text{E.5})$$

where f_b [Hz] is the carrier frequency, and c [m/s] is the speed of light in the vacuum. However, a notation more often used, is the received power expressed in decibel as follows:

$$P_{rx[dBW]} = P_{tx} + G_{tx} + G_{rx} - 20 \log_{10} d + 147.55 - L_s \quad (\text{E.6})$$

By combining Equation E.4 and Equation E.1 the *path loss* due to free-space propagation can be calculated as follows [Rap01, KW05]:

$$PL_{[dB]} = -G_{Tx} - G_{Rx} + 20 \log_{10} d - 147.55 + L_s \quad (\text{E.7})$$

To obtain valid results, a condition must be fulfilled that states that Friis free-space equation is only valid for distances longer than the far-field or Fraunhofer region [Rap01]. This

region is defined as the region beyond the far-field distance d_{fb} , where the transmitter antenna aperture and the carriers wavelength is related to it. The far-field region is the area at which the antenna effects can be neglected, and the propagating electromagnetic field behaviour is similar to an electromagnetic wave [YK06]. The Fraunhofer distance is given by the following equation:

$$d_{fb} = \frac{2D^2}{\lambda}, d_{fb} \gg D, d_{fb} \gg \lambda \quad (\text{E.8})$$

where $D_{[m]}$ is the largest physical linear dimension of the antenna, and $\lambda_{[m]}$ is the wavelength of the electromagnetic wave.

By analyzing Equation E.8, for a certain carrier frequency, the Fraunhofer distance increases quadratically as the antenna dimension increases. This propagation model is too much simplistic to be used when obstructions and reflections effects affect the wave propagation.

E.3.2 Log-distance Path Loss Model

Theoretical and measurement propagation models have shown that the average received signal power decreases logarithmically as the distance increases, whether referring to outdoor or indoor wireless channels [Rap01]. The log-distance model Equation E.9 is one of the most used propagation models, where $\overline{PL}$ is the mean *path loss*, α_{exp} is the path loss exponent, d_0 [m] is the close-in reference distance from near the transmitter antenna, and d [m] is the distance separation between the transmitter and receiver nodes:

$$\overline{PL}(d) \propto \left(\frac{d}{d_0} \right)^n \quad (\text{E.9})$$

Or can be expressed in decibel as in Equation E.10:

$$\overline{PL}(d) = \overline{PL}(d_0) + 10\alpha_{exp} \log_{10} \left(\frac{d}{d_0} \right) \quad (\text{E.10})$$

The $\overline{PL}(d_0)$ is defined as the reference path loss and is obtained from measurements, or by using the Friis free-space equation. The path loss exponent expresses the rate at which the path loss increases with distance. The value of α_{exp} is dependent from the specific propagation environment where the signal is being transmitted. Table E.1 presents typical values for the path loss exponents obtained from empirical results in different propagation environments. The reference distance should always correspond to the far-field of the antenna, so that near-field effects do not change the reference path loss.

E.3.3 Log-normal Shadowing Path Loss Model

The model from Equation E.10 neglects the variations that the surrounding environment adds to the *path loss* between two points. This leads to experimental results, which are

Table E.1: Path loss exponents and standard deviations measurements for different propagation environments and frequencies (adapted from [Rap01]).

Environment		Frequency [MHz]	α_{exp}	σ
Stores	Retail	914	2.2	8.7
	Grocery		1.8	5.2
Office	Hard Partition	1500	3.0	7.0
	Soft Partition	900	2.4	9.6
		1900	2.6	14.1
Factory Line of Sight	Textile/Chemical	1300	2.0	3.0
		4000	2.1	7.0
	Paper/Cereals	1300	1.8	6.0
	Metalworking	1300	1.6	5.8
Factory Obstructed	Textile/Chemical	4000	2.1	9.7
	Metalworking	1300	3.3	6.8

different than the mean *path loss* predicted by Equation E.10. Empirical results have shown that for any value of d , the path loss $PL(d)$ at a certain location will be random and log-normally distributed (in dB) [Rap01].

It is possible to include this shadowing effect in the log-distance path loss propagation model, by adding a shadowing variance, a normally distributed random variable X_σ (in dB) with standard deviation σ (also in dB), as given by Equation E.11:

$$\begin{aligned}
 PL(d)_{[dB]} &= \overline{PL}(d_0) + X_\sigma \\
 &= \overline{PL}(d_0) + 10\alpha_{exp} \log_{10} \left(\frac{d}{d_0} \right) + X_\sigma
 \end{aligned} \tag{E.11}$$

where the average received power, $P_{rx}(d)$, given by Equation E.12, can be calculated by applying Equation E.1:

$$P_{rx}(d)_{[dBm]} = P_{tx}[dBm] - PL(d)[dB] \tag{E.12}$$

In other words, the log-normal shadowing will induce the measured signal levels at a specific location between the transmitter and receiver nodes to have a Gaussian (normal) distribution around a distance which depends on the mean *path loss*.

E.3.4 IEEE 802.15.4 Path Loss Models

The propagation models are obtained by computing measured data, as mentioned before. In WSNs, the IEEE 802.15.4 standard [IEE06] is the most suitable for our evaluations. Two path loss models that apply for the IEEE 802.15.4 standard at 2.4 GHz are described here. A comparison between the theoretical results from the two models is performed. Simulation results are also presented for the normalized DPSR for the free-space and IEEE 802.15.4 propagation models. These IEEE 802.15.4 models are based upon the log-distance path loss propagation model.

E.3.4.1 Path Loss Model 1 (Outdoor)

The IEEE 802.15.4 standard [IEE06] defines a path loss model more suitable for outdoor applications for communications at 2.4 GHz, as follows:

$$PL(d)[dB] = \begin{cases} -G_{tx} - G_{rx} + 40.2 + 20 \log_{10}(d), & 0.5 \text{ m} \leq d \leq 8 \text{ m} \\ -G_{tx} - G_{rx} + 58.5 + 33 \log_{10}\left(\frac{d}{8}\right), & d > 8 \text{ m} \end{cases} \quad (\text{E.13})$$

By analyzing Equation E.13, the minimum distance accountable for this IEEE 802.15.4 propagation model is 0.5 m. For the first eight meters the model follows a free-space path loss model propagation model (by considering the Friis free-space equation). For distances longer than eight meters, a log-distance path loss model with $d_0 = 8 \text{ m}$ and $n = 3.3$ is considered. In this model no log-normal shadowing is assumed.

E.3.4.2 Path Loss Model 2 (Indoor)

Later, the IEEE 802.15.4 working group [MGAL04] announced an indoor propagation model for the IEEE 802.15.4 standard at 2.4 GHz. This model is similar to the outdoor propagation model, since it also considers the free-space propagation model (but only for the first four meters). For distances longer than four meters losses of 0.7 dB/m are added. This indoor propagation model adds the log-normal shadowing with $\sigma = 3 \text{ dB}$ and 9 dB , at 8 m and 100 m , respectively, in both parts of the equation. The path loss propagation model equation for this model is given by Equation E.14:

$$PL(d)[dB] = \begin{cases} -G_{tx} - G_{rx} + 56.2 + 20 \log_{10}(d) + X_\sigma, & 0.5 \text{ m} \leq d \leq 4 \text{ m} \\ -G_{tx} - G_{rx} + 56.2 + 20 \log_{10}(d) + 0.7(d - 4) + X_\sigma, & d > 4 \text{ m} \end{cases} \quad (\text{E.14})$$

In the context of IEEE 802.15.4 standard, in Equation E.15, $\sigma(d)$ as a function of the distance, by using a linear interpolation, as presented in Figure E.1.

$$\sigma(d) = 0.065d + 2.48 \quad (\text{E.15})$$

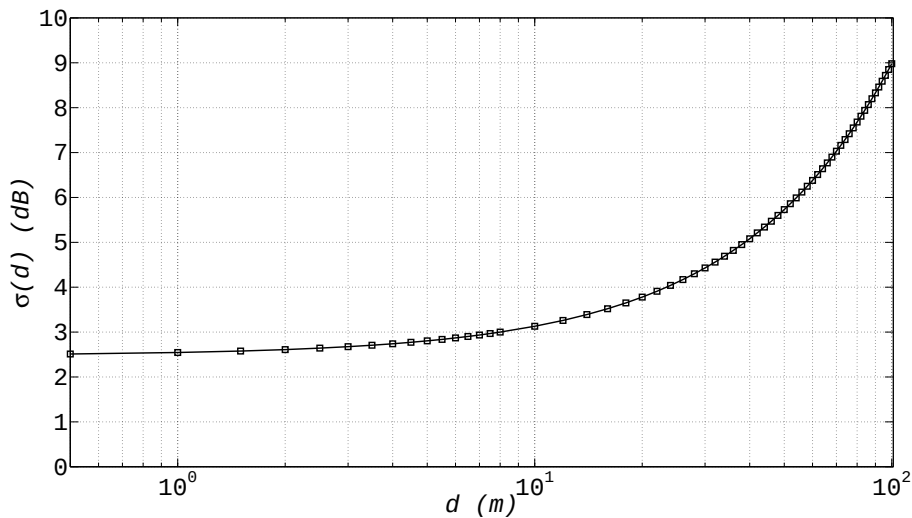


Figure E.1: Linear interpolation for the standard deviation as function of distance.

By observing Figure E.1, as the distance increases the standard deviation also increases. However, between 0.5 and 8 m the slope is lower than the one for distances longer than 8 m.

E.3.4.3 Comparison of the IEEE 802.15.4 Path Loss models

Figure E.2 presents a comparison between the different indoor path loss models when considering σ in function of distance, and when a fixed value of $\sigma = 8$ dB is considered. By analyzing Figure E.2 it is clear that the curves of each of the indoor path loss models are similar. In the MiXiM framework the indoor path loss model, with a fixed value of $\sigma = 8$ dB, is the one that is implemented. Figure E.2 also compares both indoor path loss models for the outdoor path loss model.

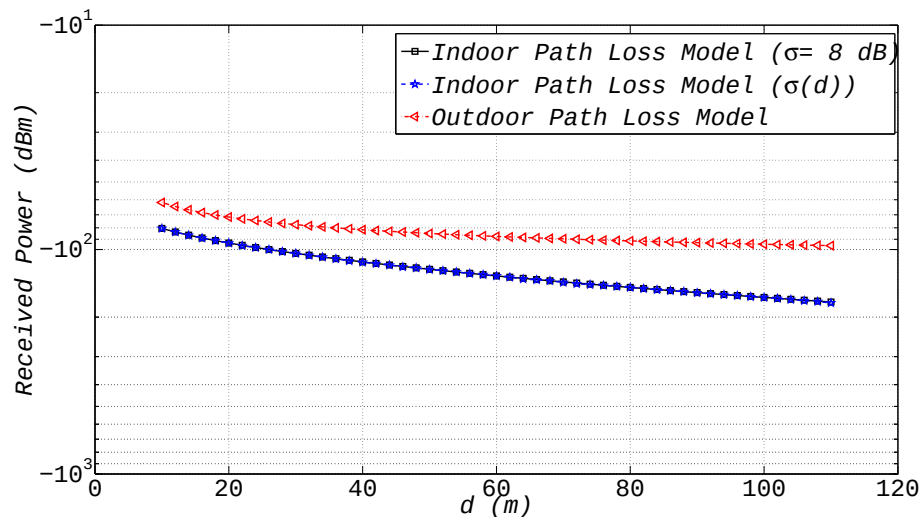


Figure E.2: Comparison of the IEEE 802.15.4 path Loss models as function of distance.

E.3.4.4 Simulation Results for Normalized Data Packet Success Rate under IEEE 802.15.4 Path Loss models

This section presents the results for a set of simulations performed with the Scheduled Channel Polling (SCP) MAC protocol, under the MiXiM Framework simulator. The simulation scenario consists of two sensor nodes, where only one node generates and sends 20 data packets. The distance between the sensor nodes is increased until they stop receiving data packets successfully. Moreover, these simulations are performed for the free-space, outdoor, and indoor propagation models.

By observing Figure E.3, it can be observed that the indoor path loss model is the one that adds more path loss effects to the signal, as the distance separation between the two sensor nodes increases. This effect is noted in the fast decay of the Data Packet Success Rate (DPSR) as distance increases, when compared with the other propagation models. Another important aspect that should be pointed is the presence of the fading effect in the outdoor and indoor path loss models as distance increases. Depending on what propagation model we are dealing with, three areas can be defined in the chart: i) the connected area, where nodes present maximum DPSR, ii) the transitional area, where nodes may lose some data packets receptions, and iii) unconnected area, where nodes do

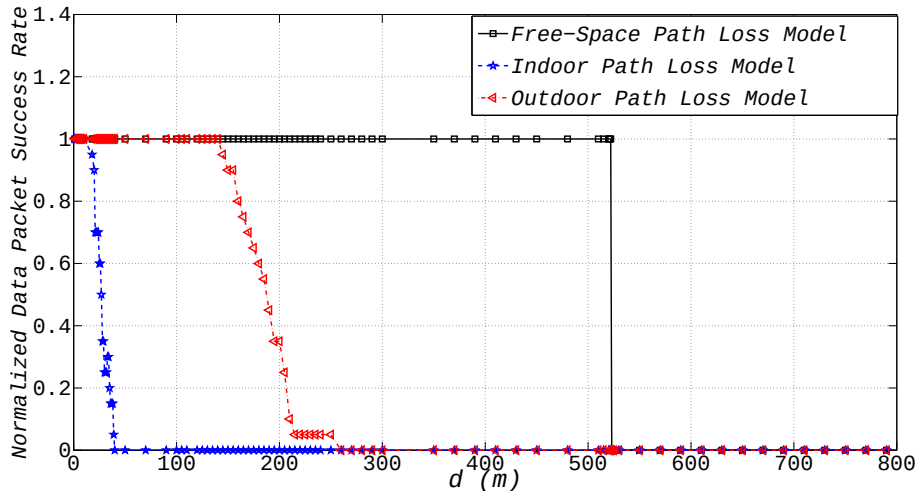


Figure E.3: Normalized data packet success rate as function of distance.

not receive any data packets. For the free-space path loss model, the results show that the DPSR decreases suddenly from a full data packets reception to a zero data packets reception.

E.3.5 IEEE 802.15.6 (draft) Path Loss model (WBAN)

The IEEE 802.15.4 standard [IEE06] has been widely used in several areas (e.g., agriculture, habitat, traffic, and healthcare). However, when researchers have the need to monitor vital signs from a patient, they had to attach the sensor nodes to the patient. While attaching the sensor nodes to the human body, another problem appeared related with the propagation of the signal in the vicinity of the human body. As an answer to this need, the IEEE 802.15.6 working group (related with wireless body area network) was founded, to characterize the electromagnetic wave propagation from devices that are close to or inside the human body. The IEEE 802.15.6 task group is working to provide a new standard for body area networks. However, until February 2012 there has only been a draft version of the IEEE 802.15.6 standard [IEE10]. Now there is a final release of the standard. The complexity of the human tissues structure and body shape make it difficult to obtain a simple path loss model for BAN. Moreover, if the antennas for BAN applications are placed on or inside the body, the BAN channel model needs to take into account the influence of the body on the radio propagation.

Three types of nodes are described in the IEEE 802.15.6 standard as follows:

- **Implant node:** This node is placed inside the human body, and could be immediately below the skin or further deeper, inside the body tissue;
- **Body Surface node:** This node is placed on the surface of the human skin or, at most, two centimetres away from it;
- **External node:** This node is not in contact with human skin (around a few centimetres and up to 5 meters away from the body).

If body surface communications are considered, the distance between the transmitter and receiver nodes should be assumed as the distance around the body, when the transmitter

Table E.2: Path loss coefficients and standard deviations for different propagation environments ([MGAL04]).

Environment	η_1	η_2	σ
Hospital Room	6.6	36.1	3.80
Anechoic Chamber	29.3	-16.8	6.89

and receiver nodes are not placed in the same surface, rather than account the distance as a straight line through the body. This allows accounting for the wave diffraction.

In terms of maximum power limitation for on-body medicals devices it is regulated by the regulatory bodies of each country. In Europe, this regulation is performed by the ETSI, which establishes a maximum output power of 25 μ W ERP. In the United States of America, the FCC and the International Telecommunications Union (ITU-R) are responsible for the regulation of the maximum power consumption. They establish that the output power is set to a maximum of 25 μ W EIRP (which is around 2.2 dB lower than the ERP level).

For our evaluation studies, we are interested in scenarios where the IEEE 802.15.6 devices are operating in a body surface to body surface (LoS and Non-Line-of-Sight(NLoS)) scenario at 2.4 GHz.

Body Surface to Body Surface Scenario

The following path loss model is based on measurements performed under carrier frequencies that vary between 2.4 and 2.5 GHz. The measurement set up, derivation and data analysis can be found in [ATT⁺08]. The path loss model for a body surface scenario is given by Equation E.16:

$$PL(d)[dB] = \eta_1 \log_{10}(d) + \eta_2 + X_\sigma \quad (\text{E.16})$$

The coefficients η_1 and η_2 for the path loss calculation are obtained by the authors from [ATT⁺08] through linear fitting. The distance between the transmitter and receiver nodes should be considered in millimetres, while the X_σ is a normally distributed variable with standard deviation, σ . Table E.2 summarizes the corresponding path loss model parameters for the hospital room and anechoic chamber.

Appendix F

IEEE 802.15.4 PHY Layer

The main purpose of the PHY layer is to establish an interface with the physical medium where the communications are done. The PHY layer is the lowest layer in the WSN protocol stack and it is responsible by the control (enable and disable) of the radio transceiver, energy detection, link quality, CCA, channel selection and the transmission and reception of message packets that are exchanged in physical medium [GCB03].

F.1 IEEE 802.15.4 Country Regulations

The governments or a telecommunications regulatory institute of a country regulates and administer the radio-frequency spectrum. In almost all cases, there are some frequency bands allocations just for unlicensed operation, in order to (the manufacturer can) ensure operation within some pre-established limits in output power, duty cycle, modulation and other parameters. In the case of Europe, Japan, Canada and the United States of America, the regulation consists in unlicensed bands but they are type-approved DSSS services. The IEEE 802.15.4 standard is written so that the conforming devices can be manufactured to operate in any of the three bands. Two of these bands are limited to specific geographical regions, but one band is available for nearly worldwide service. In Europe, the European Telecommunications Standards Institute (ETSI) has published recommendations about the IEEE 802.15.4 standard and, within the European service area, there is one common band with operation allowed between 868.0 and 868.6 MHz, which supports a single channel of low data rate service with less than 1 % transmission duty cycle [GCB03]. In United States of America, the national regulatory agency is the Federal Communications Commission (FCC) and just like in Europe there is only one band available for service. This band is called the 915 MHz and it covers the range between 902 and 928 MHz. This band enables the use of ten channels of low data rate service. Worldwide, in order to obtain economies of scale in product design, it is desirable to employ a single band that is available on nearly all world. To decide which band should be employed, the studies concluded that the band has to be unlicensed, have sufficient width (to enable the use of many channels) and be high enough in the spectrum, so that efficient antennas could be applied. The selected band is the 2.4 GHz ISM band, which extends from 2400 to 2483.5 MHz. This band presents a wavelength of 12.25 cm and allows for employing efficient antennas. A 2.4 GHz transceiver may also support the 868/915 MHz bands, but it is not required by IEEE 802.15.4.

F.2 IEEE 802.15.4 Frequency Bands

In the IEEE 802.15.4 version which was released in September 2006, three bands for unli-

censed operation were defined:

- **868-868.6 MHz (868 MHz band):** This unlicensed band is available in most European countries for a 20 kbps DSSS service. IEEE 802.15.4 standard also refers to this band as the “868 MHz” band;
- **902-928 MHz (915 MHz band):** Some portions of this unlicensed band are available in North America, Australia, New Zealand, and some countries in South America for 40 kbps DSSS service. IEEE 802.15.4 standard also refers to this band as the “915 MHz” band;
- **2400-2483.5 MHz (2.4 GHz band):** This last unlicensed band is available in most countries worldwide for the faster 250 kbps DSSS service. This band is referred as the 2.4 GHz band.

F.3 IEEE 802.15.4 Data Rates

Due to the physical characteristics of each band (and the regulations that are applied depending on the country), the IEEE 802.15.4 specifies different data rates and modulations for the three bands used by the two PHY layers.

The IEEE 802.15.4 working group specifies a total of 27 half-duplex channels across the three frequency bands mentioned before and they are described as follows:

- The 868 MHz band has a frequency between 868.0 MHz and 868.6 MHz and it is used in Europe. The modulation format used is the BPSK, with a DSSS at a chip-rate 300 kchip/s. In terms of channels a single channel is available with data rate of 20 kb/s and devices shall be capable of achieving a sensitivity of -92 dBm or better. A pseudo-random sequence of 15 chips is transmitted in a 50 μ s symbol period.
- The 915 MHz band presents a range between 902 MHz and 928 MHz and is used in the North American and Pacific area, adopting a binary phase-shift keying BPSK modulation format, with DSSS at a chip-rate of 600 kchip/s. In terms of channels it has ten channels available with data rate of 40 kb/s and devices shall be capable of achieving a sensitivity of -92 dBm or better. A pseudo-random sequence of 15 chips is transmitted in a 25 μ s symbol period.
- The unlicensed 2.4 GHz ISM band, with a range from 2400 MHz to 2483.5 MHz and since it is used worldwide, adopts a offset quadrature shift keying (O-QPSK) modulation format, with DSSS at 2 Mchip/s. In terms of channels it has sixteen channels with data rate of 250 kb/s and devices shall be capable of achieving a sensitivity of -85 dBm or better.

Table F.1 provides details regarding how the three frequency bands mentioned previously are used in the IEEE 802.15.4 standard, in terms of number of channels, DSSS spreading parameters, bit rate, symbol rate and spreading method. IEEE 802.15.4 requires that if a transceiver supports the 868 MHz band, it must support 915 MHz band as well, and vice versa as mentioned before. Therefore, these two frequency bands are always bundled

Table F.1: IEEE 802.15.4 data rates and frequencies of operation.

Frequency (MHz)	Number of Channels	DSSS Spreading Parameters		Bit Rate (Kb/s)	Symbol Rate (Ksymbol/s)	Spreading Method
		Modulation	Chip Rate (Kchip/s)			
868 – 868.6	1	BPSK	300	20	20	Binary DSSS
902 – 928	10	BPSK	600	40	40	Binary DSSS
868 – 868.6	1	ASK	400	250	12.5	20-bit PSSS
902 – 928	10	ASK	1600	250	50	5-bit PSSS
868 – 868.6	1	O-QPSK	400	100	25	16-array Orthogonal
902 – 928	10	O-QPSK	1000	250	62.5	16-array Orthogonal
2400 – 2483.5	16	O-QPSK	2000	250	62.5	16-array Orthogonal

together as the 868/915 MHz frequency bands of operation. Note that one 'symbol' is equivalent to four 'bits'.

F.4 IEEE 802.15.4 Network Topologies

The IEEE 802.15.4 network, independently of the type of topology, is always created by a PAN coordinator. Therefore, a PAN coordinator controls the network and performs the following minimum tasks:

- Allocate a unique address (16 bit or 64 bit) to each device in the network;
- Initiate, terminate and route the messages throughout the network;
- Select a unique PAN identifier for the network, in order to allow the devices within a network to use the 16 bit short addressing method and still communicate with other devices of other neighbouring networks;

F.4.1 IEEE 802.15.4 Star topology

In the star topology all devices establish a communication link with a single central controller, called the PAN coordinator. In this type of topology the PAN coordinator may be main powered while the other devices of the network will most likely be battery powered. When an FFD is activated for the first time, it may establish its own network and become the PAN coordinator. To establish its own network the PAN coordinator select a unique PAN identifier that is not used by any other network in the surrounding radios range (range around the device in which its radio can establish a communication link with other radios). This allows each star network to operate independently.

F.4.2 IEEE 802.15.4 Peer-to-peer topology

In the peer-to-peer topology there is also one PAN coordinator and in contrast to the star topology each device can communicate directly with any other device if the devices are placed close enough together to establish a successful communication link. A peer-to-peer

network can be ad hoc, self-organizing and self-healing. Any FFD in a peer-to-peer network can play the role of the PAN coordinator. The method of how to decide which device will be the PAN coordinator is done by picking the first FFD device that starts communicating as the PAN coordinator. In a peer-to-peer network, all the devices that are capable of relaying messages are FFDs, because an RFD is not capable of relay messages. On the other hand, an RFD will communicate with only one particular device (a coordinator or a router) in the network. A peer-to-peer network can be defined in to different shapes just by defining restrictions on the devices that can communicate among them. If no restriction exists, then the peer-to-peer network topology is called a *mesh topology*. It also allows multiple hops to route messages from any device to any other device in the network. It can provide reliability by multipath routing.

F.4.3 IEEE 802.15.4 Cluster Tree Topology

The cluster tree topology is a special case of a peer-to-peer network in which most devices are FFDs and an RFD may connect to a cluster-tree network as a leave node at the end of a branch. This last network topology type is not part of the IEEE 802.15.4 standard, but it is described in the ZigBee Alliance specifications. In this type of network the PAN coordinator establishes the initial network and any FFD can act as a coordinator and provide synchronization services to other devices and coordinators. The PAN coordinator forms the first cluster by establishing itself as the Cluster Head (CLH) with a Cluster Identifier (CID) of zero, choosing an unused PAN identifier, while broadcasting beacon frames to neighbouring devices. A candidate device receiving a beacon frame may request to join the network at the CLH. If the PAN coordinator allows the device to join, it will add this new device as a child device in its neighbour list. The newly joined device will add the CLH as its parent in its neighbour list and begin transmitting periodic beacons such that other candidate devices may then join the network at that device. Other feature of the cluster tree topology is the use of *multihopping*. For example, the PAN coordinator needs to send a message an RFD located in the edge of the branch, but there is a barrier between them that is hard for the signal to penetrate. The tree topology helps by relaying the message around the barrier and reach device. The advantage of using this type of topology is the increase of the network coverage area at the cost of increased message latency.

F.5 IEEE 802.15.4 PHY Specifications

As described before the physical layer of the IEEE 802.15.4 is responsible by the control of several parameters. The parameters controlled by the IEEE 802.15.4 are described below.

F.5.1 Receiver Energy Detection

The receiver EnD value is an estimation of the received signal power within the bandwidth of an IEEE 802.15.4 channel and there is no attempt to decode or identify the type of signal that is currently occupying the channel. In other words, when performing an EnD it does

not reveal whether this signal is an IEEE 802.15.4 standard compliant or not. The EnD time should be equal to 8 symbol periods. For example, if the required receiver sensitivity is -85 dBm, the EnD procedure must be able to detect and measure the energy of signals as low as -75 dBm. The minimum EnD value (0) indicates received power less than 10 dB above the specified receiver sensitivity. The range of received power spanned by the EnD values shall be at least 40 dB and the mapping from the received power in dB to EnD values shall be linear with an accuracy of ± 6 dB.

F.5.2 Link Quality Indication (LQI)

The RSS is a measure of the total energy of the received signal. Other way to evaluate the signal quality is using the SNR measure, which is the ratio of the desired signal energy to the total in-band noise energy. When considering a signal with high SNR it means that the signal has high-quality. The LQI measurement is performed for each received packet and LQI must have at least eight unique levels. This LQI measurement is generated in the PHY layer and is available to the NWK and APL layers. The minimum and maximum LQI values should be associated with the lowest and highest quality IEEE 802.15.4 signals detectable by the receiver and LQ values should be uniformly distributed between these two limits.

F.5.3 Carrier Sense (CS)

The CS technique is quite similar to the EnD technique and it is used to perform verification if whether a frequency channel is available to use. When a wireless device has the intention to transmit a message, it first switches to receive mode in order to detect the type of any possible signal that might be present in the desired frequency channel. While in EnD the signal detected in the channel is not decoded, in the CS technique the signal is demodulated so in order to perform verification whether the signal modulation and spreading are compliant with the parameters of the PHY used by the receiver device. After this verification and if the signal is compliant with the IEEE 802.15.4 PHY, the wireless device will decide if the channel is busy or not, regarding to the signal energy level.

F.5.4 Clear Channel Assessment (CCA)

When performing the CCA, the results of EnD or CS can be used to decide whether a frequency channel should be considered available or busy. The CCA period must be eight symbols.

Three CCA modes are contemplated in the IEEE 802.15.4 compliant PHY and can operate in any one of them:

- **CCA mode 1:** when considering this mode, the EnD result is the only one that is taken into account. Therefore if the energy level is above the EnD threshold, the channel is considered busy. This EnD threshold can be set by the manufacturer of the radio transceiver;
- **CCA mode 2:** when considering this mode, the CS result is the only one that is taken into account and the channel is considered busy only if the occupying signal is compliant with the PHY layer of the device that is performing the CCA;

Table F.2: Channel assignments.

Channel Page	Channel number	Frequency band	Modulation
0	0	868 MHz	BPSK
	1-10	915 MHz	BPSK
	11-26	2.4 GHz	O-QPSK
1	0	868 MHz	ASK
	1-10	915 MHz	ASK
	11-26	Reserved	-
2	0	868 MHz	O-QPSK
	1-10	915 MHz	O-QPSK
	11-26	Reserved	-
3-31	Reserved	Reserved	-

- **CCA mode 3:** this mode is the result of a logical combination (AND/OR) of mode 1 and mode 2. Therefore, there are two solutions to detect if the channel is busy:
 - * If the detected energy level is above the threshold and a compliant carrier is sensed then the channel is busy;
 - * If the detected energy level is above the threshold or a compliant carrier is sensed then the channel is considered busy.

F.5.5 Channel Selection

The IEEE 802.15.4 standard initial release has a total of 27 channels and the implementation of multiple operating frequencies bands could not be supported. For each channel page it could have a maximum of 27 channels. A channel page is a concept introduced by the IEEE 802.15.4 in 2006 to distinguish between supported PHYs, because in the previous releases of the standard the frequency channels were identified by channel numbers and there were no optional PHYs. The distribution of channels selection in different PHYs could be resumed by the Table F.2.

F.6 IEEE 802.15.4 PHY Packet Structure

The structure of the PPDU encapsulates all data structures from the higher levels of the protocol stack.

- **PPDU synchronization header:** It enables the receiver to synchronize and lock into the bit stream. The PPDU header consists of two fields, a preamble and a Start-of-Frame Delimiter (SFD). The preamble field is used by the receiver to obtain chip and symbol synchronization. The bits in the preamble field in all PHYs, except for the ASK PHYs, are binary zeros. The SFD allows the receiver to establish the beginning of the packet in the stream of bits. Remind that one “octet” is equal to one “byte” and one “symbol” is equal to four “bits”. For the lengths and durations

Table F.3: Preamble field lengths and durations.

PHY option	Modulation	Length		Duration [μ s]
868 MHz	BPSK	4 octets	32 symbol	1600
915 MHz	BPSK	4 octets	32 symbol	800
868 MHz	ASK	5 octets	2 symbol	160
915 MHz	ASK	3.75 octets	6 symbol	120
868 MHz	O-QPSK	4 octets	8 symbol	320
915 MHz	O-QPSK	4 octets	8 symbol	128
2.4 GHz	O-QPSK	4 octets	8 symbol	128

Table F.4: SFD field lengths.

PHY option	Modulation	Length	
868 MHz	BPSK	1 octet	8 symbol
915 MHz	BPSK	1 octet	8 symbol
868 MHz	ASK	2.5 octets	1 symbol
915 MHz	ASK	0.625 octet	1 symbol
868 MHz	O-QPSK	1 octet	2 symbol
915 MHz	O-QPSK	1 octet	2 symbol
2.4 GHz	O-QPSK	1 octet	2 symbol

of the preambles in all PHY options it is resumed in Table F.3 and for the length of the SFD it is resumed in Table F.4.

- **PPDU PHY header:** The PHY header is a single 8 bit field with the MSB reserved and the remaining low order bits used to specify the total number of octets in the PHY payload. The PHY payload length can be any value from 0 to 127 bytes. Packets lengths of 0 to 4 and 6 to 8 bytes are reserved. Packets of length 5 bytes are MPDU acknowledgement packets and packets with 9 or more bytes are MPDU payloads for the MAC protocol layer service.
- **PPDU PHY payload:** The PHY payload is composed of only one field called the Physical Layer Service Data Unit (PSDU). The PSDU is variable length and carries the data payload of the PPDU. All packets carry an MPDU payload for the MAC layer.

Appendix G

IEEE 802.15.4 Standard MAC Layer

G.1 SuperFrame Structure

G.1.1 Timing Parameters

The timing parameters in beacon enabled operating mode that correspond to the super-frame structure discussed in Section 4.6.4 are presented in Table G.1.

Table G.1: Timing parameters in beacon enabled operating mode.

Time Period	MAC attribute	Duration (symbols)
Unit backoff period	$aUnitBackoffPeriod$	20
Basic superframe slot	$aBaseSlotDuration$	$3 \cdot aUnitBackoffPeriod = 60$
Superframe slot		$aBaseSlotDuration \cdot 2^{SO}$
Superframe duration	SD	$aBaseSuperframeDuration \cdot 2^{SO}$
Beacon interval	BI	$aBaseSuperframeDuration \cdot 2^{BO}$

G.1.2 InterFrame Spacing

When transmitting data from one device to another, the device must wait during a short time interval between its successive transmitted frames in order to allow the receiving device to process the received frame before the next frame arrives. This feature is known as *Interframe Spacing* (IFS). The length of IFS depends on the transmitted frame size [Far08]. If the MPDU has sizes less than or equal to $aMaxSIFSFramesSize$ (default value of 18 octets) it is considered as short frames and if a MPDU size exceeds $aMaxSIFSFramesSize$ octets than it is considered as a long frame. The wait time after a short frame is named as Short IFS (SIFS) and the minimum value of SIFS is equal to $macMinSIFSPeriod$. The same way as in the short frame, the long frame is followed by a Long IFS (LIFS) and the minimum length is given by $macMinLIFSPeriod$. The values of $macMinSIFSPeriod$ and $macMinLIFSPeriod$ are 12 and 40 symbols, respectively.

G.2 IEEE 802.15.4 MAC Frames

This section presents the details on the four IEEE 802.15.4 MAC frames structures addressed in Section 4.6.5.

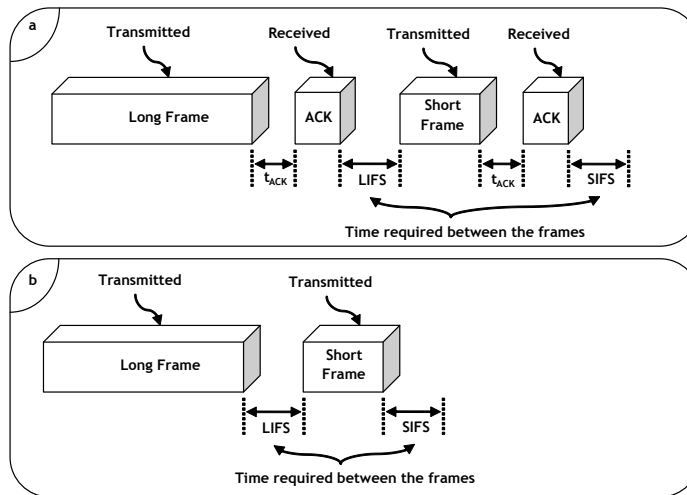


Figure G.1: The IFS in (a) Acknowledged transmission and (b) unacknowledged transmission.

G.2.1 Beacon Frames

When a beacon-enabled network is considered, a FFD device may transmit beacon frames. The entire MAC frame is used as a payload in a PHY packet. The content of the PHY payload is mentioned as the PSDU. In a beacon frame, the address field contains the source PAN ID and the source device address.

The MAC frame consists of three sections: the MAC Header (MHR), the MAC payload and the MAC Footer (MFR). The frame control field in the MHR has the information that defines the frame type, addressing fields and other control flags. The sequence number specifies the Beacon Sequence Number (BSN). The addressing field provides the source and destination addresses.

The MAC payload of a beacon frame is divided into four fields:

- *SuperFrame specification field*: contains the parameters that specify the superframe structure (if exists);
- *Pending address specification field*: contains the number and type of addresses listed in the Address List Field;
- *Address list field*: contains a list of devices addresses with data available at the PAN coordinator;
- *Beacon payload field*: optional field that will contain broadcast data to the devices that make part of its network within its range of coverage.

The receiver uses the Frame Check Sequence (FCS) field to check for any possible error in the received frame. The format of the beacon frame is shown in Figure G.2.

The subfields from the beacon frame are explained with more detailed in Figure G.3. The Beacon Order (BO) subfield determines the transmission intervals between the beacons.

The superframe is divided into 16 equal and contiguous time slots and the final CAP slot subfield defines the last time slot of the CAP. If there are any remaining time slots after the CAP, they are used as GTSs.

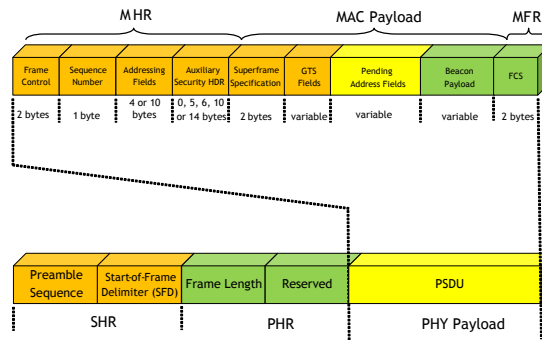


Figure G.2: MAC beacon frame structure and the PHY frame structure.

If the BLE subfield is set to one, it means that the beaconing device will turn off its receiver after a certain period of time to conserve its energy. When the beacon frame is transmitted by the PAN coordinator, the PAN coordinator subfield is set to one, helping to distinguish between a frame received from the PAN coordinator and any other coordinator in the same network.

The association permit subfield is the last bit in the superframe specification and if is set to zero, it means that the coordinator does not accept association requests at this moment.

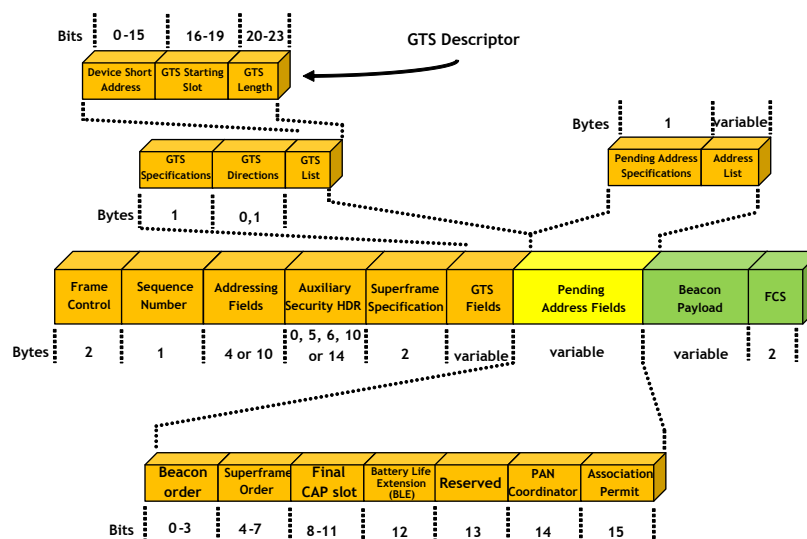


Figure G.3: Detailed description for the beacon frame fields.

The main objectives of the beacon frames are the establishment of GTSs. The GTS subfield defines whether the PAN coordinator currently accepts GTS requests and determines the number of GTSs listed in the GTS list field. A way to define direction of the GTSs is using the GTS direction subfield to set the GTSs to receive-only or transmit-only modes. The GTS list are stored the list of all GTSs that are currently maintained (GTS descriptors). The GTS descriptor contains the short address of the device that will use the GTS, the GTS starting slot and the GTS length. Finally, the pending address field contains the addresses of all devices that have data pending at the coordinator. Each device checks for its address in this field and if there is a match with the node address, then the device will contact the coordinator and request the data to be transmitted to it.

G.2.2 Data Frames

The MAC data frame, presented in Figure G.4, is used by the MAC sublayer to transmit data. The address field contains the PAN ID and the device ID of the source and/or destination, as specified in the MCPS-DATA primitive. The data payload field is provided by the NWK layer. The data contained in the MAC payload is referred to as the MAC Service Data Unit (MSDU). All the fields in this frame are similar to the beacon frame except for the superframe, GTS and pending address fields that are not present in the MAC data frame. The MAC data frame is referred to as the MAC Protocol Data Unit (MPDU) and becomes the PHY payload.

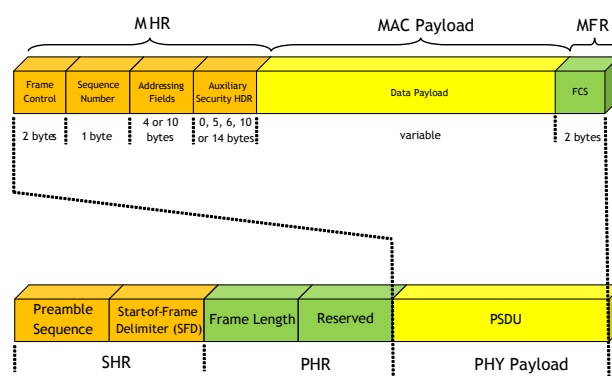


Figure G.4: The MAC data frame structure and the PHY frame structure.

G.2.3 Acknowledgement Frames

The MAC acknowledgement frame, presented in Figure G.5, is the simplest MAC frame format and there is no MAC payload present in this frame [Far08]. These frames are sent by the MAC sublayer to confirm a successful frame reception to the device that has sent the message. The acknowledgement was designed by the IEEE 802.15.4 design group to be very short in order to minimize network traffic. The acknowledgement frame does not contain the address field in the MAC header and there is no MAC payload. When a network device receives an acknowledgement frame, it first verifies if it was expecting an acknowledgement frame and then it checks if the frame sequence number matches the one it is expecting. Otherwise the acknowledgement frame is discarded. The acknowledgement frame is generated only if the received message is requesting acknowledgement and the FCS is evaluated as good or not by the receiving device.

G.2.4 MAC Command Frames

The MAC command frame is generated by the MAC sublayer and is responsible for all the MAC control transfers for each MAC command type presented in Table G.2.

The MAC commands such as requesting association or disassociation with a network are transmitted using the MAC command frame, Figure G.6. The MAC payload has two fields,

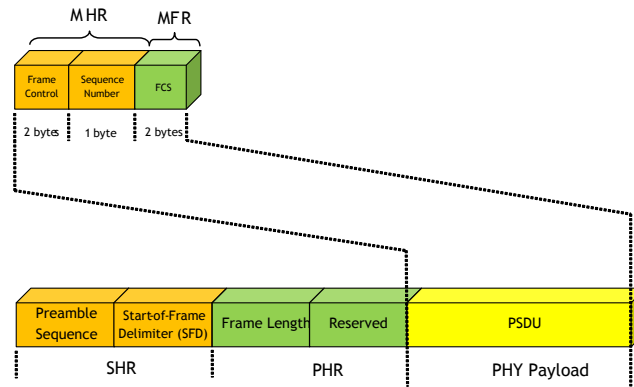


Figure G.5: The MAC acknowledgement frame structure and the PHY frame structure.

Table G.2: MAC commands frame types.

Command Identifier	Comamand Type	RFD	
		Transmit	Receive
1	Association Request	✓	-
2	Association Response	-	✓
3	Disassociation Notification	✓	✓
4	Data Request	✓	-
5	PAN ID Conflict Notification	✓	-
6	Orphan Notification	✓	-
7	Beacon Request	-	-
8	Coordinator Realignment	-	✓
9	GTS Request	-	-
10-255	Reserved	-	-

the MAC command type and the MAC command payload. The MAC command payload contains information specific to the type of command in use. The entire MAC command frame is placed in the PHY payload as a PSDU [Far08].

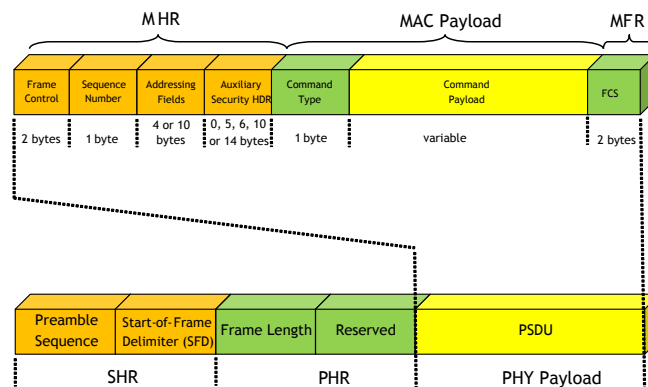


Figure G.6: IEEE 802.15.4 MAC command frame [GCB03, Far08].

G.2.5 Slotted and Unslotted CSMA-CA Algorithm Phases

The slotted CSMA-CA algorithm can be described as follows [Far08, GCB03]:

- **Phase 1** - Initially sets the number of backoffs counter and the contention window variable ($NB = 0$; $CW = 2$). The backoff exponent is used to determine the number of backoff periods a device should wait before attempting to access the channel. If the device operates on battery power, the attribute *macBattLifeExt* is set to true, BE is set to 2 or to the constant *macMinBE*, depending on the one that is smaller. Otherwise, it is set to *macMinBE*, the default value of which is 3.

- **Phase 2** - Then the CSMA-CA mechanism locates the backoff period boundary and a random number in the range 0 to $2^{BE} - 1$ is generated. The algorithm then counts down for this number of backoff periods. This period is defined as the Random Backoff Countdown (RBC) and during this period the channel activity is not accessed and the backoff counter is not stopped if detects activity in the channel. In order to disable the CA procedure at the first iteration, *BE* must be set to 0, and thus the waiting delay is null;
- **Phase 3** - Once the backoff counter reaches zero, the algorithm first checks if the remaining time within the CAP area of the current superframe is sufficient to accommodate the necessary number of CCA checks, the packet transmission and the acknowledgement (alignment with time slots). Then if this is the case, the algorithm performs the CCA at the BP boundary to assess channel activity and if the channel is busy then the algorithm goes to phase 4, otherwise the algorithm goes to phase 5;
- **Phase 4** - If the CCA result is an idle channel the packet may be transmitted. Otherwise, if the result of the CCA is a busy channel, the node concludes that there is an ongoing transmission by another device and the current transmission attempt is aborted. The CSMA-CA mechanism is then restarted, the NB and the BE are incremented by one unit and the CCA counter is reset to two. The BE must not exceed *macMaxBE* (by default equal to 5). If the number of unsuccessful backoff cycles NB exceeds the limit of *macMaxCSMABackoffs* (default value equal to 5), the algorithm finishes with channel access failure status which is reported to higher protocol layers;
- **Phase 5** - If the channel is idle, the CW variable is decremented by one unit. The CCA operation is repeated until $CW \neq 0$ (phase 3). With this step the algorithm ensures the performing of two CCA operations to prevent potential collisions of acknowledgement frames, when two or more nodes are transmitting at the same time. When channel is again sensed as idle ($CW=0$), the node attempts to transmit.

The unslotted CSMA-CA algorithm is used in a non-beacon network and can be described as follows [Far08, GCB03]:

- **Phase 1** - The unslotted CSMA-CA algorithm initially sets the number of backoffs and the backoff exponent is equal to *macMinBE* ($NB=0$, $BE= macMinBE$). The CW variable is not used, since the non-slotted CSMA-CA has no need to iterate the CCA procedure after detecting an idle channel;
- **Phase 2, 3, and 4** - These steps are quite similar to the one in slotted CSMA-CA, but there are some differences namely the fact that there is no synchronization to the backoff period boundary. Therefore, the random backoff countdown begins immediately after the arrival of the data packet from the upper layers of the protocol stack and then the CCA is performed immediately after the expiration of the random backoff delay generated in the phase 2. Since there is no superframe in unslotted CSMA-CA, the device performs the CCA check, followed by the packet transmission and acknowledgement (if requested), as soon as the random backoff countdown is finished;
- **Phase 5** - Unlike the slotted CSMA-CA, the unslotted version starts immediately the transmission of the frame after it detects an idle channel.

G.3 MAC Protocols Taxonomy

G.3.1 Unscheduled MAC protocols

- PicoRadio

PicoRadio [RAD^S+00] protocol solves the access conflict by using multiple channels, by using a scheme based on dynamic channel assignment, where each node is assigned with a unique channel. The Code Division Multiple Access (CDMA) scheme employed also uses a wake-up radio to wake-up neighbours nodes. Here the node listen to a Common Control Channel (CCC) and broadcasts a Channel Assignment Packet (ChAP) to the neighbours, in order to notify them about the channel which is going to be used. These ChAP exchanges between nodes will allow to update the channel assignment table of each node (records the channel usage in the network). During the channel setup period the nodes that wake-up will listen the channel for a certain time, in order to obtain information about the channels used by the one-hop and two-hop neighbours. After gathering this information the node chooses an unused channel and broadcasts its channel and its neighbours channel throughout the network. If two nodes choose the same channel, the first one to detect it chooses another unused channel. In PicoRadio, two channel assignment techniques can be used: sender based and receiver based. In sender based technique the sender transmits packets in its transmission channel; whilst in receiver based the receiver wakes-up to receive the packets. The wake-up radio used in this protocol is very simple which could be very sensitive, leading to the appearance of false orders to wake-up caused by noise, activating the data radio unnecessarily. Moreover, the wake-up radio is capable of carrying information, which means that the sender can send a wake-up tone addressed to a certain node.

- Practical Multi-Channel MAC

Practical Multi-Channel [LHA08] protocol utilizes multiple channels efficiently. The channel assignment is based on a control theory approach that dynamically allocates channels to nodes, and groups of nodes that are sharing the channel. This protocol assumes that the nodes do not require time synchronization. The channel assignment algorithm employed specifies that all nodes start on the same channel. Then, as nodes exchange status packets, the packet loss ratio and degrees of estimated communication success probability is measured, allowing the nodes to know the amount of interference experienced on their channel. These nodes then choose the next available channel and others ones from the same cluster will choose the same one. When a node needs to send a message to another on a different channel it changes momentarily to the destination's node channel. The employed mechanism keeps separated the routing and application layer, allowing minimizing the cost of cross-channel communication, while maximizing the traffic loads in channels. The status packets are exchanged periodically, leading to a decrease of the energy efficiency. Moreover, as nodes detect channel interference/congestion they change to another available channel which deals with the narrowband long lasting interference.

- Dynamic MAC (DSMAC)

DSMAC [LQW04] protocol adjusts dynamically the node's duty cycle, depending on the current utilization efficiency and average latency of the sensor. All nodes assume the same duty cycle at the beginning. A node will double the original duty cycle by decreasing the sleep time period length when it needs to decrease the latency or when the traffic exchanged is higher. When a node changes its duty cycle, it informs about the additional active schedule the other nodes by sending the SYNC packet that has the SYNC initiator's duty cycle. Each node maintains a synchronization table for its neighbouring nodes. Once neighbouring nodes receive the SYNC packet, they will decide if the duty cycle is increased in order to be same as the one sent by the SYNC packet sender node. The duty cycle can return to initial one, has the traffic conditions or latency becomes more stable.

- **Transmitted Initiated CyclEd Receiver (TICER)**

TICER [LRW04] protocol utilizes the cycled receiver scheme, where nodes are powered on and off periodically and beacons are transmitted on the same and single data channel. For unicast transmissions, when the node has no data packet to transmit, it wakes-up to check the channel and goes back to sleep. When it has a data packet to transmit it wakes-up and checks the channel for certain duration. If it does not sense any ongoing transmissions, it starts transmitting RTS packets. When the receiver node wakes-up it detects the RTS packets and answers with CTS packets. The sender node receives the CTS packets, which in turn starts to transmit the data packet. The exchange is finished by an Acknowledgement (ACK) packet transmitted by the receiver node. This protocol will lead to an idle listening increase at the receiver node side.

- **Receiver Initiated CyclEd Receiver (RICER)**

RICER [LRW04] protocol shares, the same principles of TICER, where a sensor node changes communication initiation from the transmitter side to the receiver side. When a sensor node has no data packet to send it wakes-up and transmits a beacon just to announce that it is awoken. After it sends the beacon, the node senses the channel for a response. If no response is detected, the node goes back to sleep. Otherwise, if a response is received, it transmits the data packet. In order to send the data packet the sender node stays awake and monitors the channel, while waiting for a wake-up beacon. After it receives the beacon the data packet is transmitted. The exchange also ends with an ACK packet. Higher energy savings are achieved for unicast and anycast communications, but for broadcast and multicast communications cannot be used because the communication must start in the receiver. It is basically a preamble sampling technique, but here the transmitter has an inverted role, which keeps receiving instead of sending a preamble. For low load of traffic this periodic beacon report can lead to an overhead.

- **SyncWUF**

SyncWUF [SS07] protocol combines the simple signalling technique with an innovative Wake-Up Frame (WUF) technique. The simple signalling technique is just a signal, while the WUF contains the information. The main idea of SyncWUF is that the sender node stores the receivers' schedules, while adapting the Wake-Up Signal (WUS). If a receiver node schedule is out-of-date the WUS length is going to be long. Multiple Short Wake-Up Frames (SWUFs) are used by the WUS in order to reduce

the extra waiting time of the WUF scheme. These SWUFs contain the destination MAC address and the current SWUF state in the whole WUF. Based on the information contained in the SWUFs the receiver nodes can decide when to turn on the transceiver in order to receive the data packets, reducing the waiting time. However, if the sender node does not exchange packets during the active period of the receiver node, it must wait until the next active period, leading to an increase of the transmission delay.

- Energy-Efficient Reliable MAC (E2RMAC)

E2RMAC [JaBA07] follows some of RMAC principle, in order to improve the energy-efficiency by reducing the idle listening and overhearing. It achieves this by using an additional wake-up radio. This wake-up radio is used every time the node wants to transmit a packet, where it sends a tone on its low power radio. By transmitting this wake-up tone the neighbours will know when they will sleep. After sending a packet, the node goes to sleep mode for a duration equal to the time needed by the receiver to forward the packet (similar to adaptive listening). E2RMAC employs immediate data forwarding to save on ACK transmissions (same as in RMAC).

- Sparse Topology and Energy Management (STEM)

STEM [JBA07] tries to conserve energy by using two separate channels: i) wake-up channel and ii) data channel. The wake-up channel is used to allow a time organization between the transmitter and the receiver, whilst the data channel is only used to data exchange when the transmitter and the receiver encounters. Therefore, to guarantee the encounter between the transmitter and the receiver, nodes follow a preamble sampling approach. Two versions of STEM have been proposed: i) STEM Tone (STEM-T) and ii) STEM Beacon (STEM-B). STEM-T employs a tone on a separate channel to wake-up neighbouring nodes, while in STEM-B the traffic generating node sends a series of beacons, which carry the MAC address of the transmitter and of the receiver. In the STEM-B version the beacons are sent through the wake-up channel in order to the sleeping nodes turn on their radios to receive the messages. The wake-up channel is formed by synchronized time slots. Comparing both versions of STEM the STEM-T will guarantee the lower latency, but with requires more overhead than STEM-B since the receivers must be idle, listening all of the time for the tones. However, STEM-T may require a separate radio transceiver for the wake-up channel.

G.3.2 Scheduled MAC protocols

- Timeout-MAC (T-MAC) protocol

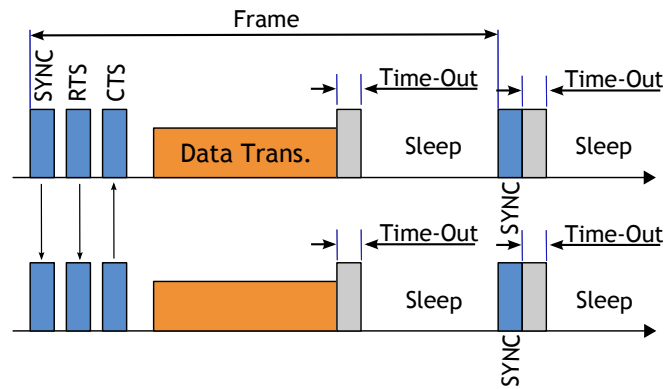


Figure G.7: T-MAC data transferring mechanism.

T-MAC [vDL03] tries to improve some flaws of the S-MAC. It tries to eliminate idle energy by adapting the length of the active period of the frame. Instead of transmitting a message during a predetermined period (as in S-MAC), messages are sent in burst at the beginning of the frame. Activation events, (such as firing of the frame timer or any radio activity) will wake-up the node to handle the type of activation event. In Figure G.7, during the first active period there is a sensor node involved in a message transmission and the second active period has a SYNC transmission. The time-out period is used when a node does not detect any activity within the time-out interval, it can assume with sure that no neighbour wants to communicate with it and goes to sleep. If there is a node that wants to communicate with it a new time-out timer is initiated. To improve the message latency the Future Request To Send (FRTS) control message is proposed. The FRTS packet informs the next hop that it has a future message transfer. T-MAC considers the buffer size of the sensor nodes when calculating the contention period. If the buffer is full, the sensor nodes will have higher priority and control the channel, avoiding the buffer overflow.

- Mobility Aware MAC (MS-MAC) protocol

The MS-MAC [PJ04] is similar to S-MAC to conserve energy when nodes are static. MS-MAC employs a new mechanism to handle mobility. This mechanism is based on the RSSI as an indication of mobility and, when necessary, triggers the mobility handling mechanism. The mechanism relies on the RSSI of periodical SYNC messages from its neighbours. When the signal changes, the receiving node presumes that the neighbour or itself are moving and the level of change of the RSSI signal can predict the mobile node's speed. This protocol allows for the creation of cluster, formed by a mobile node and its neighbours (forms an active zone). The mobile nodes can cross from one cluster to other ones, but during this crossing the node runs the synchronization periods more times resulting in higher energy consumption with lower time needed to create new connections. This mobility aware mechanism of MS-MAC allows nodes to work efficiently in both stationary and mobile scenarios. Considering a stationary scenario or when nodes move only inside a single cluster, all nodes work efficiently.

- EMACS

EMACS [DHNH03] is a TDMA based protocol, which divides the time slot into three sub periods, (communication request, Traffic control and Data sub periods. The

traffic control sub period is used to transmit the periodic control information of the nodes. The sensor node must transmit this information within his time slot, while the neighbouring nodes listen for the control packet of the neighbours. All the data transmissions occur within the data sub period. The communication request sub period can be used by a node that wants to transmit in a time slot it does not own, by transmitting a request in this sub period. Three types of nodes are possible in EMACS. The active nodes have full use of the sub periods, since they own a slot and transmit a control message within each slot they own. The passive nodes do not own a time slot and can only transmit a message after requesting a slot it does not own. The dormant nodes do not participate in the sensor network until it decides to become an active or a passive node. This allows conserving energy by activating only the number of nodes needed to perform the application functionality.

- **Lightweight MAC (LMAC)**

LMAC [VHH04] is also a TDMA based protocol. Unlike traditional TDMA-based systems, the time slots in LMAC protocol are not divided among the networking nodes by a central entity. Instead a distributed algorithm is used. Concerning its time slot, the node will always transmit a message formed by two parts: control message and a data unit. The node is collision free, because a time slot can only be controlled by a single node. The control message carries the ID of the time slot controller, the distance of the node to the gateway in hops, contains the destination address and the length of the data unit. Moreover, the control data is used to maintain synchronization. If the control message is not addressed to some nodes, the nodes will switch off their transceivers and only wake-up at the next time slot. In this protocol, the node can only transmit a single message per frame.

- **Node Activation Multiple Access (NAMA)**

NAMA [BGLA01] is a protocol where the access to the channel is controlled by assigning priorities to sensor nodes in each slot. It employs a TDMA scheme with time divided into blocks of S_b sections. Each S_b section has P_s parts and the parts contain T_p time slots, as presented in Figure G.8. Then a node selects a single part, to contend with other nodes that have chosen the same part. The last section of each block is reserved for signalling purposes. The priority is computed by each node with its neighbours and this is used to determine who will access to current time slot within the sensor node's chosen part. The sensor with the highest priority will be one that will transmit. Other protocols derived from NAMA, such as Link Activation Multiple Access (LAMA) and Pairwise-link Activation Multiple Access (PAMA). LAMA activates links to destinations sensor nodes based on the DSSS code assigned to the receiver and the priority assigned to the transmitter. PAMA activates links between sensor nodes by assigning priorities to the links, while varying the codes and priorities of links based on the current time slot. The aforementioned protocols all require a sensor node to compute the priorities of each neighbouring node for each time slot, leading to an increase of energy consumption.

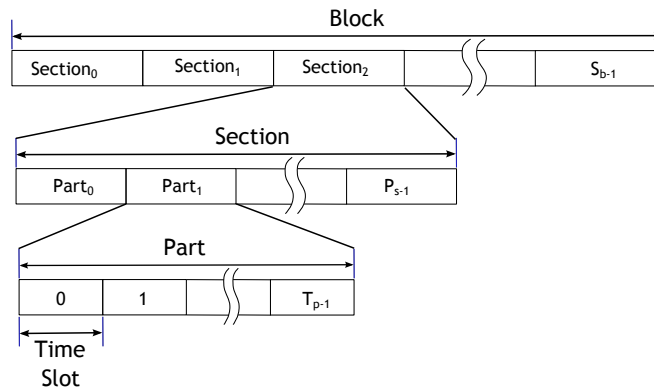


Figure G.8: Time division structure of NAMA protocol.

- Fast Path Algorithm (FPA)

FPA [LKR04] guarantees the relaying of frames by waking up the nodes for an additional time. A node uses its hop-distance from the sender to estimate when its neighbour can send a frame to it. When the node wakes-up at the estimated time only to receive and forward the frame to its downstream neighbour. These additional times are set from the information piggybacked in the first data packet sent.

- Flexible MAC (FlexiMAC)

FlexiMAC [LDC006] is able to handle the network dynamic and node mobility. A contention period is used in order to nodes exchange packets to build a data gathering tree rooted at the sink. The slot distribution is based on a Depth First Search (DFS) and the slot numbering starts with number 2 because slot number 1 is reserved for the network dynamics. The reserved slot has the name Fault Tolerant Slot (FTS). The slot assignment algorithm follows the tree. Two types of slots exist: the data gathering slots and the multifunctional ones. Data-gathering slots are used to uplink traffic from nodes to the sink, while multifunctional slots are used for the downlink traffic and synchronization. This data gathering tree has the disadvantages of the need for tree reconstruction when a link fails and only parent-child and child-parent communications are optimal. The period assigned to handle the network dynamics may lead to higher energy consumptions.

- Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH [HHT02] tries to solve the energy dissipation in sensor networks. Nodes are selected randomly as cluster heads, in order to the high energy dissipation in communicating with the base station is divided to all sensor nodes. LEACH consists in two phases: the setup phase and the steady phase. To reduce the overhead the duration of the steady phase is longer in the duration of the setup phase. In the setup phase a sensor node chooses a random number between 0 and 1. If the chosen number is less than a certain threshold, the sensor node is selected as the cluster head. After that the cluster heads inform all the surrounding nodes that he is the cluster head. Once this advertisement is performed the other nodes choose the cluster that they want to belong and the cluster heads assign the time on which the sensor nodes can send data back to the cluster heads based on a TDMA scheme. In the steady phase, the nodes can begin sensing and transmitting data to cluster heads. Data aggregation is another feature of the cluster heads. This process of selecting cluster

heads is repeated after a certain period of time. Some disadvantages are pointed, such as the need of a complex radio transceiver with DSSS and power scaling, which increases the energy consumption. Another disadvantage is the time it takes to redo the cluster. Finally, LEACH assumes that each node communicates directly with the cluster head, which can consume larger amounts of energy or restrict the sensor nodes to a certain geographical area.

G.3.3 Hybrid MAC protocols

- Wireless MAC (WiseMAC) protocol

WiseMAC [EHD04] is a preamble sampling based protocol which employs TDMA/CSMA techniques and where all sensor nodes have two communication channels. The TDMA technique is used to access the data channel, while the CSMA technique is used to access the control channel. The use of preamble sampling jointly with a non-persistent CSMA decreases the idle listening. The preamble sampling technique involves the transmission of a preamble before each data packet, to inform the potential receiving node. The size of the preamble is initially set to be equal to the sampling period. However, the potential receiver may not be ready at the end of preamble to receive the data packet, causing energy waste. WiseMAC offers a method that dynamically determines the length of the preamble, with the intention to reduce the power consumption due to a fixed length preamble. This method uses the knowledge of the sleep schedule of the transmitter node's direct neighbours. Based on neighbours' sleep schedule table, WiseMAC schedules transmissions so that the destination node's sampling time corresponds to the middle of the preamble sent. Figure G.9 describes the WiseMAC data packet transmission. Main disadvantage of WiseMAC is that decentralized sleep-listen scheduling leads to different sleep and wake-up times for each neighbour of a node. Moreover, the hidden terminal problem occurs with WiseMAC, because it is based on a non-persistent CSMA.

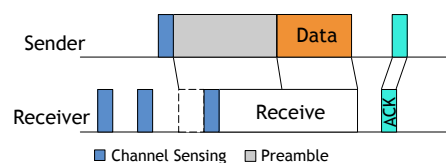


Figure G.9: Data packet transfer in WiseMAC protocol.

- Power Efficient and Delay Aware Medium Access Control for Sensor Network (PEDAMACS)

PEDAMACS [EV06] gathers information concerning traffic and topology during the setup phase in the sink. Then, based on the collected information the sink calculates a global scheduling and sends it to the entire network. In PEDAMACS is assumed that the hardware of the sink is more powerful than the remaining nodes, in order to reach all nodes when it transmits. It also follows a TDMA based scheme for the uplink feature. For the topology phase, a CSMA based scheme is used to send information to the sink. In this phase the sink node sends topology-learning packets, in order to build the spanning tree and the sink has the knowledge of the entire topology. One of the disadvantages of PEDAMACS is that only supports convergecast traffic

type. Moreover, the assumption that all nodes are reachable by the sink is not always satisfied. Nodes that did not receive the schedule information sent by the sink have to wait for the next topology learning phase and inform the sink by piggybacking this information in the reply packets to the sink.

- Zebra MAC (ZMAC)

ZMAC [RWA⁺08] combines both CSMA and TDMA schemes in order to adapt to the level of contention in the network. If the network is under low contention the ZMAC switches to CSMA scheme, and when it is under high contention it behaves like TDMA based scheme. ZMAC employs a CSMA as baseline MAC scheme, but for contention resolution it employs a TDMA schedule where the time slot assignment is performed at the time of deployment (higher overhead at the beginning). ZMAC uses a scalable channel scheduling algorithm named as DRAND. After slot assignment, each node reuses periodically its assigned slot to transmit. In ZMAC the time slot has an owner and the others are called the non-owners of that slot. In ZMAC a time slot can have a maximum of two owners, but it has to be separated two hops at least. Before transmitting each node performs a carrier sense and transmits the packet if the channel is free. ZMAC reduces the collisions since the owners of time slots have higher priority than the non-owners to transmit. By mixing CSMA with TDMA, ZMAC becomes less susceptible to timing failures, slot assignment failures and topology changes than a standard TDMA scheme. When the TDMA and CSMA mixing fails, it always relies on the CSMA by default. A disadvantage is energy consumption when slot assignment and synchronization occur frequently in the network.

- X-MAC

X-MAC [BYAH06] is an adaptive energy-efficient MAC layer protocol for duty cycled WSNs. Other duty cycle MAC protocols employ an extended preamble and preamble sampling. This long preamble introduces excess latency at each hop, while leading to suboptimal energy consumption and excessive energy consumption at non-target nodes. X-MAC proposes solutions to alleviate these problems by employing a shortened preamble approach that retains the advantages of low power listening. To solve the overhearing problem X-MAC embeds in the preamble address information of the target so that non-target receivers can quickly go back to sleep. To reduce the excessive latency and energy waste a strobed preamble is used by splitting the full-length preamble into packets with a gap between consecutive packets, giving an advantage of not always requiring the extended preamble. In Figure G.10 is presented a comparison between the LPL and X-MAC mechanisms. With this strobed preamble the listening nodes do not need to wait for the entire preamble. An adaptive algorithm for automatically adjusting the duty cycle of receivers to the offered traffic load is also employed in X-MAC. However, when light traffic loads are considered there is an increase of the idle listening at the receivers, leading to energy wastes.

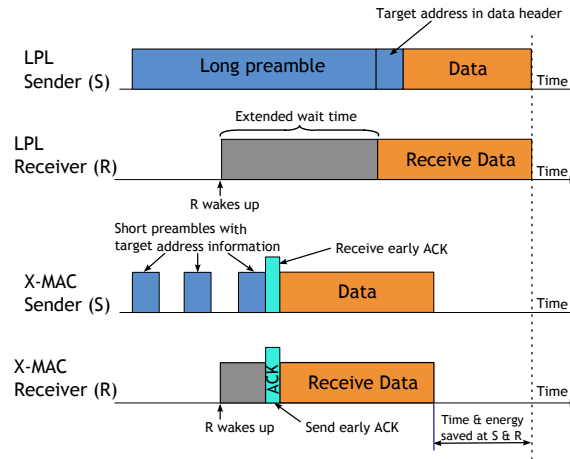


Figure G.10: Comparison of the timelines between LPL's and X-MAC's approaches.

- Y-MAC

Y-MAC [KSC08] is a multi-channel MAC protocol for high deployment WSNs. This protocol employs a scheduled access, but with some modifications. The timeslots are assigned to receivers rather than to senders. Potential senders contend in the beginning of each timeslot for the same receiver. When there is the need to transmit multiple packets, the sender and receiver choose a new channel according to a pre-established sequence. The main disadvantage of Y-MAC is the increase of the contention time when there is a high number of nodes around the sink node, which increase the data rate.

G.3.4 QoS MAC protocols

- Q-MAC

Q-MAC [LEQ05] is referred as a QoS-aware MAC protocol. A multi-hop scenario is assumed where nodes generate packets with different priorities. The main objectives of Q-MAC are to minimize the energy consumption, while providing QoS policies. To achieve these objectives Q-MAC is composed of intra-node and inter-node QoS scheduling mechanisms. The intra-node QoS scheduling mechanism classifies the sent packets according to their priorities, while the inter-node scheduling scheme controls the channel access while minimizing the energy consumption. After a packet is scheduled for transmission, the inter-node scheduling mechanism MACAW, is executed to obtain Loosely Prioritized Random Access (LPRA) among sensor nodes. The contention time is randomly generated with a contention window size CW, where the size is defined by each node's transmission urgency, packet criticality, residual energy, number of hops and queue load. In case there is a collision the CW size is doubled and the packet is retransmitted. When this size reaches a maximum value the packet is dropped.

- CoCo

CoCo [LSR04] protocol is a colouring-based real-time communication scheduling designed for multi-hop scenarios that use IEEE 802.11 MAC protocols and where all exchanged packets are unicast type. It is assumed that node locations are available

at all time, and central node with CoCo running is responsible of communication scheduling. The main objective of CoCo is the schedule of real-time communication, while avoiding collisions and minimizing the overall packet transmission time. CoCo protocol is based on weighted directed graphs and can be compared to the assignment of a colour to each edge of the graph. Here, each colour represents a set of simultaneous communication during disjoint time periods. It employs a colouring selection heuristic algorithm to solve the colouring problem of the graph. CoCo tries to schedule a set of communication events, while it envisages the minimum communication time possible in real-time WSNs. One drawback of CoCo is the central node computational limitation that does not allows for the applicability of CoCo in large-scale WSNs deployments.

G.3.5 Multiple based MAC protocols

- **Reinforcement Learning based MAC (RL-MAC) protocol**

RL-MAC [LE06a] tries to increase while saving energy, by optimizing the active and sleep periods of the frame. Nodes actively infer the state of other nodes, using reinforcement learning based control mechanism. It employs a Markov Decision Process (MDP) to model the process of active time reservation. However, there is the disadvantage of relying on a constant traffic load over a long period of time.

- **Gateway MAC (G-MAC)**

G-MAC [BMFD06] defines a node acting as a gateway for a certain time. After some time this role is rotated by other nodes, in order to balance the load among them. The G-MAC frame is composed by three sub periods: the collection period, the traffic indication period and the distribution period. In the collection period nodes contend for the channel to send packets. In the traffic indication period all nodes wake-up and listen to the channel in order to receive the Gateway Traffic Indication Information (GTIM). This GTIM also maintain synchronization among nodes. G-MAC allows time critical packets to be sent during the collection period. However, this induces to have larger overhead in the gateway node even if the roles are rotating by the nodes this will induce a large overhead and consequently an energy consumption increase. Another disadvantage is the need of the nodes to communicate directly with the gateway, requiring more gateways in the network.

G.4 Comparison of the WSN MAC Protocols

Tables G.3 to G.14 present a comparison of the characteristics of the WSN MAC protocols.

Table G.3: Unscheduled MAC protocols comparison.

MAC characteristics	Picoradio	PMC MAC	DSMAC	E2RMAC	BMAC	EA-ALPL	STEM	CSMA-MPS	TICER	WOR
Action against energy waste	-	-	-	-	-	-	-	-	-	-
Type of scheduling	-	-	-	-	-	-	-	-	-	-
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Rt	Fixed
Node mobility	Static	Static	Static	Static	Static	Static	Static	Static	Static	Static
Node traffic behaviour	Fixed	Fixed	Ad	Fixed	Fi	Ad	Fi	Fi	Fi	Fi
Type of Traffic		Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange		Uni	Uni	Uni	Uni	Uni	Uni	Uni	Uni	Uni
Traffic load		Me	Hi&Me&Lo	Lo	Me	Hi&Me&Lo	Hi&Me&Lo	Hi	Hi	Hi
Slot assignment		-	-	On	-	-	-	-	-	-
Channel Assignment	Sd & Rc	Sd & Rc	-	-	-	-	-	-	-	-
Frequency allocation	Multi	Multi	-	-	-	-	Multi	-	-	-
Frame subinterval	-	-	Sleep	-	-	-	-	-	-	-
Time reduction	-	-	App	-	-	Tf	Pre	-	-	-
Duty cycle tuning	-	-	-	-	-	-	-	-	-	-
Preamble Length Reduction	-	-	-	-	-	-	-	Pack & Pigg Single	Pack & Pigg Single	Pack & Pigg Single
Channel allocation	Dual	Multi	-	Dual	Single	Single	Dual	-	-	-
Preamble reception filtering	-	None	-	-	-	-	-	-	-	-
Communication modes	-	-	-	-	-	-	Be	Be	Be	Be
Multiplex techniques	CDMA	-	-	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA
Wake-up techniques	Radio	-	Schd	Radio	Schd	Schd	Radio	Schd	Schd	Schd
Contention window	-	-	Sg & Fi	Sg & Fi	-	-	-	-	-	-
Clustering		Yes	No	No	No	No	No	No	No	No
Synchronization		No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Channel Technique	-	-	-	-	CCA	CCA	PrS	PrS	PrS	DrS

Table G.4: Unscheduled MAC protocols comparison (cont.).

MAC characteristics	SpecMAC-D	MX-MAC	DPS-MAC	RICER	SyncWUF	PAMAS	CC-MAC	SIFT	Alert	Traw-MAC
Action against energy waste	Co	Co	Il&Co	Co	Co	Il&Co&Oh	Il&Co	Il&Co		
Type of scheduling	-	-	-	-	-	-	-	-	-	
Roles for the nodes	Fixed	Fixed	Fixed	Rt	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static	Static	Adapt	Static	Static	Static	Static	Adapt
Node traffic behaviour	Fi	Fi	Fi	Fixed	Fixed	Fixed	Fi	Fi	Fi	Fixed
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Sensor	Multi	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Uni	Uni	Uni	Uni	Uni	Uni	Var & Uni	Uni	Uni	Uni
Traffic load	Hi	Hi	Hi	Hi	Hi&Me&Lo	Hi	Hi&Me&Lo	Me	Me	Hi&Me&Lo
Slot assignment	-	-	-	-	-	-	-	-	Rc&Ngb	On
Channel Assignment	-	-	-	-	-	Sd & Rc	-	-	Sd	-
Frequency allocation	-	-	-	-	-	-	-	-	Multi	-
Frame subinterval Time reduction	-	-	-	-	-	-	-	-	-	Sleep
Duty cycle tuning	-	-	-	-	Dt	-	-	-	-	Tf
Preamble Length Reduction	Pack & Pigg Single	Pack & Pigg Single	Samp Single	Pack & Pigg Single	Pigg Single	-	-	-	-	DpR
Channel allocation	Single	Single	Single	Single	Single	Dual	Single	Single	Multi	Single
Preamble reception filtering	-	-	-	-	-	-	-	-	-	Micro
Communication modes	Be	Be	Be	Be	-	-	-	-	-	-
Multiplex techniques	CSMA	CSMA	CSMA	-	CSMA	CSMA	CSMA	CSMA	Both	CSMA
Wake-up techniques	Schd	Schd	Schd	Schd	Schd & tone	Radio	Schd	Schd	Schd	Schd
Contention window	-	-	-	-	-	-	-	Sg & Fi	Sg & Fi	-

Table G.5: Unscheduled MAC protocols comparison (cont.).

MAC characteristics	SBRP	ARBP	RARBP
Action against energy waste	Co	Co	Co
Type of scheduling	-	-	-
Roles for the nodes	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static
Node traffic behaviour	Fixed	Fixed	Fixed
Type of Traffic	Sensor	Sensor	Sensor
Node Traffic exchange	Uni	Uni	Uni
Traffic load	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo
Slot assignment	-	On	On
Channel Assignment	-	-	-
Frequency allocation	Single	Single	Single
Frame subinterval Time reduction	-	-	-
Duty cycle tuning	-	App	Range
Preamble Length Reduction	-	-	-
Channel allocation	Single	Single	Single
Preamble reception filtering	-	-	-
Communication modes	-	-	-
Multiplex techniques	CSMA	CSMA	CSMA
Wake-up techniques	Schd	Schd	Schd
Contention window	Sg & Fi	Sg & Fi	Sg & Fi
Clustering	-	-	-
Synchronization	Yes	Yes	Yes
Channel Technique	-	-	-

Table G.6: Scheduled MAC protocols comparison.

MAC characteristics	ARISHA	BitMAC	EMACs	PMAC1	MMAC	FlexiMAC	PMAC2	O-MAC	LMAC	AI-MAC
Action against energy waste	Co	Co	Co	Co	Co&Ho	Co	Co&Il	Ho	Co	Co
Type of scheduling	Cent	Cent	Local	Local	Local	Dist	Dist	Local	Dist	Dist
Roles for the nodes	Fixed	Fixed	Fixed	Adapt	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Node mobility	Adapt	Static	Static	Static	Adapt	Static	Static	Static	Static	Static
Node traffic behaviour	Fixed	Fixed	Fixed	Fixed	Adapt	Fixed	Adapt	Fixed	Fixed	Fixed
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Uni	Uni	Uni	Uni	Var	Uni	Uni	Uni	Uni	Uni
Traffic load	Me	Me	Lo	Lo	Me	Me	Hi&Me&Lo	Me	Hi&Me&Lo	Hi&Me&Lo
Slot assignment	Rc	-	Dist	Dist	Mob	Rc&Sd	Rc&Sd	Rc	Rc&Sd	Rc&Sd
Channel Assignment	-	Sd & Rc	-	-	-	-	-	-	-	-
Frequency allocation	-	-	-	-	-	-	-	-	-	-
Frame subinterval Time reduction	-	-	-	-	-	-	-	-	-	-
Duty cycle tuning	-	Tf	Pre	Pre	Mob	-	Tf	-	-	-
Preamble Length Reduction	-	-	-	-	-	-	-	-	-	-
Channel allocation	Single	Multi	Single	Single	Single	Single	Single	Single	Single	Single
Preamble reception filtering	-	-	-	-	-	-	-	-	-	-
Communication modes	-	Be	-	-	-	-	-	-	-	-
Multiplex techniques	TDMA	TDMA	TDMA	TDMA	TDMA	TDMA	TDMA	TDMA	TDMA	TDMA
Wake-up techniques	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd
Contention window	Sg & Fi	-	-	-	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi
Clustering	Yes	Yes	No	No	Yes	No	No	No	No	No
Synchronization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Channel Technique	-	PrS	-	-	-	-	-	PrS	PrS	PrS

Table G.7: Scheduled MAC protocols comparison (cont.).

MAC characteristics	SS-TDMA	SMAC	TMAC	EZMAC	SWMAC	nanoMAC	FPA	DMAC	QMAC	MS-MAC
Action against energy waste	Co	Co&Il&Ho&Ov	Il		Co	Co&Il		Oh&Il	Co&Il	
Type of scheduling	Dist	Dist	Dist	Dist	Dist	Local		Stag	Dist	Dist
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static	Static	Static	Static	Static	Static	Static	Adapt
Node traffic behaviour	Adapt	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Adapt	Adapt	Fixed
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Conv	Sensor	Sensor
Node Traffic exchange	Uni	Uni	Uni	Uni	Uni	Uni	Uni	Var	Uni	Uni
Traffic load	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo
Slot assignment	Rc&Sd	Rc&Sd	Rc&Sd	Rc&Sd	Dist	-	-	Rc&Sd	Rc&Sd	-
Channel Assignment	-	-	-	-	-	-	-	-	-	-
Frequency allocation	-	-	-	-	-	-	-	-	-	-
Frame subinterval	-	-	Sleep & Act	Sleep & Act	Act	Sleep	Sleep	-	Act& Sleep	Act
Time reduction	-	Pre	Tf	Tf	-	-	-	Tf	Tf&Dt	Mob
Duty cycle tuning	-	-	-	Pack	-	-	-	-	-	-
Preamble Length Reduction	Single	Single	Single	Single	Single	Single	Single	Single	Single	Single
Channel allocation	-	-	-	-	-	-	Pigg	-	-	-
Preamble reception filtering	-	-	-	-	-	-	-	-	-	-
Communication modes	-	-	-	-	-	-	-	-	-	-
Multiplex techniques	TDMA	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA	CSMA
Wake-up techniques	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd
Contention window	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	-	-	Sg & Fi	Sg & Fi	-
Clustering	No	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
Synchronization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Channel Technique	PrS	Cs	Cs	Cs	Cs	Cs	Cs	DaP	-	-

Table G.8: Scheduled MAC protocols comparison (cont.).

MAC characteristics	GSA	Opti. MAC	ADCA	LEACH	NAMA	LAMA	PAMA	En. TDMA	Preamble sampling
Action against energy waste	Co&Il&Ho&Ov	Il&Ho&Ov	Co&Ov	Co	Co	Co	Co		ALOHA
Type of scheduling	Glob	Dist	Stag	Cent	Dist	Dist	Dist	Cent	Co
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Dist
Node mobility	Static	Static	Static	Static	Static	Static	Static	Adapt	Fixed
Node traffic behaviour	Fixed	Adapt	Adapt	Fixed	Fixed	Fixed	Fixed	Adapt	Static
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Multi	Fixed
Node Traffic exchange	Uni	Uni	Uni	Uni	Var	Uni	Uni	Var	Sensor
Traffic load	Hi&Me&Lo	Hi&Lo	-	-	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Cte
Slot assignment	Rc&Sd	Rc&Sd	Rc&Sd	-	Sd	Sd	Sd	Rc	Hi&Lo
Channel Assignment	-	-	-	-	-	-	-	Rc	Sd
Frequency allocation	-	-	-	-	-	-	-	-	Sd & Rc
Frame subinterval Time reduction	Sched	-	-	-	-	-	-	-	-
Duty cycle tuning	Pre	Tf	Dt&Tf	-	-	-	-	Tf	-
Preamble Length Reduction	-	-	-	-	-	-	-	-	-
Channel allocation	Single	Single	Single	Single	Single	Single	Single	Multi	Dual
Preamble reception filtering	-	-	-	-	-	-	-	-	-
Communication modes	-	-	-	-	-	-	-	-	-
Multiplex techniques	CSMA	CSMA	CSMA	TDMA	TDMA	TDMA	TDMA	TDMA	CSMA/TDMA
Wake-up techniques	Schd	Schd	Schd	Schd	-	-	-	Schd	Schd
Contention window	Sg & Fi	Sg & Fi	Sg & Fi	-	Sg & Fi	Sg & Fi	Sg & Fi	-	Sg & Fi
Clustering	Yes	No	No	Yes	No	No	No	No	No
Synchronization	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Channel Technique	Cs	-	-	-	NoB	LiB	Lib	-	PrS

Table G.9: Hybrid MAC protocols comparison.

MAC characteristics	PEDAMACS	TRAMA	FLAMA	μ MAC	PACT	BMA	f-MAC	MMSN	Y-MAC
Action against energy waste		Co	Co	Co&Ov			Co	Co	
Type of scheduling	Cent	Local	Local	Local	Local	Local	-	-	Cent
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Rt	Rt	Fixed	Fixed	Fixed
Node mobility	Adapt	Static	Static	Static	Static	Static	Static	Static	Static
Node traffic behaviour	Fixed	Adapt	Adapt	Adapt	Adapt	Adapt	Fixed	Fixed	Adapt
Type of Traffic	Conv	Both	Both	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Var	Var	Var	Var	Var	Var	Var	Uni	Var
Traffic load	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Me&Lo	Hi&Me&Lo
Slot assignment	-	-	-	Rc&Nghb	NoB	NoB	-	Rc	Rc
Channel Assignment	-	-	-	-	-	-	-	-	Rc
Frequency allocation	-	-	-	-	-	-	Multi	Multi	Multi
Frame subinterval Time reduction	-	-	-	-	-	-	-	-	-
Duty cycle tuning	-	Tf	Tf	Tf&App	Tf	Tf	Pre	-	-
Preamble Length Reduction	Pigg	-	-	-	-	-	-	-	-
Channel allocation	Single	Single	Single	Single	Single	Single	Multi	Multi	Multi
Preamble reception filtering	-	-	-	-	-	-	-	-	-
Communication modes	-	-	-	Be	-	-	-	Be	-
Multiplex techniques	CSMA/TDMA	CSMA/TDMA	CSMA/TDMA	CSMA/TDMA	TDMA	TDMA	-	CSMA/FDMA	TDMA/FDMA
Wake-up techniques	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd
Contention window	-	-	-	Sg & Fi	-	Sg & Fi	-	Sg & Fi	Sg & Fi
Clustering	No	No	No	No	Yes	Yes	Yes	No	No
Synchronization	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Channel Technique	-	-	-	-	-	-	FrD	-	LPL&PrS

Table G.10: Hybrid MAC protocols comparison (cont.).

MAC characteristics	RMAC	X-MAC	CMAC	WiseMAC	RATE EST	SP	MFP	ZMAC	MH-MAC
Action against energy waste	Co	Over&Oh	Oh	Il&Oh	Il&Oh	Il&Oh	Il	Co	
Type of scheduling	-	Local	Dist	Dist	Dist	Dist	Local	Cent	Stag
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static	Static	Static	Static	Static	Static	Static
Node traffic behaviour	Adapt	Adapt	Fixed	Adapt	Adapt	Adapt	Adapt	Adapt	Adapt
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Uni	Var	Uni	Var	Var	Var	Var	Var	Var
Traffic load	Hi&Met&Lo	Hi&Met&Lo	Hi&Met&Lo	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Met&Lo
Slot assignment	Rc&Nghb	Rc&Nghb	Rc&Nghb	-	-	-	-	Rc&Nghb	-
Channel Assignment	-	-	-	-	-	-	-	-	-
Frequency allocation	-	-	-	-	-	-	-	-	-
Frame subinterval Time reduction	-	Sleep&Act	Sched	Act&Sleep	-	-	Act&Sleep	-	-
Duty cycle tuning	-	Tf	Pre	-	-	-	-	Tf	Pre
Preamble Length Reduction	Pigg	Pack & Pigg	-	DiS	DiS	DiS	-	-	Pack
Channel allocation	Single	Single	Single	Single	Dual	Single	Single	Single	Single
Preamble reception filtering	-	-	-	-	-	-	Micro	-	-
Communication modes	-	-	-	-	-	-	-	-	Be
Multiplex techniques	TDMA	CSMA	CSMA	TDMA/CSMA	TDMA/CSMA	TDMA/CSMA	TDMA/CSMA	TDMA & CSMA	CSMA
Wake-up techniques	-	Schd	Schd	Schd	Radio	Schd	Schd	Schd	Schd
Contention window	Sg & Var	-	Sg & Var	-	-	-	-	Sg & Var	Sg & Var
Clustering	No	No	No	No	No	No	No	Yes	No
Synchronization	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes/No
Channel Technique		PrS	CA	PrS	PrS	PrS	PrS&CCA	PrS	PrS

Table G.11: Hybrid MAC protocols comparison (cont.).

MAC characteristics	IEEE 802.15.4	Funneling MAC	SCP-MAC	CrankShaft	PARMAC	HMAC	GANGS	HyMAC	TMCP
Action against energy waste	Co		Co&Oh&Il	Oh	Il&Co	Il&Co		Co	Co
Type of scheduling	Cent	Cent	Glob&Local	Local	Dist	Local	Dist	Cent	-
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Cent	-
Node mobility	Adp & Sta	Static	Static	Static	Static	Static	Static	Fixed	Fixed
Node traffic behaviour	Adapt	Adapt	Adapt	Adapt	Fi	Fi	Fi	Fi	Fi
Type of Traffic	Sensor & Multi	Conv	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Uni& Var	Var	Uni& Var	Uni& Var	Uni	Uni	Uni	Uni	Uni
Traffic load	Lo& Hi	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Me	Hi&Lo	Hi&Lo	Hi&Lo	Hi&Lo
Slot assignment	On	On	On	Rc	Rc	On	Dist	Rc	Rc
Channel Assignment	standard	-	-	-	-	-	-	Multi	Multi
Frequency allocation	standard	-	-	-	-	-	-	Multi	Multi
Frame subinterval Time reduction		-	Sleep&Sched	Sleep&Sched	-	-	-	-	-
Duty cycle tuning		Tf	Tf	Tf	-	-	-	-	-
Preamble Length Reduction		-	Pigg	-	-	-	-	-	-
Channel allocation		Single	Single	Single	Single	Single	Single	Multi	Multi
Preamble reception filtering		-	-	-	-	-	-	-	-
Communication modes	Both	Be	-	-	-	-	-	-	-
Multiplex techniques		TDMA/CSMA	CSMA	TDMA	TDMA	CSMA&TDMA	CSMA&TDMA	TDMA/FDMA	TDMA/FDMA
Wake-up techniques		Schd	Schd	Schd	Schd	Schd	Schd	Schd	-
Contention window		Sg & Fi	Db & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	-
Clustering		Yes	No	No	Yes	No	Yes	No	No
Synchronization		Yes	Yes	Yes	Yes	Yes	Yes*	Yes	Yes
Channel Technique		PrS	SCP&LPL	ScP	-	-	-	LPL	CD & CA

Table G.12: QoS MAC protocols comparison.

MAC characteristics	Q-MAC	EQ-MAC	CoCo	MMSPEED
Action against energy waste			Co&Ov	
Type of scheduling	NoB	Dist	Cent	-
Roles for the nodes	Fixed	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static	
Node traffic behaviour	Fixed	Fixed	Fixed	
Type of Traffic	Prio Sensor	Prio Sensor	Prio Sensor	Prio Sensor
Node Traffic exchange	Uni	Uni	Uni	Var
Traffic load	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo
Slot assignment	Sd	Sd	-	Sd
Channel Assignment	-	-	-	-
Frequency allocation	-	-	-	-
Frame subinterval Time reduction	-	-	-	-
Duty cycle tuning	Pre	-	-	-
Preamble Length Reduction	-	-	-	-
Channel allocation	Single	Single	Single	Single
Preamble reception filtering	-	-	-	-
Communication modes	-	-	-	-
Multiplex techniques	CSMA	TDMA/CSMA	802.11	CSMA
Wake-up techniques	Schd	Schd/-	Schd	Schd
Contention window	Sg & Fi	Sg & Fi	-	Sg & Fi
Clustering	No	No	Yes	No
Synchronization	Yes	Yes	No	Yes
Channel Technique	QoS	QoS	QoS	QoS

Table G.13: Cross-Layer MAC protocols comparison.

MAC characteristics	Chang, A	MACRO	MAC-CROSS Co&I&H&Ov	MINA	Yuan, J	Seada, K	Chiang, M	Madan, R	Cui, S
Action against energy waste	-	-	Dist	Cent	Dist			Cent	
Type of scheduling	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Roles for the nodes	Static	Static	Static	Adapt	Static	Static	Adapt	Static	Static
Node mobility	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Node traffic behaviour	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor	Sensor
Type of Traffic	Var	Uni	Uni	Uni	Var	Uni	Var	Uni	Uni
Node Traffic exchange	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo
Traffic load	-	-	Rc&Sd	Rc&Sd	-	-	-	Rc&Sd	Rc&Sd
Slot assignment	-	-	-	Rc&Sd	-	-	Rc&Sd	-	-
Channel Assignment	-	-	-	Multi	-	-	-	Single	-
Frequency allocation	-	Sched&sleep	-	-	-	-	-	-	-
Frame subinterval Time reduction	-	-	-	-	-	-	-	-	-
Duty cycle tuning	-	-	Pre	-	-	-	-	-	-
Preamble Length Reduction	-	-	-	-	-	-	-	-	-
Channel allocation	Single	Single	Single	Multi	Multi	Single	Multi	Single	Single
Preamble reception filtering	-	-	-	-	-	-	-	-	-
Communication modes	-	-	-	Be	-	Be	-	-	-
Multiplex techniques	CSMA	CSMA	CSMA	TDMA + CDMA/FDMA	CDMA/OFDM		CDMA	TDMA	TDMA
Wake-up techniques	Schd	Schd	Schd	Schd	-	-	-	Schd	Schd
Contention window	-	-	Sg & Fi	-	-	-	-	Sg & Fi	Sg & Fi
Clustering	No	No	Yes	Yes	No	No	No	No	Yes
Synchronization	Yes	No	Yes	Yes	No	No	Yes/No	No	No

Table G. 14: Cross-Layer MAC protocols comparison (cont.).

MAC characteristics	TSMP	Multi-LMAC	RL-MAC	U-MAC	G-MAC	R-MAC2	1-hop MAC	MERLIN	GeRAF
Action against energy waste	Nal	Co	Co&IL&Ho&Ov	IL	IL&Ov&Co		IL	IL	Oh
Type of scheduling	Cent	Dist	Dist	Dist	Cent	Dist	Local	Cent	Dist
Roles for the nodes	Fixed	Fixed	Fixed	Fixed	Rt	Fixed	Fixed	Fixed	Fixed
Node mobility	Static	Static	Static	Static	Static	Static	Static	Static	Adapt
Node traffic behaviour	Fixed	Adapt	Adapt	Adapt	Adapt	Fixed	Fixed	Fixed	Fixed
Type of Traffic	Sensor	Sensor	Sensor	Sensor	Prio Sensor	Sensor	Sensor	Sensor	Sensor
Node Traffic exchange	Var	Uni	Uni	Var	Uni	Uni	Uni	Uni	Uni
Traffic load	Hi&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Me&Lo	Hi&Lo	Hi&Lo	Hi&Me&Lo
Slot assignment	On	Rc&Sd	Sd	-	On	Rc&Sd	-	Rc&Sd	Rc&Nghb
Channel Assignment	Rc	On	-	-	-	-	-	-	-
Frequency allocation	Multi	Multi	-	-	-	-	-	-	-
Frame subinterval Time reduction	Act	-	Act&Sleep	Act&Sleep	Sleep	-	Act&Sleep	-	Sched&sleep
Duty cycle tuning	App	Tf	Stat	Util	Pre	Dt	-	Pre	Pre
Preamble Length Reduction	-	-	-	-	-	Pack	-	-	-
Channel allocation	Multi	Multi	Single	Single	Single	Single	Single	Single	Single
Preamble reception filtering	-	-	-	-	-	-	-	-	-
Communication modes	Be	-	-	-	-	-	-	-	-
Multiplex techniques	TDMA/FDMA	TDMA/FDMA	CSMA	CSMA	TDMA	CSMA	TDMA/CSMA	CSMA	CSMA
Wake-up techniques	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd	Schd
Contention window	Sg & Var	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	Sg & Fi	-	Sg & Fi	Sg & Var
Clustering	No	No	Yes	No	Yes	No	No	Yes	No
Synchronization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Appendix H

Birthday Paradox Problem

H.1 Birthday Paradox

The occupancy problems are widely studied because they can provide heuristic approaches to the relevant problems in probability theory. These occupancy problems deal with pairings of objects. One of the most basic occupancy problem concerns in placing m balls into n bins. Apparently this simple problem is very useful in numerous applications.

H.1.1 Birthday Paradox Problem Solution

The problem is to compute the approximate probability that in a room of n people, at least two have the same birthday. For simplicity, variations in the distribution, such as leap years, twins, seasonal or weekday variations are neglected, as well as the assumption that the 365 possible birthdays are equally likely. We define as P_A , the probability of at least two people in the room having the same birthday, while $P_{A'}$ is the probability of not having two people with the same birthday. Since the events are independent of each other, the probability of all of the events occurring is given by the product of the probabilities of each of the events occurring. As an example we consider $n=23$. In consequence, $P_{A'}$ could be calculated as $P_1 \cdot P_2 \cdot P_3 \cdot P_4 \cdot \dots \cdot P_{23}$. The 23 people correspond to 23 independent events. Each event can be defined as the corresponding person to have a unique birthday among the analyzed people. In event 1 since there is no previous analyzed people the probability is given by $P_1 = 365/365 = 1$. For event 2, we must consider the previous event, i.e., event 1. Considering that birthdays are equally probable to happen on each one of the 365 days of the year, $P_2 = 364/365 = 0.997$. This happens because, the objective is to calculate the probability of not having two people with the same birthday and if person 1 was born on any of the 365 days of the year, then person 2 was born on any of the other 364 days of the year. Hence, person 1 and 2 do not share the same birthday. For person 3, the probability $P_3 = 363/365 = 0.994$. Persons 1, 2 and 3 do not share their birthday. The analysis continues until person 23 is reached, whose probability $P_{23} = 343/365 = 0.939$. $P_{A'}$ is given by the product of all the individual probabilities as follows:

$$P_{A'} = 365/365 \times 364/365 \times 363/365 \times \dots \times 343/365 = 0.49270 \quad (\text{H.1})$$

In consequence, the probability of at least two people in the room having the same birthday, P_A , is given by:

$$P_A = 1 - 0.49270 = 0.5073 \quad (\text{H.2})$$

Generalizing this process to a group of n people, where p_n is the probability of at least two of the n people sharing a birthday. As discussed before it is easier to calculate the complement of p_n ($p_{n'}$), i.e., that all n birthdays are different. According to the pigeonhole principle if $n > 365$ then $p_{n'} = 0$. When $n \leq 365$, the probability $p_{n'}$ is given by:

$$\begin{aligned}
 p_{n'} &= 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \dots \times \left(1 - \frac{n-1}{365}\right) \\
 &= \frac{365 \times 364 \times \dots (365 - n + 1)}{365^n} \\
 &= \frac{n! \cdot \binom{365}{n}}{365^n} \quad (\text{H.3})
 \end{aligned}$$

The pigeonhole principle states that if n items are put into m pigeonholes with $n > m$, then at least one pigeonhole must contain more than one item. The case of at least two of the n persons having the same birthday is the complement of all n birthdays being different. Therefore, probability p_n is given by

$$p_n = 1 - p_{n'} \quad (\text{H.4})$$

Since factorial of 365 is an extremely large number, it is computationally easier to just evaluate each term. In Figures H.1 and H.2 are presented the curves for the probability of two people that do not have the same birthday and the probability that at least two people have the same birthday in a group of n people, respectively.

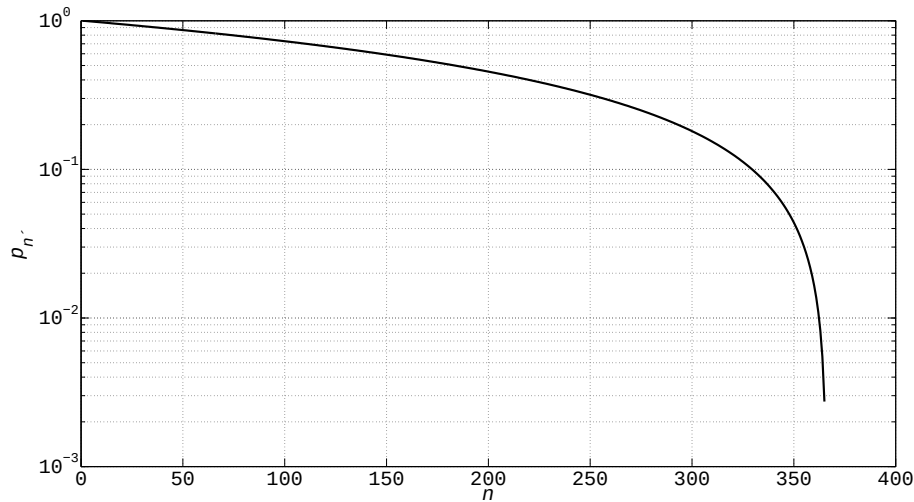


Figure H.1: Probability that two people do not have the same birthday in a group of n people.

H.2 Birthday Paradox applied to packet collision analysis in WSN

The birthday paradox comes from the observation that birthday collisions are likely to happen with relatively few people. The birthday paradox can be viewed as a “bin and balls

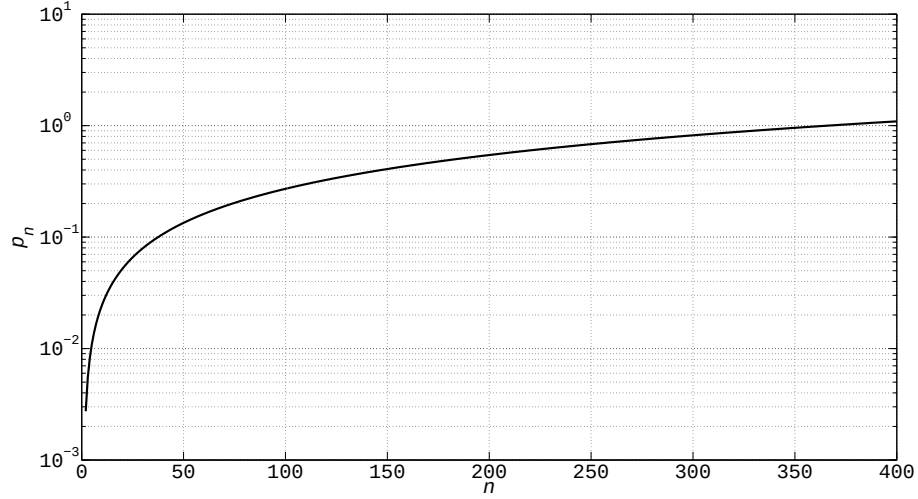


Figure H.2: Probability that at least two people have the same birthday in a group of n people.

occupancy” problem. Each of the m people is a ball, assigned independently at random to one of $p=365$ bins, which are the days of the year. The objective is to determine the probability of some bin containing two or more balls. However, in our case for the sake of simplicity, we assume that each of the m balls represents a node, while each of the p bins is a CW_2 time slot. Or, in combinatorial probability language, the envisaged success probability may be defined as the probability that the lowest order bin contains more than one ball and the remaining balls should be distributed for the remaining (highest order) bins. The remaining bins may contain more than one ball, and no ball should remain outside a bin. If the lowest order (first) bin does not contain any balls, then the next order bin is treated as the lowest order bin. Balls are indistinguishable. Since we consider only the balls indistinguishable we should use combinations with repetition. A k -combination with repetitions from a set S is given by a sequence of k not necessarily distinct elements of S , where order is not taken into account: two sequences of which one can be obtained from the other by permuting the terms define the same multiset, as follows:

$$C(n+k-1, k) = C(n+k-1, n-1) \quad (\text{H.5})$$

To begin with we must calculate the total number of possible cases. In this example we assume that $CW_1^{max} = 8$ and $n=5$ nodes. In consequence, the total number of possible cases, T_n , is given by:

$$T_n = C(8+5-1, 5) = 792 \quad (\text{H.6})$$

This is the same as the number of integer solutions of the equation:

$$X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8 = 5 \quad (\text{H.7})$$

Each one of the X_i values corresponds to one of the time slots from the contention window. Now if X_1 is greater than 1 node we put $y_1 = X_1 - 2$, $y_2 = X_2$, $y_3 = X_3$, $y_4 = X_4$, $y_5 = X_5$, $y_6 = X_6$, $y_7 = X_7$, $y_8 = X_8$ and must find the number of integer solutions as follows:

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 = 5 - 2 = 3 \quad (\text{H.8})$$

By applying the combinations with repetition formula the number of possible combinations with at least 2 nodes in the first slot, and the remaining ones distributed among the higher order slots, is given by:

$$C(3 + 8 - 1, 7) = C(10, 7) = 120 \quad (\text{H.9})$$

The same would be true in the cases when $X_1 > 2$ or $X_1 > 3$ or $X_1 > 4$. For the case when $X_1 > 2$ we put $y_1 = X_1 - 3$, $y_2 = X_2$, $y_3 = X_3$, $y_4 = X_4$, $y_5 = X_5$, $y_6 = X_6$, $y_7 = X_7$, $y_8 = X_8$ and must find the number of integer solutions of

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 = 5 - 3 = 2 \quad (\text{H.10})$$

By the same reasoning as before, the number of possible combinations with at least 3 nodes in the first slot and the remaining ones distributed among the higher order slots is given by:

$$C(2 + 8 - 1, 7) = C(9, 7) = 36 \quad (\text{H.11})$$

For the $X_1 > 3$ case we put $y_1 = X_1 - 4$, $y_2 = X_2$, $y_3 = X_3$, $y_4 = X_4$, $y_5 = X_5$, $y_6 = X_6$, $y_7 = X_7$, $y_8 = X_8$ and must find the number of integer solutions of

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 = 5 - 4 = 1 \quad (\text{H.12})$$

By the same reasoning as before the number of possible combinations with at least 4 nodes in the first slot and the remaining ones distributed among the higher order slots is given by:

$$C(1 + 8 - 1, 7) = C(8, 7) = 8 \quad (\text{H.13})$$

For the $X_1 > 4$ case we put $y_1 = X_1 - 5$, $y_2 = X_2$, $y_3 = X_3$, $y_4 = X_4$, $y_5 = X_5$, $y_6 = X_6$, $y_7 = X_7$, $y_8 = X_8$ and must find the number of integer solutions of

in the lowest order slot and the total number of possible combinations of distributing n nodes among CW_{max} time slots. This ratio is given as follows:

$$N_c = \frac{N_d}{T_n} = \frac{494}{792} = 0.6237 \quad (\text{H.16})$$

The number of different combinations in CW (with and without collisions) for the assignment of the nodes by the time slots obtained by combinatorial theory is given by Equation H.17:

$$N_t(m) = \frac{(CW_2^{max} + m - 1)!}{m!(CW_2^{max} - 1)!} \quad (\text{H.17})$$

The number of different combinations that lead to an effective collision among nodes is given by Equation H.18:

$$N_f(m) = \sum_{i=1}^{CW_2^{max}} \frac{(m - r + CW_2^{max} - i)!}{(CW_2^{max} - i)!(m - r)!} \quad (\text{H.18})$$

In the *birthday paradox* the bins are distinguishable and balls are indistinguishable. However, for our model we need to consider the bins and balls both indistinguishable. This means that besides the amount of balls that are inside of the lowest order bin, the number of the ball also matters. For the sake of simplicity, we assume that each of the n balls represents a node, while each of the p bins is a CW time slot. This means that the envisaged success probability may be defined as the probability that the lowest order bin contains more than one ball and the remaining balls should be distributed for the remaining (highest order) bins. The remaining bins may contain more than one ball, and no ball should remain outside a bin. If the lowest order (first) bin does not contain any balls, then the next order bin is treated as the lowest order bin. To begin with, the number of different arrangements in CW (with and without collision) for the assignment of nodes by the time slots is obtained by arrangements with repetition. As any of the CW^{max} slots occurs arbitrarily often so that it can be chosen several times, then one must apply arrangements with repetition. The total number of possibilities, given by Equation H.19, is obtained by imposing the condition that any number of nodes can be put in a slot:

$$A_t(n) = (CW^{max})^n \quad (\text{H.19})$$

To obtain the number of possibilities that exactly one node chooses the i -th lowest order slot and the remaining ones choose the subsequent slots, the solution is also given by arrangements with repetition. If the lowest order slot is selected by only one node, then the number of different possibilities is given by an arbitrary assignment of the $n - 1$ remaining nodes to the $CW^{max} - r$ remaining slots, while r varies between 1 and CW^{max} . The variable r is the number of the lowest order slot that is selected by only one node. Therefore, the number of arrangements, A_s , for the cases when the lowest order slot is

chosen by exactly one node is expressed by:

$$A_s(n) = n \cdot \sum_{j=1}^{CW^{max}} (CW^{max} - j)^{(n-1)} \quad (\text{H.20})$$

Thus, the number of possibilities for the lowest order slot to be chosen by more than one node, A_f is given by:

$$A_f(n) = A_t(n) - A_s(n) \quad (\text{H.21})$$

The probability, $P_{eF}(n)$, of at least two nodes choosing the lowest order slot, while considering slots and nodes indistinguishable is given by:

$$P_{eF}(n) = \frac{A_f(n)}{A_t(n)} \quad (\text{H.22})$$

The probability, $P_{eF}(n)$, that at least two nodes choose the lowest order slot with $CW^{max} = 365$ is presented in Figure H.4

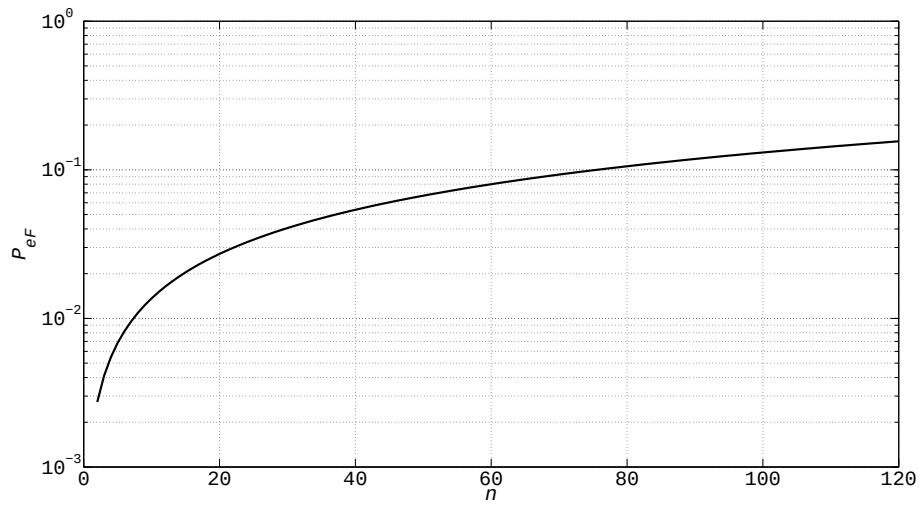


Figure H.4: Probability that at least two nodes choose the lowest order slot with $CW^{max} = 365$.

Appendix I

Computation of the CW1 and CW2 Collision Probabilities

The Matlab algorithm to analyze the CW₁ collision probability arising from the simulations can be described as follows:

- The packet generation initial instant value and the slot choice for each node and all the 50 simulation readings (packets) are collected by using six seeds and stored in a vector;
- For each equal packet generation initial instant time, the algorithm checks which nodes present the same slot choice. The nodes' slot collision flag is set to 1 for the nodes that have the same packet generation initial instant time and slot choice. Otherwise, they are assigned a value of 0. Each node has a slot collision flag to represent if the respective slot has been also chosen by other nodes. This procedure is performed in both contention windows (CW₁ and CW₂);
- If the least order slot is chosen by more than one node, then the collision ratio of the reading i is equal to 1. Otherwise, the collision ratio of the respective reading i is 0. Both contention windows are analyzed simultaneously in this stage;
- When collision ratio is equal to 1 then the $E[S]$ is equal to the number of nodes that have chosen the respective least order slot. When the collision ratio is 0 then $E[S] = 0$;
- After the previous steps, the algorithm checks whether there are more packets to be analyzed. If so, it begins with the first stage of this algorithm. Otherwise, the CW₁ and CW₂ collision probabilities are computed (for the respective contention window);
- The CW₂ collision probability calculation is only performed if at least two nodes are present in the second contention window (CW₂). Otherwise, there is no chance that a collision occurs;
- The final phase of the algorithm computes the ratio between the total number of collision ratio readings, ν , with value 1 and the total number readings performed, β , for the CW₁ and CW₂ collision probabilities;
- The threshold which is applied to check if there is enough nodes to guarantee a transmission (2 nodes minimum) is given by:

$$\begin{cases} P_{cF} = \frac{\sum \nu}{\beta} & \text{if } E[S] > 1 \\ P_{cF} = 0 & \text{if } E[S] \leq 1 \end{cases} \quad (1.1)$$

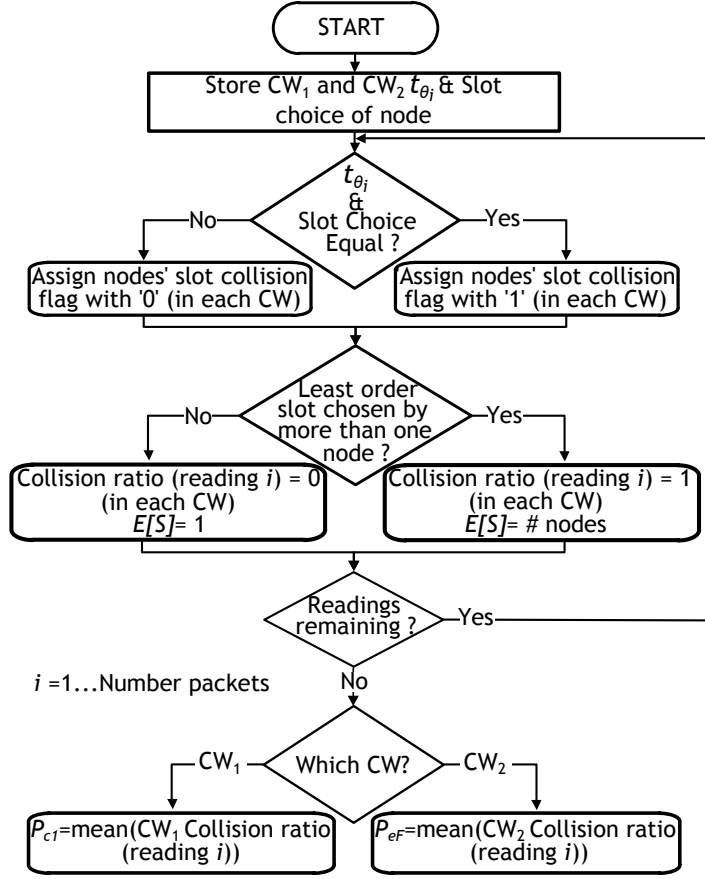


Figure I.1: Flowchart for the algorithm to analyze the CW₁ and CW₂ collision probabilities.

For the unsaturated regime, we have made some minor modifications in the aforementioned CW₁ and CW₂ algorithm. Since the packet generation initial instant times of the nodes are uniformly distributed, we had to implement a routine that identifies the G -th interval, to which the packet generation initial instant value belongs to. For the nodes that are in the same G -th interval, the algorithm performs the same procedures (like for the saturated regime).

For the CW₂ collision probability under unsaturated regime, Equation I.1 is rewritten as follows:

$$\begin{cases} \widehat{P_{cF}} = \frac{\sum \nu}{\beta} & \text{if } \widehat{E[S]} > 1 \\ \widehat{P_{cF}} = 0 & \text{if } \widehat{E[S]} \leq 1 \end{cases} \quad (I.2)$$

The flowchart for these CW₁ and CW₂ collision probabilities algorithms is presented in Figure I.1.

Appendix J

Extra Results for the MC-SCP-MAC Protocol

Extra results for the MC-SCP-MAC protocol are presented in the following sections of this Appendix.

J.1 Extra Results of the Collision probabilities of MC-SCP-MAC

Figure J.1 presents the MC-SCP-MAC detailed simulation results for the CW_1 collision probability in saturated and unsaturated regimes, for $CW_1^{max} = 8$.

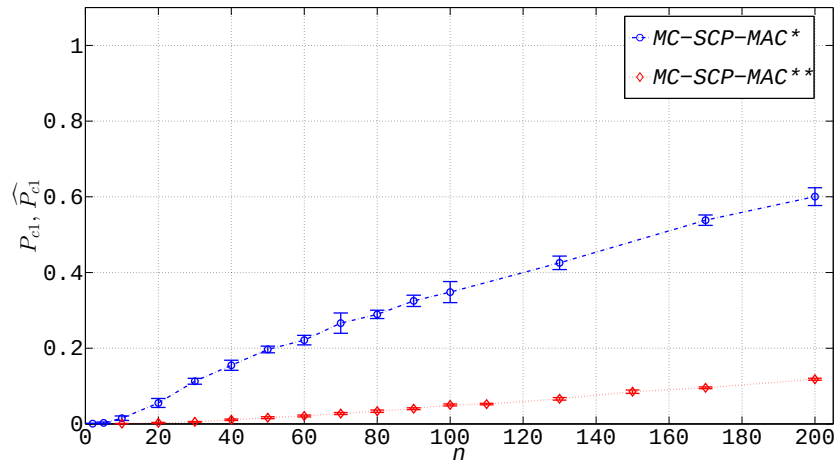


Figure J.1: MC-SCP-MAC simulation results for the CW_1 collision probability as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure J.2 presents the MC-SCP-MAC detailed simulation results for the expected number of nodes that pass from CW_1 to CW_2 in the saturated and unsaturated regimes, for $CW_1^{max} = 8$.

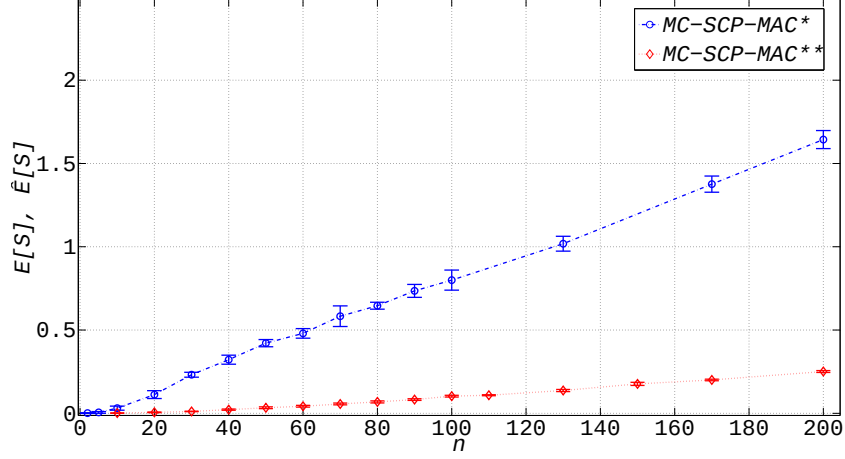


Figure J.2: MC-SCP-MAC simulation results for the $E[S], \hat{E}[S]$ as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_1^{max} = 8$.

Figure J.3 presents the detailed simulation results for the CW_2 collision probability from the MC-SCP-MAC in saturated and unsaturated regimes, whilst considering $CW_k^{max} = 8$, $k \in \{1, 2\}$.

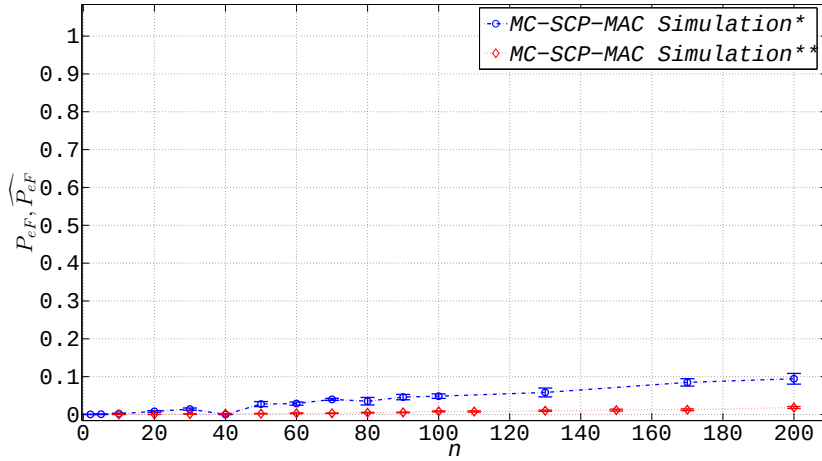


Figure J.3: MC-SCP-MAC simulation results for the CW_2 collision probability as a function of n in saturated (*) and unsaturated (**) regimes, for $CW_k^{max} = 8$, $k \in \{1, 2\}$

J.2 Extra Results for the Energy Performance from the IR Concept

Figure J.4 includes similar analysis for the energy consumption per node whilst considering that each node generates and sends 600 packets to the PAN. It is observable that the increase of the number of slot channels leads to a higher energy consumption per node for a value of $N_{ch} = 8$ slot channels. For the case when the MC-SCP-MAC has $N_{ch} = 8$ slot channels available, the energy consumption is similar for the different network sizes.

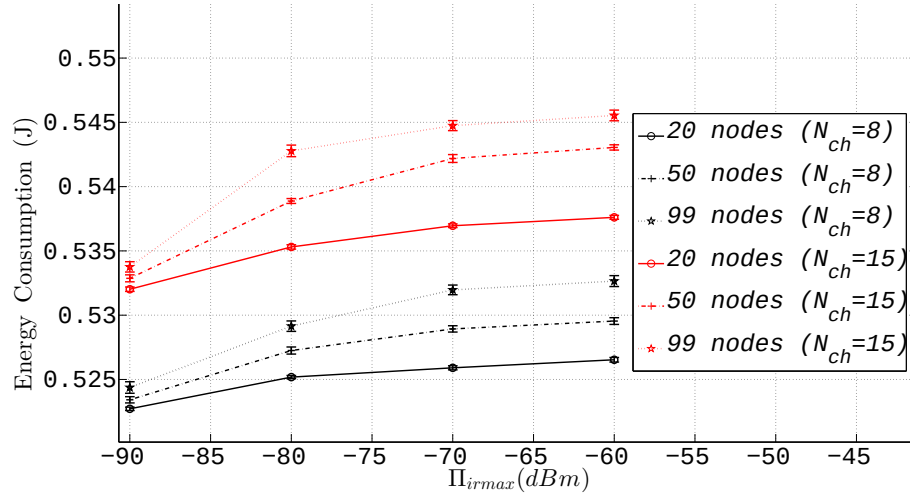


Figure J.4: Average energy consumption per node as a function of Π_{irmax} , when IR is enabled for different sizes of network (50 packets) and number of data slot channels, i.e., $N_{ch} \in \{8, 15\}$.

J.3 Extra Results of the Impact of Traffic Patterns in the Overall Performance

Figure J.5 presents detailed results for the aggregate throughput for the MC-SCP-MAC, MC-LMAC, MMSN and CSMA protocols, with periodic traffic generation. These results provide a detailed description of the results depicted in Figure 8.35.

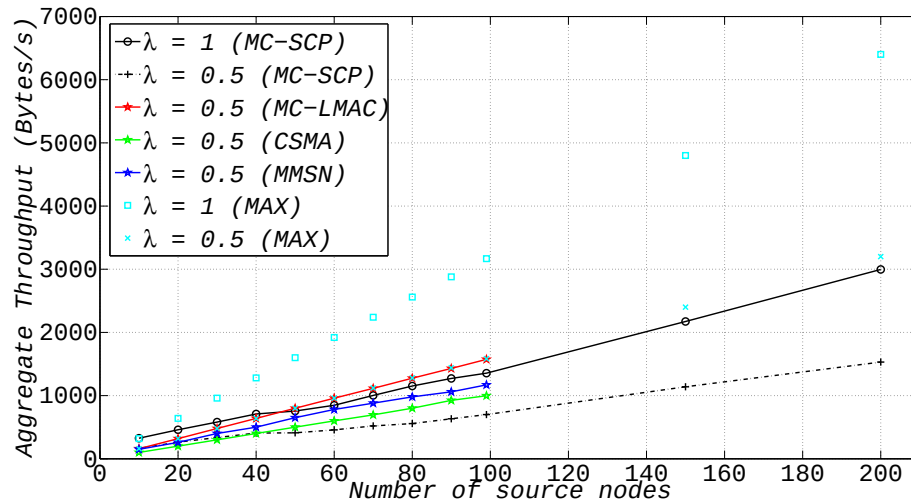


Figure J.5: Aggregate throughput as a function of the number of sources for MC-SCP-MAC, MC-LMAC, CSMA and MMSN with periodic traffic generation.

Figure J.6 shows the aggregate throughput for the MC-SCP-MAC protocol with exponential and periodic traffic generation for $\lambda \in \{1/2; 1\} s^{-1}$. These results provide a detailed description of the results shown in Figure 8.35.

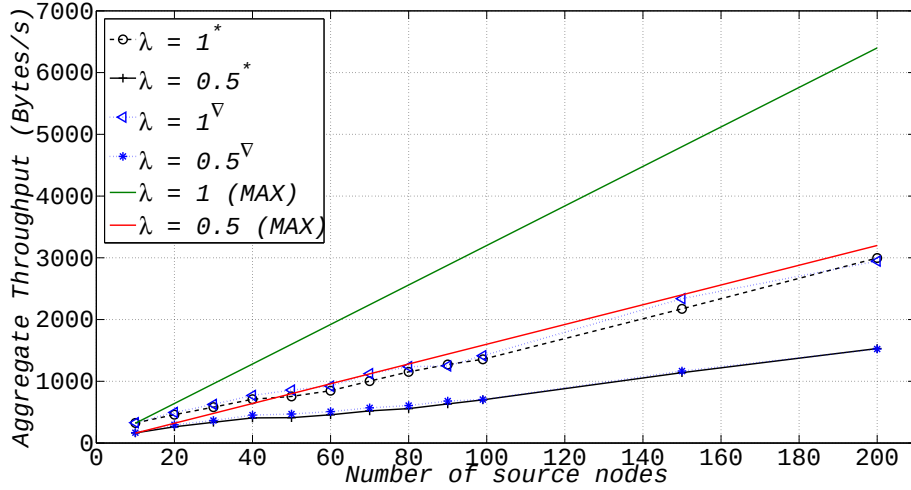


Figure J.6: Aggregate throughput as a function of the number of sources for MC-SCP-MAC with periodic (*) and exponential (∇) traffic generation.

J.4 Extra Results of the Impact of Traffic Patterns in Higher Density Deployments

Figure J.7 shows the aggregate throughput for the MC-SCP-MAC, MC-LMAC, MMSN and CSMA protocols with periodic traffic generation. These results describe in detail the results shown in Figure 8.40.

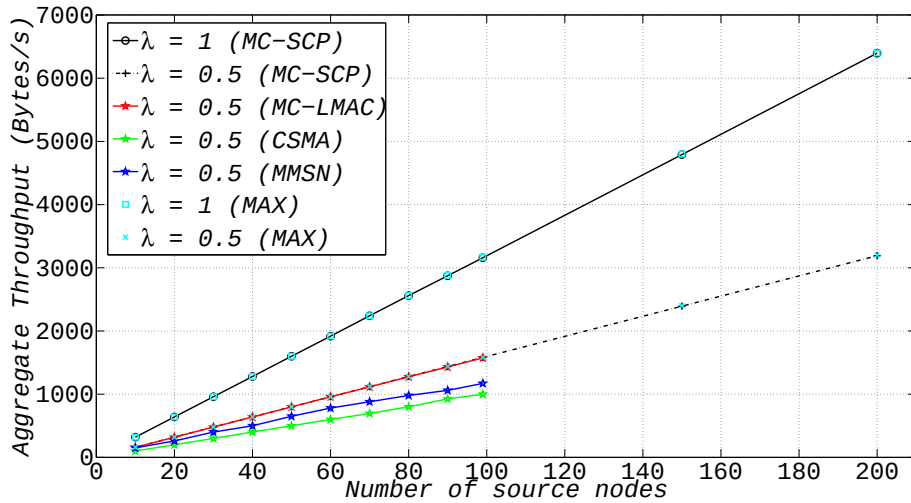


Figure J.7: Aggregate throughput as a function of the number of sources for the MC-SCP-MAC, MC-LMAC, CSMA and MMSN protocols with periodic traffic generation in the $50 \times 50 \text{ m}^2$ deployment scenario.

Figure J.8 presents the aggregate throughput for the MC-SCP-MAC protocol with periodic and exponential traffic generation. These results describe in detail the results from Figure 8.40.

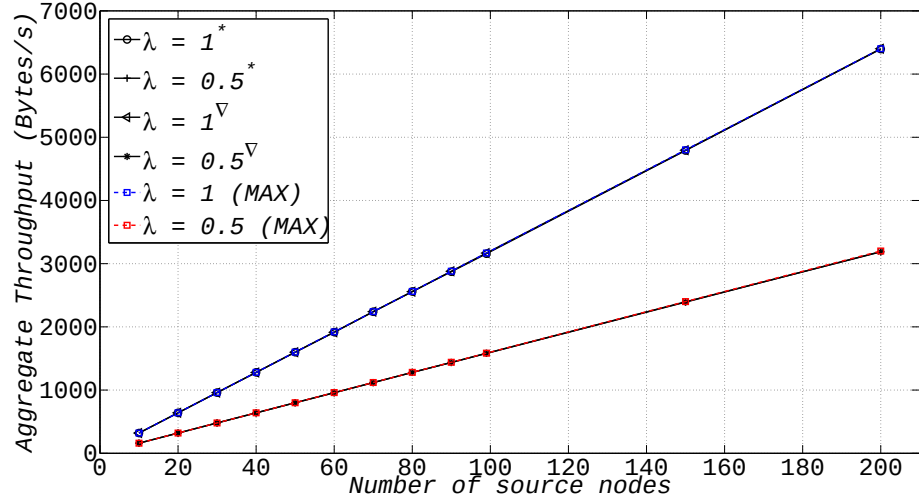


Figure J.8: Aggregate throughput as a function of the number of sources for MC-SCP-MAC protocol with periodic (*) and exponential (▽) in the $50 \times 50 \text{ m}^2$ deployment scenario.

J.5 Extra Results of the MC-SCP Performance Analysis in the Cluster Topology

Figure J.9 presents the aggregate throughput metric of MC-SCP when IR is disabled with the number of slot channels as a parameter for traffic generation rates of $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ considering an exponential profile. Figure J.9 shows that, as the number of slot channels increases, the aggregate throughput decreases. The highest values of aggregate throughput correspond to the case when the data generation rate is higher.

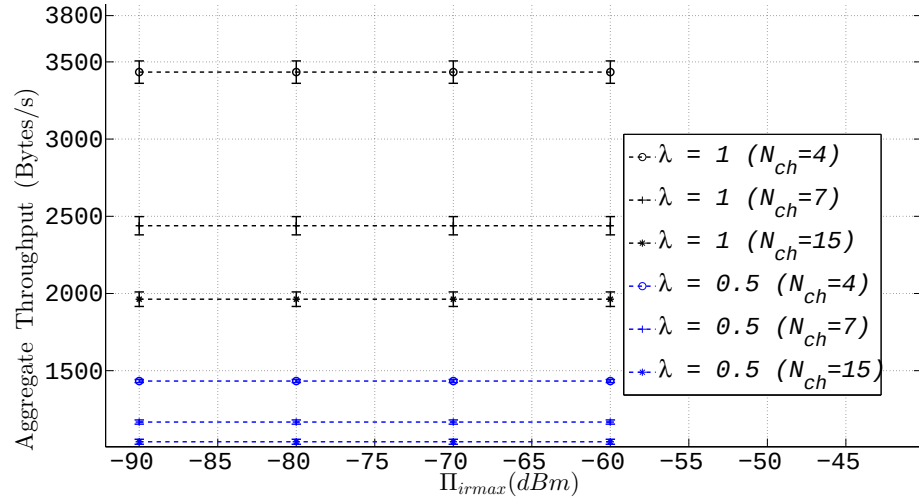


Figure J.9: Aggregate throughput as a function of Π_{irmax} for MC-SCP-MAC when IR is disabled with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} \text{ s}^{-1}$).

The results for the delivery ratio when IR is disabled with the number of slot channels as a parameter for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$ considering an exponential profile are presented in Figure J.10. Figure J.10 shows that as the number of slot channels increases, the delivery ratio decreases. The highest values of delivery ratio correspond to the case when the data generation rate is higher.

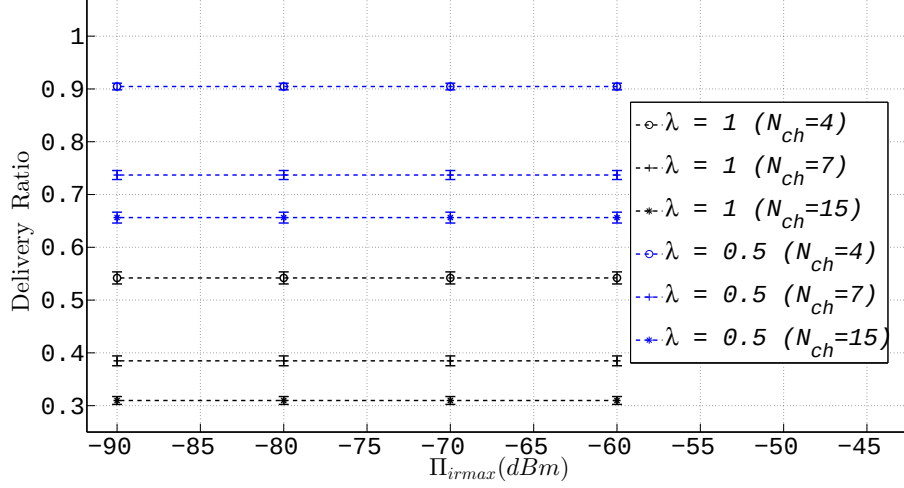


Figure J.10: Delivery ratio as a function of Π_{irmax} for MC-SCP-MAC when IR is disabled with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} \text{ s}^{-1}$).

The results for the energy consumption per node when IR is disabled with the number of slot channels as a parameter for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$, whilst considering an exponential profile, are presented in Figure J.11. From Figure J.11, we conclude that, as the number of slot channels increases, the energy consumption increases. The highest values of energy consumption correspond to the case when the data generation rate is lower. In Figure J.11 the energy consumption whilst considering a traffic generation rate $\lambda = 1 \text{ s}^{-1}$ presents similar values as the number of slot channels increases.

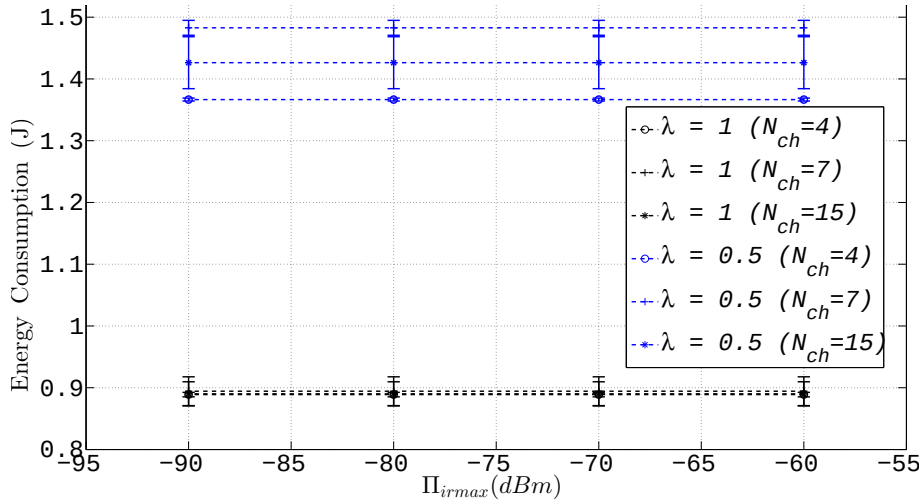


Figure J.11: Energy consumption per node as a function of Π_{irmax} for MC-SCP-MAC when IR is enabled (*) and disabled (∇) with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} \text{ s}^{-1}$).

Figure J.12 presents the results for the end-to-end latency when IR is disabled with the number of slot channels as a parameter for traffic generation rates $\lambda \in \{0.5; 1\} \text{ s}^{-1}$, whilst considering an exponential profile. From Figure J.12 we can conclude that, as the number of slot channels increases the latency is constant for all the cases. The values of the latency vary from 21.2 s to 21.8 s for all the considered number of slot channels.

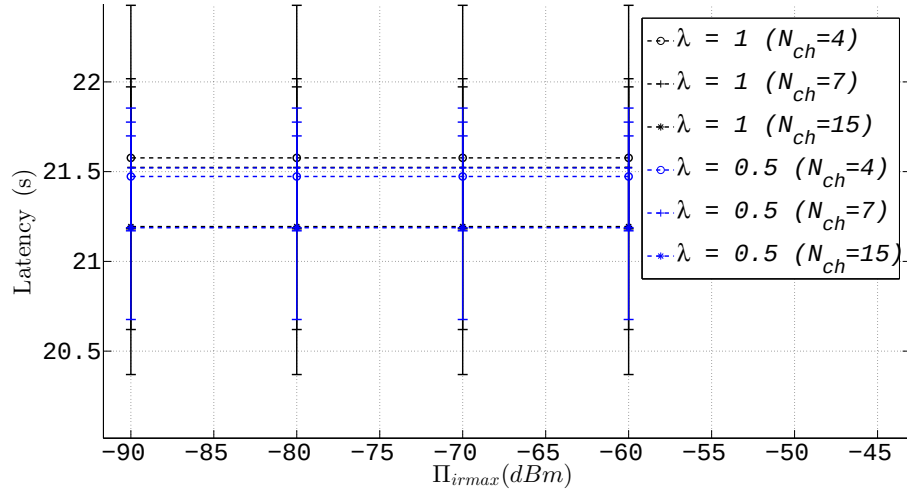


Figure J.12: Latency as a function of Π_{irmax} for MC-SCP-MAC when IR is enabled (*) and disabled (∇) with the number of slot channels as a parameter for exponential traffic generation ($\lambda \in \{0.5; 1\} \text{ s}^{-1}$).

J.6 Extra Results of the Impact of Density in the MC-SCP-MAC Protocol

Figure J.13 addresses the aggregate throughput of MC-SCP-MAC in terms of side length of the deployment scenario for a periodic traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$.

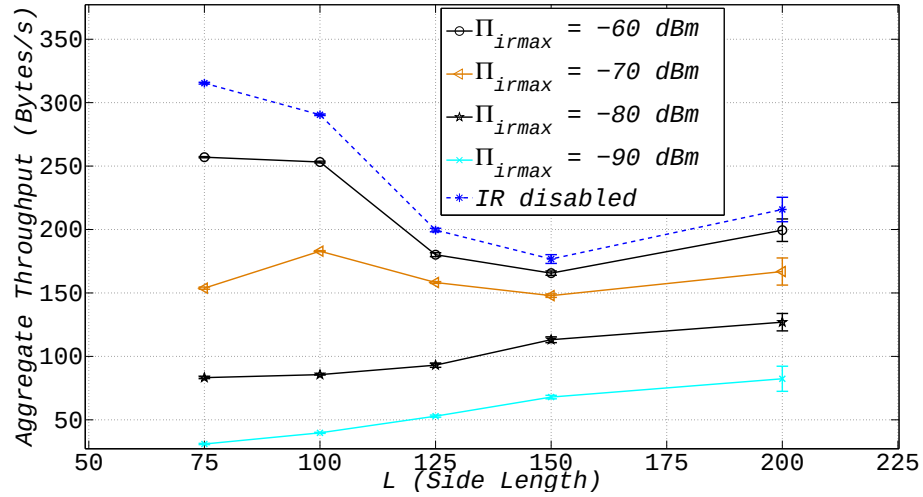


Figure J.13: Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with periodic traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

It is observable that the highest aggregate throughput is verified when the IR is disabled, while the case with different values of sensing range, Π_{irmax} , always presents the highest values of aggregate throughput. The low values of aggregate throughput verified when IR is enabled is caused by the drop of redundant data packets. The case with the lowest value of sensing range (i.e., $\Pi_{irmax} = -60 \text{ dBm}$) is the one that presents the highest values of aggregate throughput when IR is enabled. As observed in Figure 8.45, for a value of the side length larger than 150 m the aggregate throughput increases.

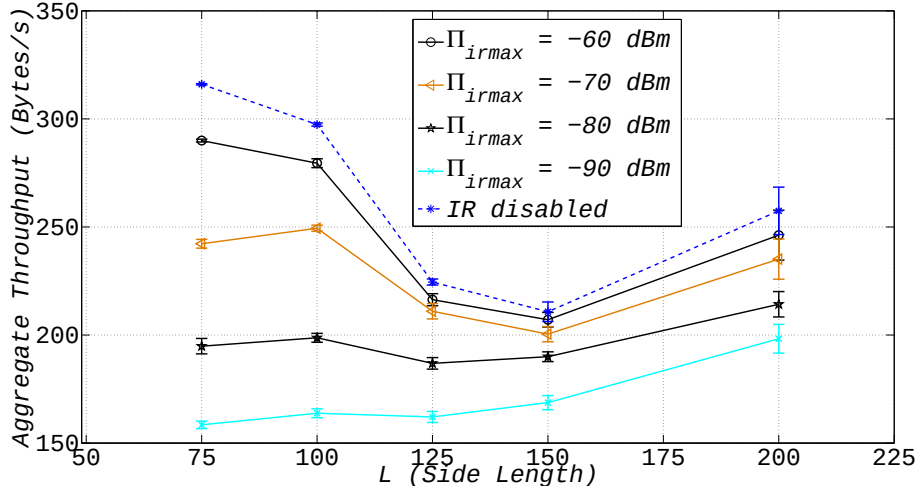


Figure J.14: Aggregate throughput in MC-SCP-MAC as a function of the deployment scenario side lengths with exponential traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

Figure J.14 presents the aggregate throughput of MC-SCP-MAC as a function of the side length of the deployment scenario when considering an exponential traffic profile with a generation rate of $\lambda = 1/10 \text{ s}^{-1}$. In here, the highest aggregate throughput is verified when the IR is disabled, while the case with different values of sensing range Π_{irmax} presents always the lowest values for the aggregate throughput. By comparing Figures J.13 and J.14, we are able to conclude that, under the exponential traffic profile, MC-SCP-MAC achieves better aggregate throughput, when IR is enabled or disabled. The case with the longest value of sensing range (i.e., $\Pi_{irmax} = -60 \text{ dBm}$) is the one that presents the highest values of aggregate throughput (when IR is enabled).

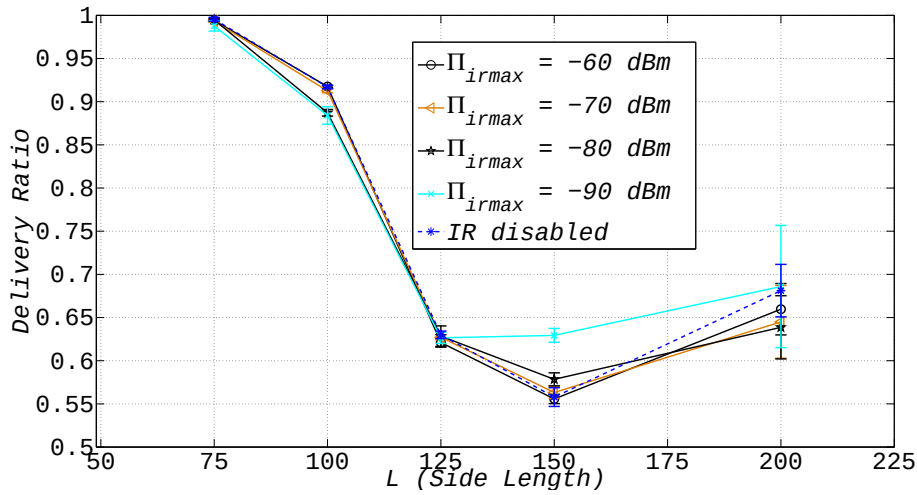


Figure J.15: Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

Figure J.15 shows the delivery ratio as a function of the side length of the deployment scenario for MC-SCP-MAC when considering a periodic traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$. It is observable in these conditions that the delivery ratio presents a similar behaviour to the one shown in Figure 8.47 for the MC-SCP-MAC (under periodic traffic profile generation). In denser scenarios, the delivery ratio achieves the maximum value. As the side length becomes longer, the delivery ratio decreases. For side lengths

longer than 150 m, the delivery ratio starts to increase again.

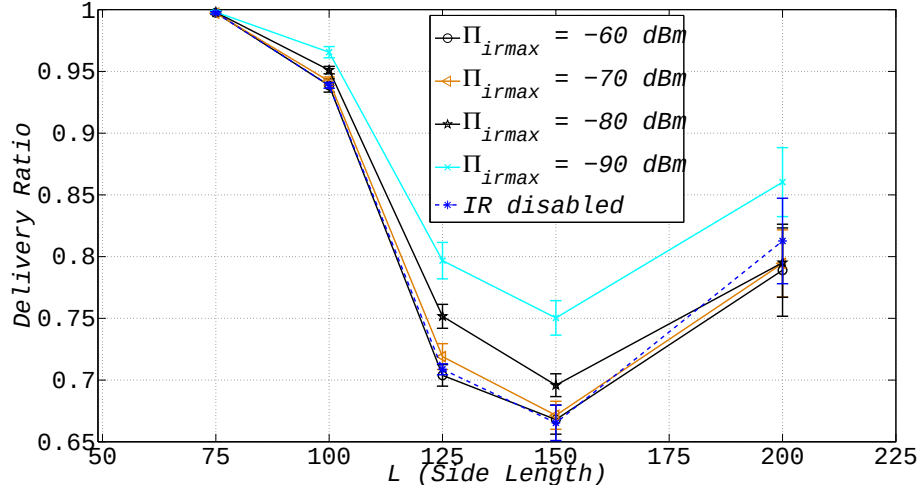


Figure J.16: Delivery ratio of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

Figure J.16 addresses the delivery ratio of MC-SCP-MAC as a function of the side length of the deployment scenario whilst considering an exponential traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$. By comparing these results with the ones from Figure J.15, for side lengths that vary between 50 and 125 m, the delivery ratios are similar, whereas for side lengths longer than 125 m, in the exponential case, the delivery ratios are higher than is in the periodic one. Figure J.17 presents the latency of MC-SCP-MAC as a function of the side length of the deployment scenario when considering a periodic traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$.

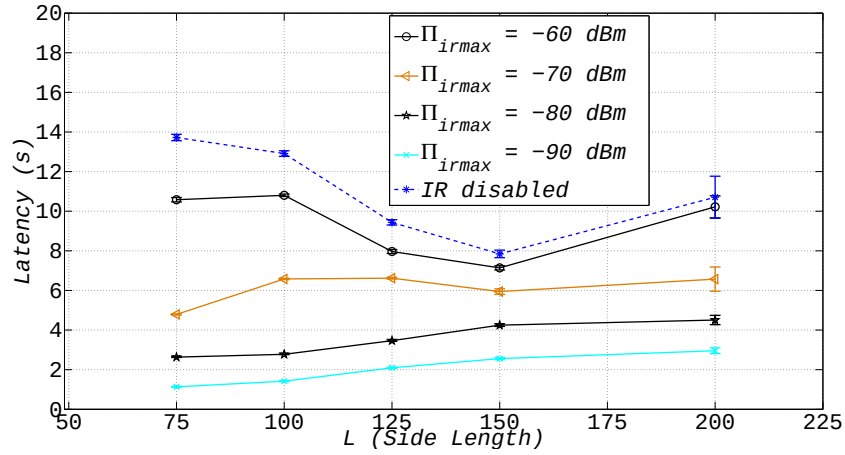


Figure J.17: Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

It is observable that MC-SCP-MAC presents lower values for the latency with the IR enabled, for all the values of the sensing range, Π_{irmax} . As the value of sensing range, Π_{irmax} , increases, the latency also increases, for all the considered side lengths. The short values for the latency verified in the case in which the IR is enabled are due to the reduction of the redundant data packets waiting in queue to be transmitted. The decrease of the data generation rate leads to a slight decrease of the mean latency, for all the considered cases (when compared with the results from Figure 8.49). As the

side lengths becomes longer the latency for the cases with IR enabled and sensing values $\Pi_{irmax} \in \{-90; -80\}$ dBm presents similar values (which are the shortest values of latency in these tests). Figure J.18 shows the results for the latency of MC-SCP-MAC in terms of the side length of the deployment scenario whilst considering an exponential traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$.

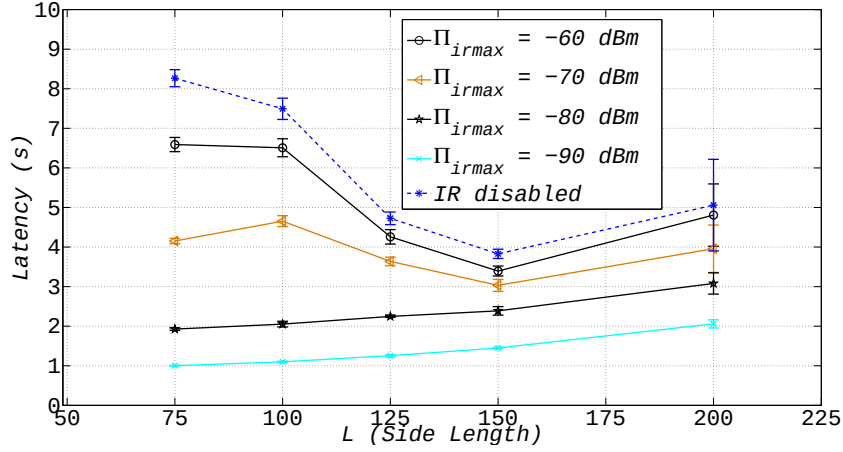


Figure J.18: Latency of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

The verified latency is shorter in the case with the IR enabled for all the sensing range values. As the value of sensing range, Π_{irmax} , increases, the latency also increases (for all the considered side lengths). As the side lengths get longer, the latency presents similar values for the cases when IR is enabled, for values for the sensing range $\Pi_{irmax} \in \{-90; -80\}$ dBm and are the smallest values of latency in these tests. For side lengths that vary between 75 and 150 m, the values of the latency decrease for all the cases except for sensing values $\Pi_{irmax} \in \{-90, -80\}$ dBm, in which they increase. For side lengths longer than 150 m, the values for the latency show a small increase.

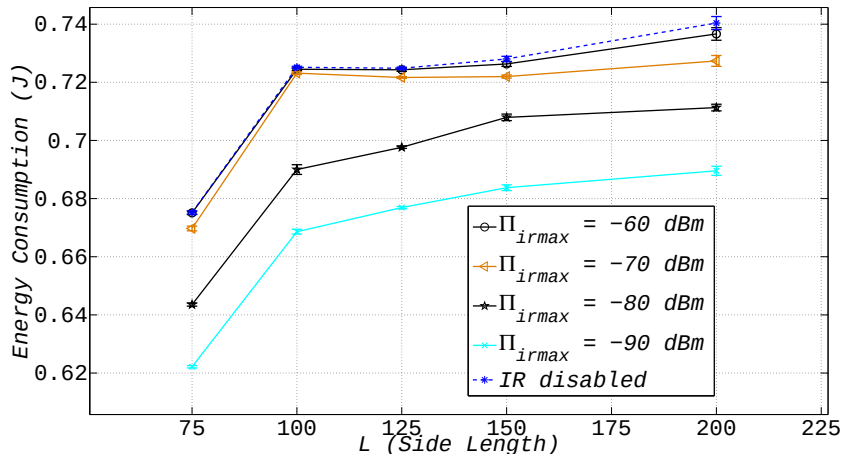


Figure J.19: Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with periodic traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

By comparing these results with the ones from Figure J.17, for all the considered side lengths, the latency is shorter when exponential traffic profile is preferred. Figure J.19 presents the results for the energy consumption as a function of the side lengths whilst considering periodic traffic profile of MC-SCP-MAC with a generation rate $\lambda = 1/10 \text{ s}^{-1}$, as

well as the enabling and disabling of the IR. As the side length becomes longer the energy consumption also increases, as expected. By comparing these results with the ones from Figure 8.51 (with a higher data generation rate) the energy consumption is higher in the case where the data is generated in a much lower frequency. This is easily explained by the time it takes to generate another packet to transmit. If the IR is enabled, the energy consumption decreases. The lowest values for the energy consumption matches the case when IR is enabled and presents a value for the sensing range $\Pi_{irmax} = -90$ dBm.

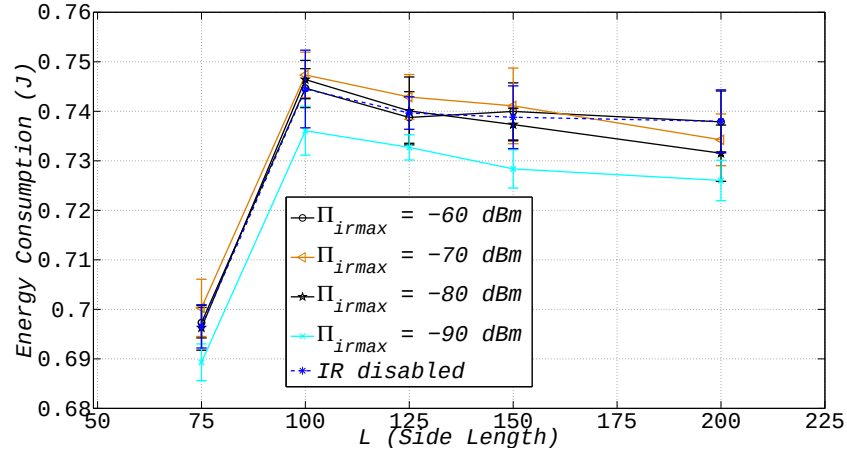


Figure J.20: Energy consumption per node of MC-SCP-MAC as a function of the deployment scenarios side lengths with exponential traffic generation ($\lambda = 1/10 \text{ s}^{-1}$) when IR enabled or disabled.

Figure J.20 shows the results for the energy spent by the MC-SCP-MAC as a function of the side lengths, whilst considering exponential traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$, as well as considering the enabling and disabling of the IR. In Figure J.20 it is observable that energy consumption achieves the maximum value for a side length of 100 m. Beyond 100 m, the energy consumption decreases as the side lengths becomes larger. The lowest values of energy consumption are verified when the IR is enabled and present a value for the sensing range value $\Pi_{irmax} = -90$ dBm.

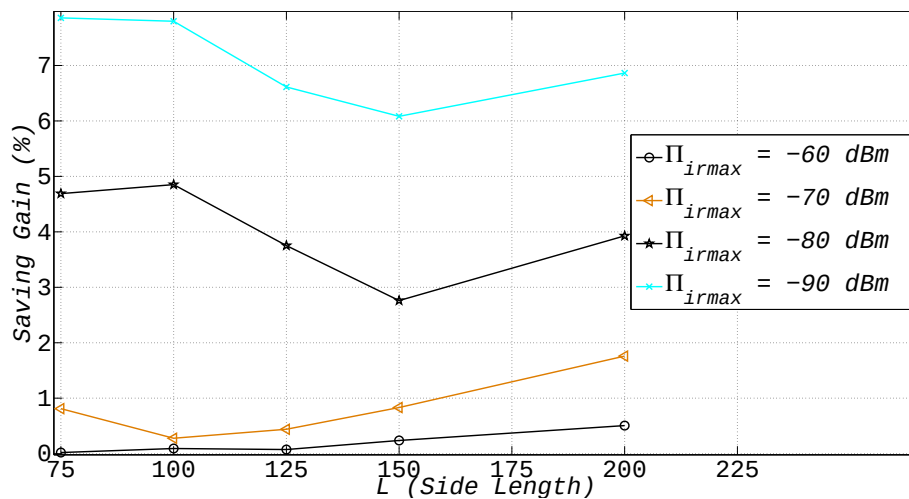


Figure J.21: Saving gain percentage per node of MC-SCP-MAC as a function of the deployment scenarios side lengths when IR is enabled with periodic traffic generation ($\lambda = 1/10 \text{ s}^{-1}$).

By comparing these results with the ones from Figure J.19 (with periodic traffic profile), the energy consumption in the case of exponential traffic profile generation presents

higher energy consumption. However, in the periodic traffic case, for side length larger than 100 m, the energy consumption tends to increase, whereas, in the exponential traffic profile it decreases for the same interval of the side lengths. The results presented in Figure J.21 evaluate the energy saving gains that can be achieved with the employment of the IR concept as a function of the side lengths whilst considering periodic traffic profile with a generation rate $\lambda = 1/10 \text{ s}^{-1}$. At first glance, the energy savings gains that can be achieved with this traffic generation interval are higher than the ones presented in Figure 8.53. It is noticeable that the use of IR is only efficient for denser scenarios and for sensing values $\Pi_{irmax} \in \{-90; -80; -70\} \text{ dBm}$.

References

- [AA07] Baris Atakan and Özgür B. Akan. On event signal reconstruction in wireless sensor networks. *Proc. of the 6th international IFIP-TC6 conference on Ad Hoc and sensor networks, wireless networks, next generation internet (Networking'07)*, pages 558-569, May 2007. 24
- [ADB⁺04] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita. A line in the sand: a wireless sensor network for target detection, classification, and tracking. *Computer Networks*, 46(5):605-634, 2004. Available from: <http://dx.doi.org/10.1016/j.comnet.2004.06.007>. 255
- [AGZAKMP10] Islam T. Almalkawi, Manel Guerrero Zapata, Jamal N. Al-Karaki, and Julian Morillo-Pozo. Wireless multimedia sensor networks: Current trends and future directions. *Sensors*, 10(7):6662-6717, 2010. Available from: <http://www.mdpi.com/1424-8220/10/7/6662>. 25
- [AHS06] Karl Aberer, Manfred Hauswirth, and Ali Salehi. A middleware for fast and flexible sensor network deployment. In *Proc. of the 32nd Very Large Data Bases Conference (Demo Session)*, pages 1199-1202, Seoul; Korea, September 2006. 50
- [AMC07] Ian F. Akyildiz, Tommaso Melodia, and Kaushik R. Chowdhury. A Survey on Wireless Multimedia Sensor Networks. *Computer Networks*, 51:921-960, 2007. 25
- [AMC08] Ian F. Akyildiz, Tommaso Melodia, and Kaushik Chowdhury. Wireless Multimedia Sensor Networks: Applications and Testbeds. *Proc. of the IEEE*, 96(10):1588-1605, 2008. 25
- [Aqu] Aqua wireless sensor networks project. Available from: <http://www.tslab.ssvl.kth.se/csd/projects/0726/>. 33, 333
- [AR05] Josephine Ammer and Jan Rabaey. Low power synchronization for wireless sensor network modems. In *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 2005)*, pages 670-675, New Orleans, LA, USA, March 2005. 20
- [Ash92] D. L. Ash. A comparison between OOK/ASK and FSK modulation techniques for radio links. *Technical report*, 1992. Available from: <http://www.rfm.com/products/apnotes/ookvsfsk.pdf>. 190
- [ASSC02] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. *Computer Networks*, 38:393-422, 2002. 92
- [ASSdGC06] T. Antoine-Santoni, J.F. Santucci, E. de Gentili, and B. Costa. Using Wireless Sensor Network for Wildfire detection. A discrete event approach of

- environmental monitoring tool. In *Proc. of the 1st International Symposium on Environment Identities and Mediterranean Area (ISEIMA '06)*, pages 115-120, Corte-Ajaccio, France, July 2006. 33, 43, 47, 334
- [ASSDGC08] T. Antoine-Santoni, J.F. Santucci, E. De Gentili, and B. Costa. Wild-fire impact on deterministic deployment of a wireless sensor network by a discrete event simulation. In *Proc. of the 14th IEEE Mediterranean Electrotechnical Conference (MELECON 2008)*, pages 204-209, Ajaccio, France, May 2008. 33, 43, 47, 334
- [Ast] The astra project. Available from: <http://research.cs.ncl.ac.uk/astra/>. 33, 43, 47, 336
- [AT809] *AT86RF231 Datasheet*, 2009. Datasheet. Available from: http://www.atmel.com/dyn/resources/prod_documents/doc8111.pdf. 181
- [ATT⁺08] Takahiro Aoyagi, Junichi Takada, Kenichi Takizawa, Norihiko Katayama, Takehiko Kobayashi, Kamyaz Yazdandoost, Huan bang Li, and Ryuji Kohno. Channel model for wearable and implantable WBANs (IEEE 802.15-08-0416-04-0006). Technical report, 2008. 373
- [AU04] M. Ali and Z.A. Uzmi. An energy-efficient node address naming scheme for wireless sensor networks. In *Proc. of the International Networking and Communication Conference (INCC 2004)*, pages 25-30, Lahore, Pakistan, June 2004. 23
- [Ayl06] Ryan Aylward. Senseable: A wireless, compact, multi-user sensor system for interactive dance. In *Proc. of the International Conference on New Interfaces for Musical Expression (NIME 06)*, pages 134-139, Paris, France, June 2006. 34
- [AZM10] J. Ansari, X. Zhang, and P. Mahonen. Multi-radio medium access control protocol for wireless sensor networks. *International Journal of Sensor Networks*, 8(1):47-61, July 2010. Available from: <http://dx.doi.org/10.1504/IJSNET.2010.034066>. 200
- [BAL⁺08] Luís M. Borges, Pedro Araújo, António S. Lebres, Andreia Rente, Rita Salvador, Fernando J. Velez, J. Martinez de Oliveira, Norberto Barroca, and João M. Ferro. Overview of Progress in Smart-Clothing Project for Health Monitoring and Sport Applications. In *Proc. of the first International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2008)*, Aalborg, Denmark, October 2008. 6, 56, 57
- [BAL⁺10] Luís M. Borges, Pedro Araújo, António S. Lebres, Andreia Rente, Rita Salvador, Fernando J. Velez, J. Martinez de Oliveira, Norberto Barroca, and João M. Ferro. Wearable Sensors for Foetal Movement Monitoring in Low Risk Pregnancies. In Aimé Lay-Ekuakille and Subhas Chandra Mukhopadhyay, editors, *Wearable and Autonomous Biomedical Devices and Systems for Smart Environment: Issues and Characterization*, volume 75 of ISBN: 978-3642156861, pages 115-136. Springer, Norwell, MA, USA, 2010. 6

- [BBV⁺11] Norberto Barroca, Luís M. Borges, Fernando J. Velez, Filipe Monteiro, Marcin Górski, and João Castro-Gomes. Wireless Sensor Networks applied to Engineering Structures. Technical Report TR-1-2011, Universidade da Beira Interior, Covilhã, Portugal, November 2011. 7
- [BBV⁺12] Norberto Barroca, Luís M. Borges, Fernando J. Velez, Marcin Górski, and João Castro-Gomes. Wireless Sensor Networks for Temperature and Humidity Monitoring within Concrete Structures. *submitted to Construction & Building Materials (considered for publication with major revisions)*, October 2012. 7
- [BBVL08] Luís M. Borges, Norberto Barroca, Fernando J. Velez, and António S. Lebres. Flex Sensor Belt. Technical Report TR-3-2008, Universidade da Beira Interior, Covilhã, Portugal, March 2008. 6
- [BBVL09] Luís M. Borges, Norberto Barroca, Fernando J. Velez, and António S. Lebres. Smart-Clothing Wireless Flex Sensor Belt Network for Foetal Health Monitoring. In *Proc. of WiPH 2009 - International Workshop on Wireless Pervasive Healthcare (held in conjunction with 3rd International Conference on Pervasive Computing Technologies for Healthcare 2009)*, London, UK, March 2009. 6
- [BCL07a] Luís M. Borges, Filipe Carvalho, and António S. Lebres. Industry Process Management With Wireless Sensors. In *Proc. of 10th Portuguese-Spanish Conference in Electrical Engineering*, Madeira, Portugal, July 2007. 6
- [BCL07b] Luís M. Borges, Filipe Carvalho, and António S. Lebres. InterNodal Network - An Autoconfigurable Wireless Network. In *Proc. of Conftele2007 - 6th Conference of Telecommunications*, Peniche, Portugal, May 2007. 6, 8
- [BCL07c] Luís M. Borges, Filipe Carvalho, and António S. Lebres. Measuring with Wireless Networks. In *Proc. of the 6th International Conference on Measurement (MEASUREMENT)*, Smolenice Castle, Slovakia, May 2007. 6
- [BCP08] S. Basagni, A. Carosi, and C. Petrioli. Mobility in wireless sensor networks. In A. Boukerche, editor, *Algorithms and Protocols for Ad Hoc and Sensor Networks*, pages 267-305. John Wiley & Sons, Inc., New York, NY, 2008. Available from: <http://dx.doi.org/10.1002/9780470396360.ch10>. 12
- [BCVL07] Luís M. Borges, Filipe Carvalho, Fernando J. Velez, and António S. Lebres. Rede Internodal Implementação e Aplicação Prática de Redes de Sensores sem Fios. In *Actas da Engenharia'2007 - Inovação e Desenvolvimento*, Covilhã, Portugal, November 2007. 6, 86
- [BDO⁺05] Stephen J. Bellis, Kieran Delaney, Brendan O'Flynn, John Barton, Kafil M. Razeeb, and Cian O'Mathuna. Development of field programmable modular wireless sensor network nodes for ambient systems. *Computer Communications*, 28(13):1531-1544, 2005. Available from: <http://portal.acm.org/citation.cfm?id=1646641.1646681>. 33, 333
- [BDWL10] Abdelmalik Bachir, Mischa Dohler, Thomas Watteyne, and Kin Leung. MAC Essentials for Wireless Sensor Networks. *IEEE Communications Surveys &*

Tutorials, 12(2):222-248, 2010. Available from: <http://dx.doi.org/10.1109/SURV.2010.020510.00058>. 2, 11, 111, 129

- [BEH⁺06] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In *Proc. of the Workshop on World-Sensor-Web (WSW'06): Mobile Device Centric Sensor Networks and Applications*, pages 117-134, Boulder, CO, USA, October 2006. 51
- [BEOiRTUE07] J. Bień, L. Elfgren, J. Olofsson, and 6 Program Ramowy Badań i Rozwoju Technicznego Unii Europejskiej. *Sustainable bridges: assessment for future traffic demands and longer lives*. Dolnośląskie Wydawn. Edukacyjne, 2007. 33, 43, 47, 332
- [BGdMT06] Gunter Bolch, Stefan Greiner, Hermann de Meer, and Kishor S. Trivedi. *Queueing Networks and Markov Chains: Modeling and Performance Evaluation with Computer Science Applications*. Wiley-Interscience, 2nd edition, April 2006. 159
- [BGLA01] Lichun Bao and J. J. Garcia-Luna-Aceves. A new approach to channel access scheduling for ad hoc networks. In *Proc. of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom' 01)*, pages 210-221, July 2001. Available from: <http://doi.acm.org/10.1145/381677.381698>. 393
- [BLA⁺09] Luís M. Borges, António S. Lebres, Pedro Araújo, Fernando J. Velez, Andreia Rente, Rita Salvado, J. Martinez de Oliveira, Norberto Barroca, and João M. Ferro. Smart-Clothing, Innovation on Mobile Healthcare. In *Actas da Engenharia'2009 - Inovação e Desenvolvimento*, Covilhã, Portugal, November 2009. 6
- [BMFD06] M.I. Brownfield, K. Mehrjoo, A.S. Fayez, and IV Davis, N.J. Wireless sensor network energy-adaptive mac protocol. In *Proc. of the 3rd IEEE Consumer Communications and Networking Conference (CCNC 2006)*, volume 2, pages 778-782, January 2006. 398
- [BMS⁺08] G. Bhatti, A. Mehta, Z. Sahinoglu, J. Zhang, and R. Viswanathan. Modified Beacon-Enabled IEEE 802.15.4 MAC for Lower Latency. In *Proc. of the IEEE Global Telecommunications Conference (GLOBECOM 2008)*, pages 1-5, November 2008. Available from: <http://dx.doi.org/10.1109/GLOCOM.2008.ECP.173>. 249
- [Bor08a] Luís M. Borges. Accelerometer ADXL330. Technical Report TR-2-2008, Universidade da Beira Interior, Covilhã, Portugal, January 2008. 6
- [Bor08b] Luís M. Borges. On-Off Belt. Technical Report TR-5-2008, Universidade da Beira Interior, Covilhã, Portugal, April 2008. 6
- [Bor08c] Luís M. Borges. Smart-Clothing SoftPot Belt. Technical Report TR-6-2008, Universidade da Beira Interior, Covilhã, Portugal, March 2008. 6
- [Bor08d] Luís M. Borges. Study and test of the μ DRIVE-uSD-G1 module. Technical Report TR-4-2008, Universidade da Beira Interior, Covilhã, Portugal, April 2008. 6

- [Bue08] N.R. Buenfeld. *Intelligent Monitoring of Concrete Structures*. CIRIA Series. CIRIA, 2008. 68
- [Bue11] N. R. Buenfeld. Editorial: Automated monitoring of concrete structures - research opportunities. *Magazine of Concrete Research*, 63(2):79-80, February 2011. 359
- [BVF⁺09] Norberto Barroca, Fernando J. Velez, João M. Ferro, Luís M. Borges, and António S. Lebres. Desenho de Protocolos de Controlo de Acesso ao Meio Eficientes do Ponto de Vista Energético em Redes de Sensores Sem Fios. In *Actas da Engenharia'2009 - Inovação e Desenvolvimento*, Covilhã, Portugal, November 2009. 56, 60
- [BVF⁺10] Norberto Barroca, Fernando J. Velez, João M. Ferro, Luís M. Borges, and António S. Lebres. Energy-Aware Wireless Sensor Networks MAC Modelling and Simulation with Efficient Transceivers. In *Proc. of the 13th International Symposium on Wireless Personal Multimedia Communications (WPMC'10) (invited paper for the Special Session on "Internet of Things")*, Recife, Pernambuco, Brasil, October 2010. 7
- [BVFB10] Norberto Barroca, Fernando J. Velez, João M. Ferro, and Luís M. Borges. Energy-Aware Sensor MAC Modelling and Simulation for WBAN Applications with Efficient Transceivers. In *the 10th Meeting of the Management Committee of COST 2100 - Pervasive Mobile Ambient Wireless Communications*, TD(10)039, Athens, Greece, February 2010. 7
- [BVL08a] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Taxonomies for the Classification and the Characterisation of Wireless Sensor Networks Services and Applications. In *the 5th Meeting of the Management Committee of COST 2100- Pervasive Mobile Ambient Wireless Communications*, TD(08)532, Trondheim, Norway, June 2008. 6, 7
- [BVL08b] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Wireless Sensor and Actuator Networks Services and Applications: Characterisation and Classification Taxonomies. In *Proc. of the 11th International Symposium on Wireless Personal Multimedia Communications (WPMC'08)*, Lapland, Finland, September 2008. 6
- [BVL09] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Taxonomy for Wireless Sensor Networks Services Characterisation and Classification. In *Proc. of Conftele2009 - 7th Conference of Telecommunications*, Vila da Feira, Portugal, May 2009. 6
- [BVL10] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Lessons Learned from Implementing the Energy-Aware Schedule Channel Polling MAC Protocol in the Mobility Framework Simulator. In *the 12th Meeting of the Management Committee of COST 2100 - Pervasive Mobile Ambient Wireless Communications*, TD(10)12063, Bologna, Italy, November 2010. 7
- [BVL11] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Performance Evaluation of the Schedule Channel Polling MAC Protocol Applied to Health

Monitoring in the Context of IEEE 802.15.4. In *Proc. of the 17th European Wireless Conference 2011 (EW'2011) (invited paper)*, Vienna, Austria, April 2011. 7

- [BVL12] Luís M. Borges, Fernando J. Velez, and António S. Lebres. Taxonomy for the Characterization and Classification of Wireless Sensor Networks Applications. *submitted to IEEE Communications Surveys & Tutorials*, June 2012. 6
- [BVLW12] Luís M. Borges, Fernando J. Velez, António S. Lebres, and Thomas Watteyne. Performance Modelling of the Collision Probability in a Two-Phase Contention Scheme for Scheduled Channel Polling. *submitted to Computer Networks*, July 2012. 7
- [BYAH06] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard Han. X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks. In *Proc. of the 4th International Conference on Embedded Networked Sensor Systems (SenSys '06)*, pages 307-320, New York, NY, USA, 2006. ACM. Available from: <http://doi.acm.org/10.1145/1182807.1182838>. 116
- [Cap10] *Datasheet Filter Cap SF2 for Humidity and Temperature Sensor SHT2x*, 2010. Datasheet. Available from: http://www.sensirion.com/en/pdf/product_information/Datasheet_filter-cap_sf2.pdf. 77
- [CBCO12] C. Cano, B. Bellalta, A. Cisneros, and M. Oliver. Quantitative analysis of the hidden terminal problem in preamble sampling wsns. *Ad Hoc Networks*, 10(1):19 - 36, 2012. Available from: <http://www.sciencedirect.com/science/article/pii/S1570870511000862>. 278
- [CC107] *CC1100 Datasheet*, 2007. Datasheet. Available from: <http://www.ti.com/lit/ds/symlink/cc1100.pdf>. 138, 181
- [CC207] Chipcon CC2420 Datasheet: <http://focus.ti.com/lit/ds/symlink/cc2420.pdf>, Texas Instruments, 2007. 138, 181, 192, 219
- [CCH12] Thang Vu Chien, Hung Nguyen Chan, and Thanh Nguyen Huu. A comparative study on hardware platforms for wireless sensor networks. *International Journal on Advanced Science, Engineering and Information Technology*, 2(1):70-74, 2012. Available from: http://ijaseit.insightsociety.org/index.php?option=com_content&view=article&id=9&Itemid=1&article_id=157. 25
- [CDLNL06] Paulo J. S. Cruz, Abraham Diaz De Leon, Joao P. Nunes, and Christopher K. Y. Leung. Design and mechanical characterization of fibre optic plate sensor for crack monitoring. *Sensors and Materials*, 18(6):283-299, 2006. 359
- [CH12] Chih-Yuan Chang and San-Shan Hung. Implementing RFIC and sensor technology to measure temperature and humidity inside concrete structures. *Construction and Building Materials*, 26(1):628-637, January 2012. 78, 359

- [CIS] The Internet of Things: INFOGRAPHIC. Available from: <http://blogs.cisco.com/news/the-internet-of-things-infographic/>. 51
- [CL54] H. Chernoff and E.L. Lehmann. The Use of Maximum Likelihood Estimates in χ^2 Tests for Goodness of Fit. *Annals of Mathematical Statistics*, 25(3):579-586, 1954. 172
- [CL99] C.C. Chow and V.C.M. Leung. Performance of IEEE 802.11 medium access control protocol over a wireless local area network with distributed radio bridges. In *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 1999)*, pages 535-539, September 1999. 190
- [CLWY07] Z. Chen, C. Lin, H. Wen, and H. Yin. An Analytical Model for Evaluating IEEE 802.15.4 CSMA/CA Protocol in Low-Rate Wireless Application. *Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, pages 899-904, May 2007. Available from: <http://www.computer.org/portal/web/csdl/doi/10.1109/AINAW.2007.77>. 190
- [CLZ06] Elaine Cheong, Edward A. Lee, and Yang Zhao. Joint Modeling and Design of Wireless Networks and Sensor Node Software. Technical Report UCB/EECS-2006-150, EECS Department, University of California, Berkeley, November 2006. Available from: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2006/EECS-2006-150.html>. 325
- [CMGL05] Shuguang Cui, Ritesh Madan, Andrea J. Goldsmith, and Sanjay Lall. Joint routing, mac, and link layer optimization in sensor networks with energy constraints. In *Proc. of the IEEE International Conference on Communications (ICC 2005)*, pages 725-729, Seoul, Korea, May 2005. 18
- [CMR06] H. Chang, V. Misra, and D. Rubenstein. A general model and analysis of physical layer capture in 802.11 networks. In *Proc. of Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Infocom)*, Barcelona, Spain, April 2006. 190, 192
- [CMYP09] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Sensor network security a survey. *IEEE Communications Surveys & Tutorials*, 11(2):52-73, 2009. 12
- [COS06] COST 2100. EU COST Action 2100: Pervasive Mobile Ambient Wireless Communications [online]. 2006. Available from: <http://www.cost2100.org/> [cited 18 July 2012]. 6
- [COS10] COST IC0905 TERRA. EU COST Action IC0905 TERRA: Techno-Economic Regulatory Framework for Radio Spectrum Access for Cognitive Radio/Software Defined Radio [online]. 2010. Available from: <http://www.cost-terra.org/> [cited 18 July 2012]. 6, 7
- [COS11] COST IC1004. EU COST Action IC1004: Cooperative Radio Communications for Green Smart Environments [online]. 2011. Available from: <http://www.ic1004.org/> [cited 18 July 2012]. 6

- [CRU06] Report on WSN applications, their requirements, application-specific WSN issues and evaluation metrics. Technical Report Deliverable D112.1, IST NoE CRUISE, 2006. Available from: <http://www.ist-CRUISE.eu>. 32
- [CSNH⁺12] Raúl Chávez-Santiago, Keith E. Nolan, Oliver Holland, Norberto Barroca, João M. Ferro, Luís M. Borges, Fernando J. Velez, Vânia Gonçalves, and Ilangko Balasingham. Cognitive Radio for Medical Body Area Networks Using Ultra Wide-band. *IEEE Wireless Communications Magazine, Topic: Cognitive Radio Networks: A Pratical Perspective*, 19(4):74-81, August 2012. 7
- [CV04] D. Chen and P. K. Varshney. QoS Support in Wireless Sensor Networks: A Survey. In *Proc. of the 2004 International Conference on Wireless Networks (ICWN 2004)*, Las Vegas, Nevada, USA, June 2004. xxxi, 17, 18
- [CV07] Sing-Yiu Cheung and Pravin Varaiya. Traffic surveillance by wireless sensor networks: Final report. Technical Report ISSN 1055-1425, University of California, Berkeley, 2007. 33, 42, 46, 331
- [CWGD10] Feng Chen, Nan Wang, Reinhard German, and Falko Dressler. Simulation study of IEEE 802.15.4 LR-WPAN for industrial applications. *Wireless Communications and Mobile Computing*, 10(5):609-621, May 2010. Available from: <http://dx.doi.org/10.1002/wcm.v10:5>. 18
- [dB11] Lina Maria Pestana Leão de Brito. *A Hierarchical and Generic Model for Context-Awareness in Collaborative Wireless Sensor Networks*. PhD thesis, Universidade da Madeira, Funchal, Portugal, 2011. 25
- [dBRP08] Lina de Brito and Laura Rodriguez Peralta. A collaborative model for wireless sensor networks applied to museums' environmental monitoring. In Yuhua Luo, editor, *Cooperative Design, Visualization, and Engineering*, volume 5220 of *Lecture Notes in Computer Science*, pages 107-116. Springer Berlin / Heidelberg, 2008. 25
- [DF09] Gustavo S. Duffó and Silvia B. Farina. Development of an embeddable sensor to monitor the corrosion process of new and existing reinforced concrete structures. *Construction and Building Materials*, 23(8):2746 - 2751, 2009. Available from: <http://www.sciencedirect.com/science/article/pii/S0950061809001123>. 359
- [DFEV05] Henri Dubois-Ferrière, Deborah Estrin, and Martin Vetterli. Packet combining in sensor networks. In *Proc. of the 3rd international conference on Embedded networked sensor systems (SenSys'05)*, pages 102-115, San Diego, California, USA, 2005. Available from: <http://doi.acm.org/10.1145/1098918.1098930>. 190
- [DHJ⁺06] Prabal Dutta, Jonathan Hui, Jaein Jeong, Sukun Kim, Cory Sharp, Jay Taneja, Gilman Tolle, Kamin Whitehouse, and David Culler. Trio: Enabling sustainable and scalable outdoor wireless sensor network deployments. In *Proc. of the The Fifth ACM/IEE International Conference on Information Processing in Sensor Networks (ACM/IEEE IPSN/SPOTS 2006)*, pages 407-415, Nashville, Tennessee, USA, April 2006. 33, 335

- [DHNH03] S. Dulman, L. Hoesel, T. Nieberg, and P. Havinga. Collaborative communication protocols for wireless sensor networks. In *Proc. of the European Research on Middleware and Architectures for Complex and Embedded Systems Workshop*, Pisa, Italy, April 2003. 392
- [DL03] T. van Dam and K. Langendoen. An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proc. of the Third ACM International Conference on Embedded Networked Sensor Systems (SenSys'03)*, pages 171-180, Los Angeles, CA, USA, November 2003. Available from: <http://www.st.ewi.tudelft.nl/~koen/papers/sensys03.pdf>. 116
- [dLGLM⁺07] Delia Rodríguez de Llera González, Xin Liu, Abdullah Mansoor, Hanyi Wang, Shuo Li, Yue Ruan, and Tingting Ai. Project report for the hardware circuit design of the aquawsn: Final report. Technical report, School of Information and Communication Technology, 2007. 33, 333
- [dOdON08] S. de Oliveira, T.R. de Oliveira, and J.M. Nogueira. A security management framework for sensor networks. In *Proc. of the IEEE Network Operations and Management Symposium (NOMS 2008)*, pages 935-938, Salvador, Bahia, Brazil, April 2008. 22
- [DRS⁺05] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G.S. Sukhatme. Robomote: enabling mobility in sensor networks. In *Proc. of the 4th International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 404-409, Los Angeles, California, USA, April 2005. 33, 331
- [e-S] Capturing of ambient intelligence for beyond 3g mobile communication systems through wireless sensor networks:e-sense. Available from: <http://www.ist-e-sense.org/>. 34, 340
- [EGHK99] Deborah Estrin, Ramesh Govindan, John Heidemann, and Satish Kumar. Next century challenges: scalable coordination in sensor networks. In *Proc. of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*, pages 263-270, Seattle, Washington, USA, August 1999. Available from: <http://dx.doi.org/10.1145/313451.313556>. 22
- [EH02] A. El-Hoiydi. Aloha with Preamble Sampling for Sporadic Traffic in Ad Hoc Wireless Sensor Networks. In *Proc. of IEEE International Conference on Communications (ICC 2002)*, volume 5, pages 3418-3423, New York, USA, 2002. 116, 119
- [EHD04] A. El-Hoiydi and J.-D. Decotignie. Wisemac: an ultra low power mac protocol for the downlink of infrastructure wireless sensor networks. In *Proc. of the Ninth International Symposium on Computers and Communications (ISCC 2004)*, pages 244-251, Alexandria, Egypt, June 2004. 116, 238, 244, 395
- [EHK⁺07] L. Evers, P.J.M. Havinga, J. Kuper, M.E.M. Lijding, and N. Meratnia. SensorScheme: Supply chain management automation using wireless sensor networks. In *Proc. of the IEEE Conference on Emerging Technologies and*

Factory Automation (ETFA 2007), pages 448-455, Patras, Greece, September 2007. 33, 335

- [EKP⁺06] Cz. Evaggelos, E. Karvounis, C. Papaloukas, M. Tsipouras, P. Bougia, I. Dimitrios, and K. Naka. Remote Maternal and Fetal Health Monitoring during Pregnancy. In *Proc. the International Special Topic Conference on Information Technology Applications in Biomedicine (ITAB2006)*, Ioannina, Greece, October 2006. 55, 56
- [ERA12] *ERA400TRS transceiver Datasheet*, 2012. Datasheet. Available from: <http://www.lprs.co.uk/assets/files/erA3v6DS.pdf>. 84
- [ERI] Vision 2020-50 billion connected devices. Available from: http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c. 51, 53
- [ESVS⁺09] S.C. Ergen, A. Sangiovanni-Vincentelli, Xuening Sun, R. Tebano, S. Alalusi, G. Audisio, and M. Sabatini. The tire as an intelligent sensor. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 28(7):941-955, 2009. 33, 43, 47, 336
- [EV06] S.C. Ergen and P. Varaiya. PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks. *IEEE Transactions on Mobile Computing*, 5(7):920-930, July 2006. 395
- [Far08] Shahin Farahani. *ZigBee Wireless Networks and Transceivers*. Newnes, Newton, MA, USA, 2008. xxix, 95, 97, 98, 99, 103, 106, 107, 108, 110, 367, 383, 386, 387, 388
- [FBB08] João M. Ferro, Luís M. Borges, and Norberto Barroca. Simulation Tools. Technical Report TR-1-2008, Universidade da Beira Interior, Covilhã, Portugal, October 2008. 7
- [FBVL07a] João M. Ferro, Luís M. Borges, Fernando J. Velez, and António S. Lebres. Applications of Wireless Sensor Networks. In *Proc. of The 2007 International Conference of Wireless Networks (held in the context of WCE'2007 - World Congress on Engineering) (ICWN'2007)*, London, UK, July 2007. 6
- [FBVL07b] João M. Ferro, Luís M. Borges, Fernando J. Velez, and António S. Lebres. Applications of Wireless Sensor Networks. In *the 3rd Meeting of the Management Committee of COST 2100 - Pervasive Mobile Ambient Wireless Communications*, TD-327, Duisburg, Germany, September 2007. 7
- [FBVL09] João M. Ferro, Luís M. Borges, Fernando J. Velez, and António S. Lebres. Uma Visão das Futuras Aplicações de Redes de Sensores Sem Fios. In *Actas da Engenharia'2007 - Inovação e Desenvolvimento*, Covilhã, Portugal, September 2009. 6
- [FDC⁺09] M. Friedrich, G. Dobie, Chung Chee Chan, S.G. Pierce, W. Galbraith, S. Marshall, and G. Hayward. Miniature Mobile Sensor Platforms for Condition Monitoring of Structures. *IEEE Sensors Journal*, 9(11):1439-1448, November 2009. 69

- [Fel68] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. Wiley, January 1968. Available from: <http://www.amazon.ca/exec/obidos/redirect?tag=citeulike04-20{&}path=ASIN/0471257087>. 162, 164
- [FFR09] E. Farella, M. Falavigna, and B. Ricco. Aware and smart environments: The Casattenta project. In *Proc. of the 3rd International Workshop on Advances in Sensors and Interfaces (IWASI 2009)*, pages 2-6, Bari, Italy, June 2009. 34, 337
- [FLQ07] Weiwei Fang, Yi Liu, and Depei Qian. EDDS: An efficient data delivery scheme for address-free wireless sensor networks. In *Proc. of the International Conference on Networking (ICN'07)*, Sainte-Luce, Martinique, France, April 2007. IEEE Computer Society. 23
- [FV05] Jaime Ferreira and Fernando J. Velez. Enhanced umts services and applications characterisation. *Teletronikk Strategies in Telecommunications*, 101(1):113-131, March 2005. 14
- [FXHZ10] B. Firner, C. Xu, R. Howard, and Y. Zhang. Multiple receiver strategies for minimizing packet loss in dense sensor networks. In *Proc. of the eleventh ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'10)*, pages 211-220, Chicago, Illinois, USA, September 2010. Available from: <http://doi.acm.org/10.1145/1860093.1860122>. xxiii, xxxii, 4, 29, 189, 190, 192, 193, 194, 195, 196, 197, 199, 200, 217
- [GBH⁺03] Frank Glatowski, Jan Blumenthal, Matthias H, Marc Haase, Hagen Burchardt, and Dirk Timmermann. Service oriented software architecture for sensor networks. In *Proc. of the International Workshop on Mobile Computing (IMC03)*, pages 93-98, Rockstock, Germany, June 2003. 18
- [GBM⁺08] A. Gluhak, M. Bauer, F. Montagut, V. Stirbu, M. Johansson, J. B. Vercher, and M. Presser. Towards an architecture for a real world internet. In *Proc. of the Autonomous and Spontaneous Networks Symposium*, pages 117-134, Paris, France, November 2008. 50
- [GBV10] C. Gezer, C. Buratti, and R. Verdone. Capture effect in iee 802.15.4 networks: modelling and experimentation. In *Proc. of the 5th IEEE international conference on Wireless pervasive computing (ISWPC'10)*, pages 204-209, Mondena, Italy, May 2010. Available from: <http://dl.acm.org/citation.cfm?id=1856330.1856366>. 190, 192, 193, 200, 211
- [GCB03] J. A. Gutiérrez, E. H. Callaway, and R. L. Barrett. *Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4*. IEEE Standards. Standards Information Network - IEEE Press, United States of America, 1 edition, 2003. xxix, 98, 110, 375, 387, 388
- [GEWD05] D. Gracanin, M. Eltoweissy, A. Wadaa, and L. A. Dasilva. A service-centric model for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(6):1159-1166, 2005. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1435510. 13, 93

- [GGSK11] I. Guvenc, S. Gezici, Z. Sahinoglu, and U. C. Kozat. *Reliable Communications for Short-Range Wireless Systems*. Cambridge University Press, United Kingdom, 2011. 212
- [GHIGGHPD07] Carlos F García-Hernández, Pablo H Ibargüengoytia-González, Joaquín García-Hernández, and Jesús A Pérez-Díaz. Wireless sensor networks and applications : a survey. *Journal of Computer Science*, 7(3):264-273, 2007. 13, 16
- [GJ05] C. Gribbin and D. James. Assessing fetal health. *Current Obstetrics & Gynaecology*, 15(4):221-227, 2005. 56
- [GM05] C. Gui and Prasant Mohapatra. Virtual patrol: a new power conservation design for surveillance using sensor networks. In *Proc. of the 4th International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, pages 246-253, Los Angeles, California, USA, April 2005. 33, 332
- [Gol05] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005. 20
- [GPS⁺06] Alexander Gluhak, Mirko Presser, Zach Shelby, Paolo Scotton, Wolfgang Schott, and Pierre Chevillat. e-sense reference model for sensor networks in b3g mobile communication systems. In *Proc. of the 15th IST Summit 2006 Workshop*, Myconos Greece, June 2006. 30
- [GSB⁺09] J. Goldman, K. Shilton, J. Burke, D. Estrin, M. Hansen, N. Ramanathan, S. Reddy, V. Samanta, M. Srivastava, and R. West. Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world. *Foresight & Governance Project, White Paper*, 2009. 51, 52
- [HDB04] B. Hohlt, L. Doherty, and E. Brewer. Flexible power scheduling for sensor networks. In *Proc. of the 3rd international symposium on Information processing in sensor networks (IPSN '04)*, pages 205-214, Berkeley, California, USA, 2004. Available from: <http://doi.acm.org/10.1145/984622.984653>. 199
- [HHT02] M.J. Handy, M. Haase, and D. Timmermann. Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection. In *Proc. of the 4th International Workshop on Mobile and Wireless Communications Network*, pages 368-372, Stockholm, Sweden, September 2002. 116, 394
- [HJB03] Bret Hull, Kyle Jamieson, and Hari Balakrishnan. Bandwidth management in wireless sensor networks. In *Proc. of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'03)*, pages 306-307, Los Angeles, CA, USA, November 2003. 18
- [HK03] Fei Hu and Sunil Kumar. Qos considerations in wireless sensor networks for telemedicine. In *Proc. of the SPIE ITCOM Conference*, Orlando, Florida, USA, September 2003. 31

- [HKL⁺06] Tian He, Sudha Krishnamurthy, Liqian Luo, Ting Yan, Lin Gu, Radu Stoleru, Gang Zhou, Qing Cao, Pascal Vicaire, John A. Stankovic, Tarek F. Abdelzaher, Jonathan Hui, and Bruce Krogh. VigilNet: An integrated sensor network system for energy-efficient surveillance. *ACM Transactions on Networking*, 2(1):1-38, 2006. Available from: <http://doi.acm.org/10.1145/1138127.1138128>. 33, 43, 47, 335
- [HKWW06] Vlado Handziski, Andreas Köpke, Andreas Willig, and Adam Wolisz. TWIST: a scalable and reconfigurable testbed for wireless indoor experiments with sensor networks. In *Proc. of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality (REALMAN '06)*, pages 63-70, Florence, Italy, May 2006. Available from: <http://doi.acm.org/10.1145/1132983.1132995>. 33, 331
- [HL07] Gertjan P. Halkes and Koen Langendoen. Crankshaft: An Energy-Efficient MAC-Protocol for Dense Wireless Sensor Networks. In *Proc. of the fourth European Wireless Sensor Network (EWSN07)*, pages 228-244, Delft, The Netherlands, January 2007. 121, 130
- [HLBW08] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei. Survey of hardware systems for wireless sensor networks. *Journal of Low Power Electronics*, 4(1):11-20, 2008. 24, 25
- [HNS⁺06] S. Han, Y. Nam, Y. Seok, T. Kwon, and Y. Choi. Two-phase Collision Avoidance to Improve Scalability in Wireless LANs. In *Proc. of the 49th Annual IEEE Global Telecommunications Conference (GLOBECOM'2006)*, San Francisco, California, USA, November 2006. 130, 233
- [Hog] The hogthrob project. Available from: <http://www.hogthrob.dk>. 33, 336
- [HSI⁺01] John Heidemann, Fabio Silva, Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, and Deepak Ganesan. Building efficient wireless sensor networks with low-level naming. In *Proc. of the 18th ACM Symposium on Operating Systems Principles (SOSP '01)*, pages 146-159, Banff, Alberta, Canada, 2001. Available from: <http://doi.acm.org/10.1145/502034.502049>. 82
- [HSSWM07] Hoi-Sheung, W. So, J. Walrand, and Jeonghoon Mo. McMAC: A Parallel Rendezvous Multi-Channel MAC Protocol. In *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 2007)*, pages 334-339, Hong Kong, China, March 2007. 243
- [HvDL05] Gertjan P. Halkes, Tijs van Dam, and Koen Langendoen. Comparing energy-saving mac protocols for wireless sensor networks. *Mobile Networks and Applications (MONET)*, 10(5):783-791, 2005. 130
- [HvS02] Z. Hadzi-velkov and B. Spasenovski. Capture effect in IEEE 802.11 basic service area under influence of Rayleigh fading and near/far effect. In *Proc. of 13th IEEE Personal, Indoor and Mobile Radio Communications*, pages 172-176, London, United Kingdom, September 2002. 190

- [HXS⁺12] P. Huang, L. Xiao, S. Soltani, M. Mutka, and N. Xi. The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey. *IEEE Communications Surveys Tutorials*, 14(4):1-20, 2012. 11
- [Hyg12] *Datasheet Hygroclip*, 2012. Datasheet. Available from: <http://http://www.rotronic-usa.com/ds/Hygroclip.pdf>. 75
- [IEE02] IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). *IEEE Std 802.15.1-2002*, pages 1-473, 14 2002. 95
- [IEE03a] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs). *IEEE Std 802.15.3-2003*, pages 0-315, 2003. 95
- [IEE03b] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). *IEEE Std 802.15.4-2003*, pages 0-670, 2003. 96
- [IEE03c] IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *ANSI/IEEE Std 802.11, 1999 Edition (R2003)*, pages i-513, 2003. 95
- [IEE04] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. *IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001)*, pages 1-857, 2004. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1350465. 95
- [IEE06] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). Technical report, 2006. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1700009. 207, 369, 372
- [IEE07] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Net-

- works - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, pages 1-203, 2007. 96, 108, 110, 116, 235
- [IEE10] IEEE Std 802.15.6 draft, 15-10-0245-06-0006-tg6-draft. Technical report, 2010. 372
- [IKKV08] P. Iso-Ketola, T. Karinsalo, and J. Vanhala. HipGuard: A wearable measurement system for patients recovering from a hip operation. In *Proc. of the 2nd International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth 2008)*, pages 196-199, Tampere, Finland, February 2008. 34, 339
- [IM04] J. Ibriq and I. Mahgoub. Cluster-based routing in wireless sensor networks: Issues and challenges. In *Proc. of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'04)*, pages 795-796, San Jose, California, USA, July 2004. 22
- [IM09] D. Inaudi and L. Manetti. Reinforced Concrete Corrosion Wireless Monitoring System. In *Proc. of the 4th International Conference on Structural Health Monitoring on Intelligent Infrastructure*, Zurich, Switzerland, July 2009. 69
- [INS11] INSYSM. EU FP7 INSYSM Project: Intelligent Systems for Structures Strengthening and Monitoring [online]. 2011. Available from: <http://insysm.polsl.pl/> [cited 18 July 2012]. 6, 7
- [ISH10] M. Imran, A.M. Said, and H. Hasbullah. A Survey of Simulators, Emulators and Testbeds for Wireless Sensor Networks. In *Proc. of the 2010 International Symposium in Information Technology (ITSim)*, volume 2, pages 897-902, Kuala Lumpur, Malaysia, June 2010. 2
- [IVHJH11] Ozlem Durmaz Incel, Lodewijk van Hoesel, Pierre Jansen, and Paul Havinga. Mc-lmac: A multi-channel mac protocol for wireless sensor networks. *Ad Hoc Networks*, 9(1):73 - 94, 2011. Available from: <http://www.sciencedirect.com/science/article/pii/S1570870510000624>. 234, 235, 256, 271, 277, 279, 280, 285
- [JBA07] Vivek Jain, Ratnabali Biswas, and Dharma P. Agrawal. Energy-Efficient and Reliable Medium Access in Sensor Networks. In *Proc. of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2007)*, pages 1-8, June 2007. 391
- [JBT06] Kyle Jamieson, Hari Balakrishnan, and Y.C. Tay. Sift: a MAC Protocol for Event-Driven Wireless Sensor Networks. In *Proc. of the Third European Workshop on Wireless Sensor Networks (EWSN)*, volume 3868, pages 260-275, Zurich, Switzerland, February 2006. 129
- [JDB99] R. Jain, A. Durrezi, and G. Babic. Throughput fairness index: an explanation. *ATM Forum Contribution* 99, 45, 1999. 303

- [JH09] M.R. Jongerden and B.R. Haverkort. Which battery model to use? *IET Software*, 3(6):445-457, December 2009. 9, 154
- [JKLK08] Ho Min Jung, Byung Ki Kim, Wan Yeon Lee, and Young Woong Ko. Icls : Intelligent cricket-based location tracking system using sensor fusion. In *Proc. of the Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD2008)*, pages 461-466, Phuket, Thailand, August 2008. 33, 335
- [JM06] T.M. Johnson and M. Margalho. Wireless sensor networks for agroclimatology monitoring in the brazilian amazon. In *Proc. of the International Conference on Communication Technology (ICCT '06)*, pages 1-4, Guilin, China, November 2006. 33, 334
- [JOW⁺02] Philo Juang, Hidekazu Oki, Yong Wang, Margaret Martonosi, Li Shiuan Peh, and Daniel Rubenstein. Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebrantet. in *Proc. of the 10th Annual Conference on Architectural Support for Programming Languages and Operating Systems*, 30(5):96-107, December 2002. Available from: <http://doi.acm.org/10.1145/605432.605408>. 33, 336
- [JR07] V.M.D. Jagannath and B. Raman. WiBeaM: Wireless bearing monitoring system. In *Proc. of the 2nd International Conference on Communication Systems Software and Middleware (COMSWARE 2007)*, pages 1-8, Bangalore, India, January 2007. 33, 42, 46, 332
- [Jur07] Raja Jurdak. *Wireless Ad Hoc and Sensor Networks: A Cross-Layer Design Perspective (Signals and Communication Technology)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007. 17, 21, 69
- [KGG⁺09] P. Kuryloski, A. Giani, R. Giannantonio, K. Gilani, R. Gravina, V.-P. Seppä, E. Seto, V. Shia, C. Wang, P. Yan, A.Y. Yang, J. Hyttinen, S. Sastry, S. Wicker, and R. Bajcsy. DexterNet: An open platform for heterogeneous body sensor networks and its applications. In *Proc. of the Sixth International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2009)*, pages 92-97, Berkeley, CA, USA, June 2009. 34, 43, 47, 340
- [KHH05a] Mauri Kuorilehto, Marko Hännikäinen, and Timo D. Härmäläinen. A Survey of Application Distribution in Wireless Sensor Networks. *EURASIP Journal Wireless Communications Networking*, 2005(5):774-788, 2005. Available from: <http://dx.doi.org/10.1155/WCN.2005.774>. 89
- [KHH05b] Mauri Kuorilehto, Marko Hännikäinen, and Timo D. Härmäläinen. A survey of application distribution in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2005:774-788, 2005. Available from: <http://dx.doi.org/10.1155/WCN.2005.774>. 13
- [KKJ11] Sumit Kushwaha, Vinay Kumar, and Sanjeev Jain. Node architectures and its deployment in wireless sensor networks: A survey. In Archana Mantri, Suman Nandi, Gaurav Kumar, and Sandeep Kumar, editors, *High Performance Architecture and Grid Computing*, volume 169 of *Communications in Computer and Information Science*, pages 515-526. Springer

Berlin Heidelberg, 2011. Available from: http://dx.doi.org/10.1007/978-3-642-22577-2_70. 25

- [KKK11] Manish Karani, Ajinkya Kale, and Animesh Kopekar. Wireless Sensor Network Hardware Platforms and Multi-channel Communication Protocols: A Survey. In *Proc. of the 2nd National Conference on Information and Communication Technology*, pages 20-23, Nagpur, Maharashtra, India, November 2011. 25
- [KL99] J. H. Kim and J. K. Lee. Capture effects of wireless CSMA/CA protocols in Rayleigh and shadow fading channels. *IEEE Transactions on Vehicular Technology*, 48(4):1277-1286, July 1999. 190
- [KLC⁺10] Jeonggil Ko, Jong Hyun Lim, Yin Chen, Rvázvan Musvaloiu-E, Andreas Terzis, Gerald M. Masson, Tia Gao, Walt Destler, Leo Selavo, and Richard P. Dutton. MEDiSN: Medical emergency detection in sensor networks. *ACM Transactions on Embedded Computing Systems*, 10(1):361-362, 2010. Available from: <http://doi.acm.org/10.1145/1814539.1814550>. 34, 43, 46, 338
- [KLJ⁺06] Mikyung Kang, Junghoon Lee, Yongmoon Jin, Gyung-Leen Park, and Hanil Kim. Design of a prioritized error control scheme based on load differentiation for time sensitive traffic on the wireless lan. *Journal of Networks*, 1(2):45-51, 2006. Available from: <http://ojs.academypublisher.com/index.php/jnw/article/view/01024551>. 19
- [Knu97] Donald E. Knuth. *The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms, section 3.2.1: The linear congruential method. pages 1026*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997. 239
- [KS09] M. Klopfer and I. Simonis, editors. *SANY - an open service architecture for sensor networks*. SANY Consortium, 2009. 50
- [KSC08] Youngmin Kim, Hyojeong Shin, and Hojung Cha. Y-MAC: An Energy-Efficient Multi-channel MAC Protocol for Dense Wireless Sensor Networks. In *Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08)*, pages 53-63, St. Louis, Missouri, USA, April 2008. 397
- [KSEG⁺08] A. Kuntz, F. Schmidt-Eisenlohr, O. Graute, H. Hartenstein, and M. Zitterbart. Introducing Probabilistic Radio Propagation Models in OMNeT++ mobility framework and cross validation check with NS-2. In *Proc. of the First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SimuTools '08)*, page 72, Marseille, France, March 2008. 170
- [KSK⁺08] M. Kuorilehto, J. Suhonen, M. Kohvakka, P. Hämäläinen, M. Hännikäinen, and T.D. Hamalainen. *Ultra-Low Energy Wireless Sensor Networks in Practice: Theory, Realization and Deployment*. John Wiley & Sons, 2008. 91, 92, 100, 103

- [KSW⁺08] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. T. Klein Haneveld, T. E. V. Parker, O. W. Visser, Hermann S. Lichte, and S. Valentin. Simulating wireless and mobile networks in omnet++ the mixim vision. In *Proc. of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (Simu-tools '08)*, pages 71-79, Marseille, France, March 2008. Available from: <http://dl.acm.org/citation.cfm?id=1416222.1416302>. 181, 200, 201, 218
- [KT75] L. Kleinrock and F. Tobagi. Packet switching in radio channels: Part i--carrier sense multiple-access modes and their throughput-delay characteristics. *IEEE Transactions on Communications*, 23(12):1400-1416, 1975. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1092768>. 189, 254
- [KVSA04] A. Kochut, A. Vasan, A.U. Shankar, and A. Agrawala. Sniffing Out the Correct Physical Layer Capture Model in 802.11b. In *Proc. of the 12th IEEE International Conference on Network Protocols (ICNP 2004)*, pages 252-261, Berlin, Germany, October 2004. Available from: <http://dl.acm.org/citation.cfm?id=1025124.1025897>. 200
- [KW05] Holger Karl and Andreas Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, 2005. 13, 14, 16, 20, 23, 28, 82, 90, 213, 214, 367
- [LDBO⁺05] Y. Li, F. De Bernardinis, B. Otis, J.M. Rabaey, and A.S. Vincentelli. A low-power mixed-signal baseband system design for wireless sensor networks. In *Proc. of the IEEE Custom Integrated Circuits Conference (CICC 2005)*, pages 55-58, San Jose, California, USA, September 2005. 20
- [LDCO06] W. L. Lee, A. Datta, and R. Cardell-Oliver. FlexiMAC: A flexible TD-MA-based MAC protocol for fault-tolerant and energy-efficient wireless sensor networks. In *Proc. of 14th IEEE International Conference on Networks (ICON '06)*, volume 2, pages 1-6, Singapore, Republic of Singapore, September 2006. 394
- [LE06a] Zhenzhen Liu and I. Elhanany. RL-MAC: A QoS-Aware Reinforcement Learning based MAC Protocol for Wireless Sensor Networks. In *Proc. of the 2006 IEEE International Conference on Networking, Sensing and Control (ICNSC '06)*, pages 768-773, Florida, USA, April 2006. 398
- [LE06b] J. Luo and A. Ephremides. Power levels and packet lengths in random multiple access with multiple-packet reception capability. *IEEE Transactions on Information Theory*, 52(2):414-420, 2006. 190
- [LEM] Tracking user position in immersive environments using wireless sensor networks. Available from: <http://gems.leme.org.pt/PmWiki/index.php/Projects/LEMeRoom>. 33, 43, 46, 335
- [LEQ05] Yang Liu, I. Elhanany, and Hairong Qi. An Energy-Efficient QoS-aware Media Access Control Protocol for Wireless Sensor Networks. In *Proc. of the IEEE*

International Conference on Mobile Adhoc and Sensor Systems Conference (MASS 2005), pages 191-194, Washington, DC, USA, November 2005. 397

- [LGF07] Hung-Cuong Le, H. Guyennet, and V. Felea. OBMAC: An Overhearing Based MAC Protocol for Wireless Sensor Networks. In *Proc. of the International Conference on Sensor Technologies and Applications (SensorComm 2007)*, pages 547-553, Valencia, Spain, October 2007. 251
- [LH06] M. Lacage and T. R. Henderson. Yet another network simulator. In *Proc. of the 2006 workshop on ns-2: the IP network simulator (WNS2 '06)*, Pisa, Italy, October 2006. Available from: <http://doi.acm.org/10.1145/1190455.1190467>. 200
- [LHA08] Hieu Khac Le, D. Henriksson, and T. Abdelzaher. A Practical Multi-channel Media Access Control Protocol for Wireless Sensor Networks. In *Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08)*, pages 70-81, St. Louis, Missouri, USA, April 2008. 389
- [LKL⁺07] J. Lee, W. Kim, S. J. Lee, D. Jo, J. Ryu, T. Kwon, and Y. Choi. An experimental study on the capture effect in 802.11a networks. In *Proc. of the second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization (WinTECH'07)*, pages 19-26, New York, NY, USA, 2007. ACM. Available from: <http://dx.doi.org/10.1145/1287767.1287772>. xxxii, 190, 192, 193, 194, 195, 200
- [LKR04] G. Lu, B. Krishnamachari, and C.S. Raghavendra. An adaptive energy-efficient and low-latency mac for data gathering in wireless sensor networks. In *Proc. of the 18th International Parallel and Distributed Processing Symposium*, page 224, Santa Fe, New Mexico, April 2004. 394
- [LMFJ⁺04] Konrad Lorincz, David J. Malan, Thaddeus R.F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainland, Matt Welsh, and Steve Moulton. Sensor networks for emergency response: Challenges and opportunities. *IEEE Pervasive Computing*, 3(4):16-23, 2004. 34, 338
- [Lor04] Andreas Vad Lorentzen. Low-power processors for the hogthrob project. Master's thesis, Technical University of Denmark DTU, Lyngby, 2004. 33, 336
- [LQW04] P. Lin, C. Qiao, and X. Wang. Medium access control with a dynamic duty cycle for sensor networks. In *Proc. of the 2004 IEEE Wireless Communications and Networking Conference (WCNC 2004)*, volume 3, pages 1534-1539, Atlanta, Georgia, USA, March 2004. 390
- [LRLK08] J. Lee, J. Ryu, S. Lee, and T. Kwon. Revamping the ieee 802.11a phy simulation models. In *Proc. of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems (MSWiM'08)*, pages 28-36, Vancouver, British Columbia, Canada, 2008. Available from: <http://doi.acm.org/10.1145/1454503.1454513>. 189, 217, 254

- [LRW04] E.-Y.A. Lin, J.M. Rabaey, and A. Wolisz. Power-efficient Rendez-Vous Schemes for Dense Wireless Sensor Networks. In *Proc. of the 2004 IEEE International Conference on Communications*, volume 7, pages 3769-3776, Paris, France, June 2004. 390
- [LSR04] Huan Li, P. Shenoy, and K. Ramamritham. Scheduling communication in real-time sensor applications. In *Proc. of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2004)*, pages 10-18, Toronto, Canada, May 2004. 397
- [MA09] I. Martínez and C. Andrade. Examples of reinforcement corrosion monitoring by embedded sensors in concrete structures. *Cement and Concrete Composites*, 31(8):545 - 554, 2009. <ce:title>Sustainability of Civil Engineering Structures - Durability of Concrete</ce:title>. Available from: <http://www.sciencedirect.com/science/article/pii/S0958946509000936>. 359
- [Mah06] Nitaigour P. Mahalik. *Sensor Networks and Configuration: Fundamentals, Standards, Platforms, and Applications*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006. 92
- [Mar04] Geoff Martin. An evaluation of ad-hoc routing protocols for wireless sensor networks. Master's thesis, Newcastle University, United Kingdom, 2004. 33, 43, 47, 336
- [MC03] Rex Min and Anantha Chandrakasan. Top five myths about the energy consumption of wireless communication. *SIGMOBILE Mobile Computing and Communications Review*, 7(1):65-67, 2003. Available from: <http://doi.acm.org/10.1145/881978.881998>. 29
- [MC05] A. Sangiovanni Vincentelli M. Carloni, A. Ferrari. Research activity in the area of distributed wireless embedded systems. Technical report, University of Trento, 2005. 18
- [MCP⁺02] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *Proc. of the 1st ACM international workshop on Wireless sensor networks and applications (WSNA '02)*, pages 88-97, Atlanta, Georgia, USA, September 2002. Available from: <http://doi.acm.org/10.1145/570738.570751>. 33, 152, 333
- [MCS⁺10] W. McCarter, T. Chrisp, G. Starrs, N. Holmes, L. Basheer, M. Basheer, and S. Nanukuttan. Developments in Monitoring Techniques for Durability Assessment of Cover-Zone Concrete. In *Proc. of the 2nd International Conference on Durability of Concrete Structures*, Sapporo, Japan, November 2010. 359
- [MDN12] D. Messaoud, D. Djamel, and B. Nadjib. Survey on Latency Issues of Asynchronous MAC Protocols in Delay-Sensitive Wireless Sensor Networks. *IEEE Communications Surveys Tutorials*, 14(4):1-23, 2012. 11

- [MGAL04] 6. F. Martin, P. Gorday, J. Adams, and H.v. Leeuwen. IEEE 802.15.4 PHY Capabilities. Technical report, 2004. xxxiii, 370, 373
- [MGN⁺05] Sarah Mount, Elena Gaura, Robert M. Newman, Alastair R. Beresford, Sam R. Dolan, and Michael Allen. Trove: a physical game running on an ad-hoc wireless sensor network. In *Proc. of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies (sOc-EUSAI '05)*, pages 235-239, Grenoble, France, October 2005. Available from: <http://doi.acm.org/10.1145/1107548.1107607>. 34, 340
- [MHA04] Yong Ma and James H. Aylor. System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology. *IEEE Transactions on Mobile Computing*, 3(3):286-294, 2004. Available from: <http://dx.doi.org/10.1109/TMC.2004.27>. 18
- [MID04] MIDRA. Users needs report. Technical Report Deliverable D11- WP7, -, 2004. 33, 333
- [MKPS01] Seapahn Meguerdichian, Farinaz Koushanfar, Miodrag Potkonjak, and Mani B. Srivastava. Coverage problems in wireless ad-hoc sensor networks. In *Proc. of the IEEE International Conference on Computer Communications (INFOCOM 2001)*, pages 1380-1387, Anchorage, Alaska, April 2001. 16
- [MLT09] *MLT1010 Datasheet*, 2009. Datasheet. Available from: http://www.adinstruments.com/products/hardware/research/product/MLT1010*D/. 62
- [MRX08] S. Misra, M. Reisslein, and G. Xue. A survey of multimedia streaming in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 10(4):18-39, 2008. Available from: <http://dx.doi.org/10.1109/SURV.2008.080404>. 18
- [MSM05] J. Misić, S. Shafi, and V. B. Misić. Maintaining Reliability Through Activity Management in 802.15.4 Sensor Networks. In *Proc. of the Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks*, pages 5-15, Lake Buena Vista, FL, USA, 2005. Available from: <http://dx.doi.org/10.1109/QSHINE.2005.31>. 190
- [MSP12a] *MSP430-P-1232 Datasheet*, 2012. Datasheet. Available from: <http://www.ti.com/lit/ds/symlink/msp430f1232.pdf>. 84
- [MSP12b] *Proto-Board MSP430-P-1232M Schematic*, 2012. Schematic. Available from: <https://www.olimex.com/dev/images/msp430-p1232m-sch.gif>. 83
- [MV04] W. John McCarter and O. Vennesland. Sensor systems for use in reinforced concrete structures. *Construction and Building Materials*, 18:351-358, 2004. 68

- [MYT⁺06] JD Margulici, Samuel Yang, Chin-Woo Tan, Pulkit Grover, and Andre Markarian. Innovative transportation products and services evaluation of wireless traffic sensors-sensys: Final report. Technical report, Sensys Networks, 2006. 33, 331
- [Nam84] C. Namislo. Analysis of mobile radio slotted aloha networks. *IEEE Journal on Selected Areas in Communications*, 2(4):583-588, 1984. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1146088>. 190
- [Nic05] D. Niculescu. Communication paradigms for sensor networks. *IEEE Communications Magazine*, 43(3):116-122, March 2005. Available from: <http://dx.doi.org/10.1109/MCOM.2005.1404605>. 93
- [NSR08] Ashley Norris, Mohamed Saafi, and Peter Romine. Temperature and moisture monitoring in concrete structures using embedded nanotechnology/microelectromechanical systems (MEMS) sensors. *Construction And Building Materials*, 22(2):111-120, February 2008. 68
- [OAVRH07] El Moustapha Ould-Ahmed-Vall, George F. Riley, and Bonnie S. Heck. Large-scale sensor networks simulation with gtsnets. *Simulation*, 83(3):273 - 290, Mar. 2007. Available from: <http://dx.doi.org/10.1177/0037549707081183>. 328
- [oro09] Towards the future internet - a european research perspective, 2009. Available from: <http://oro.open.ac.uk/24440/>. 51
- [oST01] Information Technology Laboratory (National Institute of Standards and Technology). *Announcing the Advanced Encryption Standard (AES)*. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD :, 2001. 98
- [PCB00] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proc. of the 6th annual international conference on Mobile computing and networking (MobiCom'00)*, pages 32-43, Boston, Massachusetts, USA, August 2000. Available from: <http://portal.acm.org/citation.cfm?doid=345910.345917>. 190, 254
- [PCKC05] S. Pack, J. Choi, T. Kwon, and Y. Choi. Application aware data aggregation in wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(6), 2005. 16, 22
- [PEE⁺08] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, P. Varaiya, and F. Catthoor. Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer. *IEEE Transactions on Wireless Communications*, 7(9):3359-3371, 2008. 190
- [PHC04] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proc. of the Second ACM International Conference on Embedded Networked Sensor Systems (Sensys'04)*, pages 95-107, Baltimore, MD, USA, November 2004. Available from: <http://dx.doi.org/10.1145/1031495.1031508>. 116, 117, 120

- [PJ04] H. Pham and S. Jha. An Adaptive Mobility-Aware MAC Protocol for Sensor Networks (MS-MAC). In *Proc. of the 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, pages 558-560, Vancouver, Canada, October 2004. 392
- [PL11] C. Providakis and E. Liarakos. T-wieye: An early-age concrete strength development monitoring and miniaturized wireless impedance sensing system. In *Proc. of the 11th International Conference on the Mechanical Behavior of Materials (ICM11)*, volume 10, pages 484-489, Como Lake, Italy, June 2011. Available from: <http://www.sciencedirect.com/science/article/pii/S1877705811002700>. 68
- [PM88] S. K. Park and K. W. Miller. Random number generators: good ones are hard to find. *Commun. ACM*, 31(10):1192-1201, October 1988. Available from: <http://doi.acm.org/10.1145/63039.63042>. 239
- [pol09] *Polymer films*, 2009. Datasheet. Available from: <http://www.meas-spec.com/searchresults.aspx?search=Polyvinylideneoride#>. 66
- [PP11] Animesh Pathak and Viktor K. Prasanna. High-level application development for sensor networks: Data-driven approach. In Sotiris Nikolettseas and José D.P. Rolim, editors, *Theoretical Aspects of Distributed Computing in Sensor Networks*, Monographs in Theoretical Computer Science. An EATCS Series, pages 865-891. Springer Berlin Heidelberg, 2011. 51
- [PRO12] PROENERGY-WSN. PROENERGY-WSN Project: Prototypes for Efficient Energy Self-sustainable Wireless Sensor Networks [online]. 2012. Available from: <http://www.e-projects.ubi.pt/proenergy-wsn/> [cited 18 July 2012]. 6
- [PTR06] Prentice Hall PTR. *Data and Computer Communications*, 8 edition. Prentice Hall PTR, 2006. 89
- [PWVW08] Glenn Platt, Joshua Wall, Philip Valencia, and John K. Ward. The Tiny Agent - wireless sensor networks controlling energy resources. *Journal of Networks*, 3(4):42-50, 2008. 34, 337
- [QK10] B. Quinn and G. Kelly. Feasibility of embedded wireless sensors for monitoring of concrete curing and structural health. In *Proc. of the Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems 2010*, San Diego, USA, March 2010. 78
- [RADs⁺00] J.M. Rabaey, M.J. Ammer, Jr. da Silva, J.L., D. Patel, and S. Roundy. Picoradio supports ad hoc ultra-low power wireless networking. *Computer*, 33(7):42-48, July 2000. 389
- [Rap01] Theodore Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2nd edition, 2001. xxxiii, 366, 367, 368, 369

- [REHD08] J. Rousselot, A. El-Hoiydi, and J.-D. Decotignie. Low power medium access control protocols for wireless sensor networks. In *Proc. of the 14th European Wireless Conference (EW 2008)*, pages 1-5, Prague, Czech Republic, June 2008. 138, 139, 170, 171, 177, 181
- [res09] *Respisenze device*, 2009. Datasheet. Available from: <http://www.respisenze.com/en/index.php>. 65
- [RMC02] Wireless Communication Rex, Rex Min, and Anantha Ch. Top five myths about the energy consumption of wireless communication. *ACM Sigmoblie Mobile Communication and Communications Review*, 6:65-67, 2002. 23
- [RML05] Andersson Rikard, Sandberg Martin, and Urszuly László. Open secure office project : Wireless sensor network, 2005. 34, 340
- [ROJ08] Antonio G. Ruzzelli, Gregory M. P. O'Hare, and Raja Jurdak. MERLIN: Cross-layer Integration of MAC and Routing for Low Duty-Cycle Sensor Networks. *Ad Hoc Networks*, 6(8):1238-1257, 2008. Available from: <http://dx.doi.org/10.1016/j.adhoc.2007.11.012>. 122
- [ROLG11] Yi Ren, Vladimir Oleshchuk, Frank Y. Li, and Xiaohu Ge. Security in mobile wireless sensor networks a survey. *Journal of Communications*, 6(2):128-142, 2011. Available from: <http://ojs.academypublisher.com/index.php/jcm/article/view/0602128142>. 12
- [RPBS11] Laura M. Rodriguez Peralta, Lina M.P.L. Brito, and João F.F. Santos. Managing collaborative sessions in wsns. In GeorgeA. Tsihrintzis, Maria Virvou, LakhmiC. Jain, and RobertJ. Howlett, editors, *Intelligent Interactive Multimedia Systems and Services*, volume 11 of *Smart Innovation, Systems and Technologies*, pages 1-10. Springer Berlin Heidelberg, 2011. Available from: http://dx.doi.org/10.1007/978-3-642-22158-3_1. 25
- [RWA⁺08] Injong Rhee, A. Warriar, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-MAC: A Hybrid MAC for Wireless Sensor Networks. *IEEE/ACM Transactions on Networking*, 16(3):511-524, June 2008. 396
- [RY06] X. Ren and H. Yu. Security mechanisms for wireless sensor networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 6(3):155-161, 2006. 22
- [SBF⁺04] T. Sivaharan, G. Blair, A. Friday, M. Wu, H. Duran-Limon, P. Okanda, and C.F. Sørensen. Cooperating Sentient Vehicles for Next Generation Automobiles. In *Proc. of the first Workshop on Applications of Mobile Embedded Systems (MobiSys)*, Boston, Massachusetts, USA, June 2004. 336
- [SBI] Secure border initiative (sbi) and sbinet project. Available from: <http://www.boeing.com/defense-space/sbinet/>. 33, 332
- [SC89] P.S. Sang and NAVAL POSTGRADUATE SCHOOL MONTEREY CA. *On Capture Effect of FM Demodulators*. Defense Technical Information Center, 1989. 190

- [SCM⁺08] N. Santhapuri, R. R. Choudhury, J. Manweiler, S. Nelakuduti, S. Sen, and K. Munagala. Message in Message MIM: A case for reordering transmissions in wireless networks. In *Proc. of Seventh ACM Workshop on Hot Topics in Networks (HotNets-VII)*, Calgary, Alberta, Canada, October 2008. 190, 194
- [Sen] SENSEI (integrating the physical with the digital world of the network of the future). Available from: <http://www.ict-sensei.org/>. 52
- [SGAP00] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie. Protocols for self-organization of a wireless sensor network. *IEEE Personal Communications*, 7(5):16-27, 2000. Available from: <http://dx.doi.org/10.1109/98.878532>. 30
- [SHB⁺06] Mani Srivastava, Mark Hansen, Jeff Burke, Andrew Parker, and Sasank Reddy. Wireless urban sensing systems. Technical Report Technical Report 65, UCLA's Center for Embedded Networked Sensing Systems (CENS), Los Angeles, CA, USA, 2006. 51, 52
- [SHT10a] *Datasheet Humidity and Temperature Sensor SHT15*, 2010. Datasheet. Available from: http://www.sensirion.com/fileadmin/user_upload/customers/sensirion/Dokumente/Humidity/Sensirion_Humidity_SHT1x_Datasheet_V5.pdf. 69, 70
- [SHT10b] *Datasheet Humidity and Temperature Sensor SHT21S*, 2010. Datasheet. Available from: http://www.sensirion.com/fileadmin/user_upload/customers/sensirion/Dokumente/Humidity/Sensirion_Humidity_SHT21S_SDM_Datasheet_V3.pdf. 70, 361
- [Sic04] M.L. Sichitiu. Cross-layer Scheduling for Power Efficiency in Wireless Sensor Networks. In *Proc. of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004)*, volume 3, pages 1740-1750, March 2004. 2
- [SK11] Sujesha Sudevalayam and Purushottam Kulkarni. Energy harvesting sensor nodes: survey and implications. *IEEE Communications Surveys and Tutorials*, 13(3):443-461, 2011. 154
- [SKA04] S. Sundresh, W. Kim, and G. Agha. SENS: A Sensor, Environment and Network Simulator. In *Proc. of the 37th Annual Symposium on Simulation (ANSS'04)*, pages 221-228, Arlington, VA, USA, April 2004. Available from: <http://dl.acm.org/citation.cfm?id=987679.987699>. 189, 254
- [Slo91] N.J.A. Sloane. *A handbook of integer sequences*. Boston Academic Press, 1991. 279
- [Sma09] Smart-Clothing. Smart-Clothing Project: Smart Clothing for Health Monitoring and Sport Applications [online]. 2009. Available from: <http://www.e-projects.ubi.pt/smart-clothing/index.html> [cited 18 July 2012]. 6, 55
- [SMZ07a] Kazem Sohraby, Daniel Minoli, and Taieb Znati. *Wireless Sensor Networks: Technology, Protocols, and Applications*. Wiley-Interscience, 2007. 31

- [SMZ07b] Kazem Sohraby, Daniel Minoli, and Taieb Znati. *Wireless Sensor Networks: Technology, Protocols, and Applications*. Wiley-Interscience, 2007. 60
- [SNVW07] E. Stevens-Navarro, V. Vivekanandan, and V. W. S. Wong. Dual and Mixture Monte Carlo Localization Algorithms for Mobile Wireless Sensor Networks. In *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 2007)*, pages 4024-4028, Hong Kong, China, March 2007. Available from: <http://dx.doi.org/10.1109/WCNC.2007.735>. 31
- [SPA10] Eliana Stavrou, Pitsillides, and Andreas. A survey on secure multipath routing protocols in WSNs. *Computer Networks*, 54:2215-2238, 2010. Available from: <http://dx.doi.org/10.1016/j.comnet.2010.02.015>. 12
- [SR11] A. Seema and M. Reisslein. Towards Efficient Wireless Video Sensor Networks: A Survey of Existing Node Architectures and Proposal for A Flex-i-WVSNP Design. *IEEE Communications Surveys Tutorials*, 13(3):462-486, 2011. 25
- [SRJB03] R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data MULEs: modeling a three-tier architecture for sparse sensor networks. In *Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03)*, pages 30-41, Anchorage, AK, USA, May 2003. 19
- [SRS12] P. Suriyachai, U. Roedig, and A. Scott. A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks. *IEEE Communications Surveys Tutorials*, 14(2):240-264, 2012. 19
- [SS07] Xiaolei Shi and G. Stromberg. SyncWUF: An Ultra Low-Power MAC Protocol for Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, 6(1):115-125, January 2007. 390
- [SSJ01] Chien-Chung Shen, Chavalit Srisathapornphat, and Chaiporn Jaikaeo. Sensor Information Networking Architecture and Applications. *IEEE Personal Communications*, 8(4):52-59, August 2001. Available from: citeseer.ist.psu.edu/shen01sensor.html. 29, 30
- [SSS10] S.K. Singh, M.P. Singh, and D.K. Singh. Routing protocols in wireless sensor networks - a survey. *International Journal of Computer Science and Engineering Survey (IJCSES)*, 1(2):63-83, 2010. 12
- [Sto06] Ivan Stojmenovic. Localized network layer protocols in wireless sensor networks based on optimizing cost over progress ratio. *IEEE Network*, 20(1):21-27, 2006. 18
- [SW04a] Naveen Sastry and David Wagner. Security considerations for ieee 802.15.4 networks. In *Proc. of the 3rd ACM Workshop on Wireless Security (WiSe '04)*, pages 32-42, Philadelphia, PA, USA, October 2004. 31
- [SW04b] H. Schwetlick and A. Wolf. PSSS - Parallel Sequence Spread Spectrum a Physical Layer for RF Communication. In *Proc. of 2004 IEEE International Symposium on Consumer Electronics*, pages 262-265, Algarve, Portugal, September 2004. 99

- [SWZ⁺08] Lei Shu, Chun Wu, Yan Zhang, Jiming Chen, Lei Wang, and Manfred Hauswirth. Nettopo: beyond simulator and visualizer for wireless sensor networks. *Special Interest Group on Embedded Systems (SIGBED) Review*, 5(3):1 - 8, October 2008. Available from: <http://doi.acm.org/10.1145/1534490.1534492>. 326
- [TAGH02] Sameer Tilak, Nael B. Abu-Ghazaleh, and Wendi Heinzelman. A taxonomy of wireless micro-sensor network models. *ACM Mobile Computing And Communications Review*, 6(2):28-36, 2002. 17
- [TBZB012] Bulent Tavli, Kemal Bicakci, Ruken Zilan, and JoseM. Barcelo-Ordinas. A survey of visual sensor network platforms. *Multimedia Tools and Applications*, 60:689-726, 2012. Available from: <http://dx.doi.org/10.1007/s11042-011-0840-z>. 25
- [TIB11] TIBUCON Project. Self Powered Wireless Sensor Network for HVAC System Energy Improvement [online]. 2011. Available from: <http://www.tibucon.eu/summary.html> [cited 20 August 2012]. 337
- [TJB04] Y.C. Tay, K. Jamieson, and H. Balakrishnan. Collision-Minimizing CSMA and its Applications to Wireless Sensor Networks. *IEEE Journal on Selected Areas in Communications*, 22(6):1048-1057, aug. 2004. 116, 118
- [TK85] Hideaki Takagi and Leonard Kleinrock. Throughput analysis for persistent csma systems. *IEEE Transactions on Communications*, 33:627-638, 1985. 116
- [TPS⁺05] Gilman Tolle, Joseph Polastre, Robert Szewczyk, David Culler, Neil Turner, Kevin Tu, Stephen Burgess, Todd Dawson, Phil Buonadonna, David Gay, and Wei Hong. A macroscope in the redwoods. In *Proc. of the 3rd International Conference on Embedded Networked Sensor Systems (SenSys'05)*, pages 51-63, San Diego, California, USA, November 2005. Available from: <http://doi.acm.org/10.1145/1098918.1098925>. 255
- [TSGJ11a] Lei Tang, Yanjun Sun, O. Gurewitz, and D.B. Johnson. PW-MAC: An energy-efficient predictive-wakeup MAC protocol for wireless sensor networks. In *Proc. of the 30th IEEE International Conference on Computer Communications (INFOCOM 2011)*, pages 1305-1313, Shanghai, China, April 2011. 238, 239
- [TSGJ11b] Lei Tang, Yanjun Sun, Omer Gurewitz, and David B. Johnson. EM-MAC: a dynamic multichannel energy-efficient MAC protocol for wireless sensor networks. In *Proc. of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '11)*, pages 23-34, Paris, France, 2011. Available from: <http://doi.acm.org/10.1145/2107502.2107533>. 236, 237, 238, 239, 252
- [Uni05] International Telecommunication Union. ITU internet report 2005: The internet of things. 2005. 53
- [Var10] A. Varga. Omnet++. In K. Wehrle, M. Günes, and J. Gross, editors, *Modeling and Tools for Network Simulation*, pages 35-58. Springer Verlag, September 2010. 138, 139, 170, 181, 182, 192, 194, 365

- [VC02] Fernando J. Velez and Luís M. Correia. Mobile broadband services: Classification, characterisation and deployment scenarios. *IEEE Communications Magazine*, 40(4):142-150, April 2002. 14
- [VCB⁺02] Andras Veres, Andrew T. Campbell, Michael Barry, Li hsiang Sun, and Student Member. Supporting service differentiation in wireless packet networks using distributed control. *IEEE Journal on Selected Areas in Communications*, 19(10):2094-2104, 2002. 18
- [vDL03] Tijs van Dam and Koen Langendoen. An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks. In *Proc. of the 1st International Conference on Embedded Networked Sensor Systems, SenSys '03*, pages 171-180, New York, NY, USA, November 2003. ACM. Available from: <http://doi.acm.org/10.1145/958491.958512>. 392
- [VH08] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proc. of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (Simutools '08)*, pages 1-10, ICST, Brussels, Belgium, Belgium, 2008. 138, 139
- [VHH04] L. F. W. Van Hoesel and P. J. M. Havinga. A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks: Reducing Preamble Transmissions and Transceiver State Switches. In *Proc. of the 1st International Workshop on Networked Sensing Systems (INSS)*, pages 205-208, Tokyo, Japan, June 2004. Society of Instrument and Control Engineers (SICE). Available from: <http://doc.utwente.nl/64756/>. 393
- [vHH09] L.F.W. van Hoesel and P.J.M. Havinga. Analysis of a self-organizing algorithm for time slot selection in schedule-based medium access. Technical Report TR-CTIT-09-06, University of Twente, Enschede, January 2009. Available from: <http://doc.utwente.nl/65358/>. 173
- [VPM⁺07] Rik Vullings, Chris Peters, Massimo Mischi, Rob Sluijter, Guid Oei, and Jan Bergmans. Artifact reduction in maternal abdominal ECG recordings for fetal ECG estimation. in *Proc. of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2007:43-46, 2007. Available from: <http://www.ncbi.nlm.nih.gov/pubmed/18001884>. 62
- [WAJR⁺04] Geoff Werner-Allen, Jeff Johnson, Mario Ruiz, Jonathan Lees, and Matt Welsh. Monitoring Volcanic eruptions with a Wireless Sensor Network. Technical Report TR-27-04, Harvard University, Cambridge, Massachusetts, 2004. 42, 46
- [WALJ⁺06] Geoff Werner-Allen, Konrad Lorincz, Jeff Johnson, Jonathan Lees, and Matt Welsh. Fidelity and yield in a volcano monitoring sensor network. In *Proc. of the 7th symposium on operating systems design and implementation (OSDI '06)*, pages 381-396, Berkeley, CA, USA, November 2006. USENIX Association. Available from: <http://portal.acm.org/citation.cfm?id=1298455.1298491>. 33, 42, 46, 333

- [WALW⁺06] Geoffrey Werner-Allen, Konrad Lorincz, Matt Welsh, Omar Marcillo, Jeff Johnson, Mario Ruiz, and Jonathan Lees. Deploying a Wireless Sensor Network on an Active Volcano. *IEEE Internet Computing*, 10(2):18 - 25, Mar. 2006. Available from: <http://dx.doi.org/10.1109/MIC.2006.26>. 326
- [WBD⁺06] T. Watteyne, A. Bachir, M. Dohler, D. Barthe, and I. Auge-Blum. 1-hopMAC: An Energy-Efficient MAC Protocol for Avoiding 1-hop Neighborhood Knowledge. In *Proc. of the 3rd Annual IEEE Communications Society Sensor and Ad Hoc Communications and Networks (SECON '06)*, volume 2, pages 639-644, Reston, VA, U.S.A., September 2006. 123
- [WCS11] Yik-Chung Wu, Q. Chaudhari, and E. Serpedin. Clock synchronization of wireless sensor networks. *Signal Processing Magazine, IEEE*, 28(1):124 -138, jan. 2011. 236, 237
- [WJCD00] C. Ware, J. Judge, J. F. Chicharo, and E. Dutkiewicz. Unfairness and capture behaviour in 802.11 adhoc networks. In *Proc. of the IEEE International Conference on Communications (ICC 2000)*, volume 1, pages 159-163, New Orleans, LA, USA, June 2000. 190
- [WLH⁺08] Yadong Wan, Lei Li, Jie He, Xiaotong Zhang, and Qin Wang. Anshan: Wireless sensor networks for equipment fault diagnosis in the process industry. In *Proc. of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08)*, pages 314-322, California, USA, June 2008. 34, 43, 46, 338
- [WMRD11] T. Watteyne, A. Molinaro, M.G. Richichi, and M. Dohler. From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols. *IEEE Communications Surveys Tutorials*, 13(4):688-707, 2011. 12
- [WPW⁺07] Wei Wang, Dongming Peng, Honggang Wang, H. Sharif, and Hsiao-Hwa Chen. Energy efficient multirate interaction in distributed source coding and wireless sensor network. In *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC 2007)*, pages 4091-4095, Hong Kong, China, March 2007. 20
- [WSKW09] K. Wessel, M. Swigulski, A. Köpke, and D. Willkomm. Mixim: the physical layer an architecture overview. In *Proc. of the 2nd International Conference on Simulation Tools and Techniques (Simutools'09)*, pages 78-86, Rome, Italy, March 2009. Available from: <http://dx.doi.org/10.4108/ICST.SIMUTOLS2009.5555>. xxiii, 139, 194, 201, 202, 204, 218, 365
- [WWJ⁺05] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler. Exploiting the capture effect for collision detection and recovery. In *Proc. of the 2nd IEEE workshop on Embedded Networked Sensors (EmNetS-II)*, pages 45-52, Washington, DC, USA, May 2005. Available from: <http://dl.acm.org/citation.cfm?id=1251990.1253398>. 189, 190, 193, 199, 254
- [YBO08] B. Yahya and J. Ben-Othman. An Energy Efficient Hybrid Medium Access Control Scheme for Wireless Sensor Networks with Quality of Service Guarantees. In *Proc. of the IEEE Global Telecommunications Conference 2008*

(*IEEE GLOBECOM 2008*), pages 1-5, New Orleans, LA, USA, December 2008. 121

- [YBO09] Bashir Yahya and Jalel Ben-Othman. Towards a classification of energy aware mac protocols for wireless sensor networks. *Wireless Communications and Mobile Computing*, 9(12):1572-1607, 2009. 11, 111, 116, 159
- [YHE04] W Ye, J Heidemann, and D Estrin. Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks. *IEEE/ACM Networking Transactions*, 12(3):493-506, June 2004. Available from: <http://dx.doi.org/10.1109/TNET.2004.828953>. 2, 7, 111, 116, 118, 121, 129
- [YK06] K.Y. Yazdandoost and R. Kohno. Antenna, Wave Propagations, and Field Regions for Body Area Network (IEEE 802.15-06-0397-00-0ban). Technical report, 2006. 368
- [YSH06] W Ye, F Silva, and J Heidemann. Ultra-Low Duty Cycle MAC with Scheduled Channel Polling. In *Proc. of the Fourth ACM International Conference on Embedded Networked Sensor Systems (SenSys'06)*, pages 321-333, Boulder, Colorado, USA, November 2006. Available from: <http://www.isi.edu/~johnh/PAPERS/Ye06a.html>. 7, 8, 120, 130, 131, 134, 143, 144, 145, 149, 151, 152, 159, 182, 186, 191, 233, 235, 236, 242, 246, 247, 251, 256
- [YV06] X Yang and NH Vaidya. A Wireless MAC Protocol using Implicit Pipelining. *IEEE Transactions on Mobile Computing*, 5(3):258-273, 2006. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1580473. 130, 233
- [ZC05] Ze Zhao and Li Cui. Easimed: A remote health care solution. In *Proc. of the 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS 2005)*, pages 2145-2148, Shanghai, China, January 2005. 34, 339
- [ZCLP07] Wensheng Zhang, Guohong Cao, and Tom La Porta. Dynamic Proxy Tree-based Data Dissemination Schemes for Wireless Sensor Networks. *Wireless Networks*, 13(5):583-595, 2007. Available from: <http://dx.doi.org/10.1007/s11276-006-6254-6>. 31
- [ZHY⁺06] G. Zhou, C. Huang, T. Yan, T. He, J. A. Stankovic, and T. F. Abdelzaher. MMSN: Multi-Frequency Media Access Control for Wireless Sensor Networks. In *Proc. of the 25th IEEE International Conference on Computer Communications (INFOCOM 2006)*, pages 1-13, Barcelona, Catalunya, Spain, April 2006. 279
- [ZK03] Marco Zúñiga and Bhaskar Krishnamachari. Integrating future large-scale wireless sensor networks with the internet. Technical Report CS 03-792, University of Southern California, February 2003. 23
- [ZZJ09] J. Zheng, J. Zheng, and A. Jamalipour. *Wireless Sensor Networks: A Networking Perspective*. John Wiley & Sons, 2009. 91