UNIVERSITY OF BEIRA INTERIOR
Faculty of Engineering
Department of Informatics

Cooperation Mechanisms for Pervasive Mobile Health Applications

Tiago Miguel Fonseca Machado

Submitted to the University of Beira Interior in candidature for the Degree of Master of Science in Informatics Engineering

Supervised by Prof. Doutor Joel José Puga Coelho Rodrigues

Department of Informatics
University of Beira Interior
Covilhã, Portugal
http://www.di.ubi.pt

Acknowledgements

First of all, I would like to thank Professor Joel José Puga Coelho Rodrigues for all the support, for all the constant words of encouragement and for supervising my Master’s Thesis. The last year was undoubtedly very important in my evolution has informatics Engineer and as a person as well.

I am most grateful to the University of Beira Interior, the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, Portugal, and SAPO – Portugal Telecom for allowing me to work on this project with them.

Many thanks to all members of NetGNA, particularly Ivo Lopes, João Isento, Bruno Silva, João Dias and Orlando Pereira.

And of course, a enourmous thanks to my family and my girlfriend, for their constant support and for all words of motivation.

Abstract

The emergence of mobile health and Web-based services along with new ubiquitous mechanisms are providing new methods to deliver services that overcomes geographical and temporal barriers, delivering information regardless place and time. With the proliferation of mobile devices, online markets have been growing with many health applications, allowing users to have access to health records, treatment plans, alerts and health goals establishment (e.g., weight loss). This recent ubiquitous paradigm is much possible due to Web Services capabilities and new data-interchange notations, as well as the evolution of mobile software development kits. However, m-health architectures that depend on wireless networks have several constraints such as mobile devices battery, processor and memory resources, as well as issues regarding network connectivity and communication delays. Cooperation mechanisms have proven to be a promising solution to approach these constraints.

In a typical cooperation strategy, information transmitted through wireless channels is usually relayed through a relay node and/or a relay station (i.e., a base station), using a packet forwarding cooperation model. While some cooperation approaches aim multiple constraints, such as bandwidth performance, wireless frequency management or localization improvement, other approaches aim one specific network or limitation inherent to mobile devices, such as battery power or processing power issues. In this work a novel cooperation strategy for m-health services following service oriented architectures is proposed in order to approach two common drawbacks in mobile health systems: the Internet connectivity

and infrastructure dependencies. A reputation-based model is used, where a Web Service is responsible for nodes reputation management, as well as for the access control. At the client-side (i.e., in the mobile device) four software modules are used in order to manage and control the ubiquitous cooperation process. The ultimate goal is to provide an alternative for remote access, where mobile devices without Internet connectivity could retrieve remotely stored health data through cooperation. Packet forwarding should occur through short and low energy consuming communications, specifically through Bluetooth interface. This results in a free of charge alternative to cellular data network connections and independent of WiFi access points.

Although the referred mechanisms aim any mobile health application, this work was carried with SAPO – Portugal Telecom and for test purposes a specific mobile health application, namely SapoFit, was used. Cooperation mechanisms were created and integrated in SapoFit, and a cooperative Web Service was built. A performance evaluation in a real scenario with different mobile devices is performed and presented in this work. The request and response message delays are measured, while varying the number of uncooperative nodes, and verifying the required time for each individual communication process. Furthermore, the memory footprint of the mobile cooperation mechanisms is revealed.

Keywords

Mobile Health, m-Health, Mobile computing, Ubiquitous Health, u-Health, Cooperation, Cooperative communications, Wireless relay communications, Healthcare Application.

Contents

List of Figures

List of Tables

Acronyms

ACT	:	Achieved Cooperation Time
ADT	:	Android Development Tools
AES	:	Advanced Encryption Standard
AP	:	Access Point
API	:	Application Programming Interface
ATT	:	Average Total Time
BAN	:	Body Area Network
BMI	:	Body Mass Index
BS	:	Base Station
BT	:	Bluetooth
BTS	:	Base Transceiver Station
CATV	:	Cable Television
CDMA	:	Code Division Multiple Access
CFB	:	Cipher Feedback
CSCW	:	Computer Supported Cooperative Work
CWS	:	Cooperative Web Service
DBMS	:	Data Base Management System
DSR	:	Dynamic Source Routing
EHR	:	Electronic Health Record
GPS	:	Global Positioning System
GSM	:	Global System for Mobile Communications
HSDPA	:	High-Speed Downlink Packet Access
IDE	:	Interface Development Environment
IN	:	Intermediary Node
IrDA	:	Infrared Data Association

JSON	:	JavaScript Object Notation
JSP	:	Java Server Pages
LAC	:	Location Area Code
LTE	:	Long Term Evolution
LR	:	Long-Range
MANET	:	Mobile Ad-hoc Network
MD	:	Mobile Device
MB	:	Megabyte
MWT	:	Maximum Waiting Period
NCM	:	Node Control Message
NetGNA	:	Next Generation Networks and Applications Group
NFC	:	Near Field Communication
NL	:	Neighbours List
OMG	:	Object Management Group
OS	:	Operating System
P2P	:	Peer-to-peer
PAN		Personal Area Network
PDA	:	Personal Digital Assistant
PHR	:	Personal Health Record
QoE	:	Quality of Experience
QoS	:	Quality of Service
RAM	:	Random Access Memory
RCM	:	Requester Control Message
RPD	:	Response Delay
REST	:	Representational State Transfer
RLN	:	Relay Node
RMS	:	Reputation Management System
RMMS	:	Remote Mobile Monitoring System
RN	:	Requester Node
RQD	:	Request Delay
RL	:	Reputation List

RTCM	:	Rede Temática de Comunicações Móveis
RV	:	Reputation Value
SDK	:	Software Development Kit
SOA	:	Service-Oriented Architecture
SRP	:	Source Routing Protocol
UML	:	Unified Modelling Language
UMTS	:	Universal Mobile Telecommunications System
USB	:	Universal Serial Bus
WBAN	:	Wireless Body Area Network
WiMAX	:	Worldwide Interoperability for Microwave Access
WLAN	:	Wireless Local Area Network
WS	:	Web Service

1. Introduction

1.1. Focus

Health was and still is a central concern for individuals, groups and the global society. Its importance cuts across all ages. There is an important need to make health services available to everyone, regardless the time and place. Mobile devices are changing many economic, social and medical realities. Millions of people who never had a computer now have a smartphone, and the number of sold mobile equipments is increasing [1]. The growing ubiquity of mobile services along with the omnipresence of wireless networks allows the creation of a new generation of electronic health systems based on mobile computing [2]. Mobile healthcare systems are becoming very popular particularly in developing countries [3] and focus towards achieving two main goals [4]: the accessibility of electronic health (e-health) applications with information available anytime and anywhere, along with ubiquitous computing [5].

One of the most widely cited definition regarding ubiquitous computing [6] belongs to Mark Weiser: "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it*". Its goal is to provide services available anytime and anywhere, with systems running continuously, persistently and transparently [7]. User should interact with technology in a transparent approach [8]. Ubiquitous computing focus on the information perceived by the user, and not by the technology behind, responsible for its operation. Ubiquitous health (u-Health) have an important role on healthcare because it allows the creation of monitoring and preventive services, running consistently and providing information as required [9]. This possibility is much related with the emergence of Web Services and mobile technologies. Since mobile phones have limited computational and storage capacity, along with limited battery power, they are not suitable to run heavy algorithms or store big amounts of data [10]. Cloud based mechanisms overcomes those limitations, processing data on the server side, and serving it to the client side (i.e., to mobile devices). Nowadays, these mechanisms are allowing the creation of new ubiquitous health systems, such as portable personal health records (PHR), which are translated in electronic health records (EHRs), allowing medical staff carry patients health records in mobile devices, simplifying the access and exchange of this data [11], [12]. Service Oriented Architectures (SOAs) approaches provides the necessary ubiquity and the necessary mechanisms to deliver mobile health services [13]. Health institutions are primarily device oriented, where software is often manually installed on specific devices, instead of being globally available and consistently updated on all workstations. A service oriented architecture allows software (i.e., health applications) to be available and consistent for both powerful workstations as for simple mobile devices, such as smartphones and tablets [14], enabling the health system as a cloud, with information in it.

With mobile devices proliferation, often in centralized areas or groups, direct communication between devices is required, which is usually carried by a wireless local area network (WLAN). However, when there is not available an access point (AP), mobile nodes (i.e., mobile devices) can create a mobile ad hoc network (MANET), forming a collection of wireless nodes in a temporary and mobile network without centralized infrastructure [15] but with network functionalities. This is particularly useful because it allows the creation of ad hoc groups for field survey operations in remote areas, teams of construction workers on sites could share blueprints and schematics, to coordination of rescue efforts in emergency situations and disaster areas, among others infrastructure-less situations [16]. However, there are some constraints regarding m-health services in wireless networks, such as communication rates, reliability and network connectivity. There are also specific limitations regarding the nodes resources in these networks, like processor power, battery and storage capacity. Beside performance and bandwidth issues, usually considered the major constraints to obtain an optimal packet route in MANETs [17], cooperation mechanisms also focus on solving others limitations. Toward these issues in wireless networks, cooperation is expected to play a central role in the evolution of pervasive service-oriented mobile health applications.

In a closed MANET [18], mobiles nodes cooperate with each other towards a common goal, and have well defined boundaries, not providing open access. In a open MANET [19], mobile nodes have different goals, and share their different resources. Anyone can enter and leave the network at any time. In such type of networks nodes are responsible for all security tasks. In any case, for cooperation to take place (i.e., to ensure packet forwarding), the cooperative node needs to sacrifice its resources, where battery is usually the most sacrificed component. Thus, in some cooperation models a node may refuse to cooperate and sacrifice its own resources, while attempting to benefit from other nodes. Such node is called selfish or misbehaving node [20], [21]. In order to prevent and solve this issue, there are two main types [22] of incentive methods: reputation-based systems, and pricing based incentives. In a reputation-based system nodes behaviour is observed and it is calculated a node reputation value, in order to detect and punish low reputed nodes and isolate them from the network. In pricing-based incentives, nodes are paid for cooperative actions, allowing them to benefit of virtual payments. As it will be approached later, there are several benefits in cooperative communication in MANETs, such as network performance gains, infrastructure dependency, among other advantages [23], [24]. However there are also many challenges in cooperation design, such as bandwidth issues, mobile resources limitations, synchronization and security issues, that could decrease cooperative gains and possibly compromising the efficiency and effectiveness of the network. It is required to carefully approach these issues in order to create a fully efficient and effective cooperation system.

The existence and dissemination of mobile devices with multiple wireless network interfaces has opened many new cooperation possibilities, overcoming limitations due to a single wireless technology. Is now possible to collaborate among multiple mobile devices (MDs) over alternative wireless technologies [25]. Thus, it is possible to create cooperate wireless network architectures where mobile nodes communicate with the base station (BS) or an AP over a long-range (LR) wireless technology, such as UMTS (Universal Mobile Telecommunications System)/ High-Speed Downlink Packet Access (HSDPA), Long Term Evolution (LTE) or Worldwide Interoperability for Microwave Access (WiMAX), using other interfaces to communicate with other mobile nodes over short-range (SR) links, such as Bluetooth, Near Field Communication (NFC) or over a Wireless Local Area Network. Location-awareness [26], [27] can also be used in order to improve node localization, particularly in wireless networks, enabling localization improvement in indoor environments [28], and providing methods to determinate outdoor position more accurately.

1.2. Objectives and Problem Definition

The main objective of this dissertation is to assure that all users of a service-oriented mobile health application, regardless of their connectivity options (i.e., if they have or do not have Internet connectivity through WiFi or cellular network), can accomplish a request for a service and retrieve remote health information. It proposes a reputation-based cooperation strategy for mobile health services, where cooperation mechanisms ubiquitously work in mobile applications. In this model, Web Services are used in order to demonstrate how cooperative mobile health applications with service oriented architectures and Internet connectivity dependency can be used anytime and particularly anywhere, not being confined in a geographical boundary with infrastructure dependency. A cooperation system is used to provide packet forwarding through Bluetooth to mobile devices without Internet connectivity, embracing an alternative to WiFi and 3G/4G modules and providing a larger global connectivity. Although it aims any m-health application, for test purposes the ubiquitous cooperation mechanisms will be integrated with a specific m-health Google Android application, namely SapoFit.

To accomplish this main objective, the following intermediate objectives were identified:

- A detailed study of the state-of-the-art in cooperation mechanisms and approaches, its challenges, advantages and incentive methods, along with the necessary review of mobile health, ubiquitous computing and ubiquitous health;

- The system requirements analysis in order to fetch all necessities of the system;

- The analysis and study of the Google Android Operating System and Web Services architecture.

- Design and implementation of the cooperation mechanisms, including the deployment of a mobile Application Programming Interface (API) on the Android Operating System (OS), along with a Web Service, based on requirements analysis;

- Integration and testing of cooperation mechanisms on the test application.

- The system validation along with the performance evaluation of the cooperation mechanisms;

Finally, this dissertation will summarize all mentioned objectives, make conclusions and propose future work.

1.3. Main Contributions

This section is devoted to the scientific contributions of this dissertation to the state-of-the-art on mobile and ubiquitous health, as well as on cooperation mechanisms.

The main contribution of this dissertation is a performance evaluation of cooperation mechanisms for m-health applications, including a proposal of an infrastructure independent alternative model in order to ensure global connectivity to the Internet across service oriented mobile health applications. This proposal presents a reputation-based cooperation strategy where a Web Service is responsible for the reputation management and access control. A paper with this contribution was accepted for presentation at the Global Communications Conference (IEEE GLOBECOM 2012), Communications QoS, Reliability, and Modeling Symposium (CQRM), Anaheim, USA, December 3-7, 2012 [29].

The second contribution extends the previous proposal with a novel cooperation strategy for mobile health applications, providing a more profound performance evaluation analytical analysis. This contribution was submitted submitted to a major international journal and is under revision.

This work was also presented at the 15th seminar of the Rede Temática de Comunicações Móveis (RTCM), University of Minho, Guimarães, Portugal, June 15, 2012.

1.4. Dissertation Structure

This dissertation is organized in six chapters. This chapter, the first, presents the context of the dissertation, focusing on the topic under study, the objectives, the main contributions and the dissertation structure and its main contributions.

Chapter 2 presents the related work, approaching the literature review on mobile health, including a study on electronic health records and personal health records. It is also presented a literature review on ubiquitous health systems, focusing on the importance of ubiquity and usability. It also presents some mobile ubiquitous solutions. Last, cooperation mechanisms are approached, along with its challenges, advantages, incentive methods and relevant approaches that exist in the literature.

Chapter 3 approaches the requirements analysis for the cooperation system, presenting the essential requirements, used technologies in this work, the behavioural, interaction and structural system diagrams.

Chapter 4 approaches the ubiquitous cooperation mechanisms. First is shortly introduced the android platform and its used ubiquitous mechanisms, such as the necessary Android service. Next, the chapter focus on the cooperation system architecture, which includes the reputation-based strategy and all remaining necessary pervasive mechanisms, namely the node and requester control messages, the neighbours and reputation lists, as well as the cooperative Web Service.

Chapter 5 presents the performance evaluation and system validation. It contains a short presentation of the aimed mobile health test application, demonstrates the created cooperation scenario, performing and focusing on the performance evaluation of the ubiquitous cooperation mechanisms, which includes performance metrics and the performance analysis.

Finally, Chapter 6 summarizes all performed work in this dissertation, presents conclusions on the results of this work, and proposes future work.

2. Related Work

In order to fully understand the context of the thesis objectives and have an awareness of the state-of-the-art, it is required to approach the related work, as a study of the literature review. Over the years, mobile health systems has been widely growing [30]. Health information technologies have been evolving in the past two decades, and many recent contributions are providing an increased healthcare quality to the modern societies [31]. The pervasiveness and ubiquity of technologies, results in new paradigms to the delivery of healthcare, and provides opportunities to create and use new technological solutions to manage wellness [32], such as mobile solutions that provides users methods to retrieve health information anytime and anywhere. At the same time, cooperation mechanisms have also evolved over the last decade, and have already proven that they can solve many constraints related to mobile network architectures [33], such as network performance issues, energy limitations as well as connectivity concerns.

This chapter presents the literature review in mobile health in Section 2.1, while approaching its limitations and challenges, electronic and personal health records. In Section 2.2 is shortly presented the literature review in ubiquitous health, and in Section 2.3 is presented the focus of this chapter, in cooperation mechanisms. It will be approached the challenges to cooperative systems design, its advantages, the existing incentive methods and the most relevant and existing approaches. Last, Section 2.4 will summarize the chapter.

2.1.Mobile Health (m-Health)

Mobile Health (or m-health) resides in health services integration and utilization through mobile technologies. The most widely cited definition belongs to Istepanian et al [34] as "*emerging mobile communications and network technologies for healthcare*". Nowadays, a common use for m-health services from the particular perspective of the user can be found in applications that aim to inform and alert the user so they could have a preventive awareness in their health care. However, m-health is also used for personal health care remote management, patients active state monitoring, treatment support and patients management with chronic diseases. Thus, m-health is widely used in telemedicine [35]. In the Figure 1 is presented the general mobile architecture of a mobile health system.

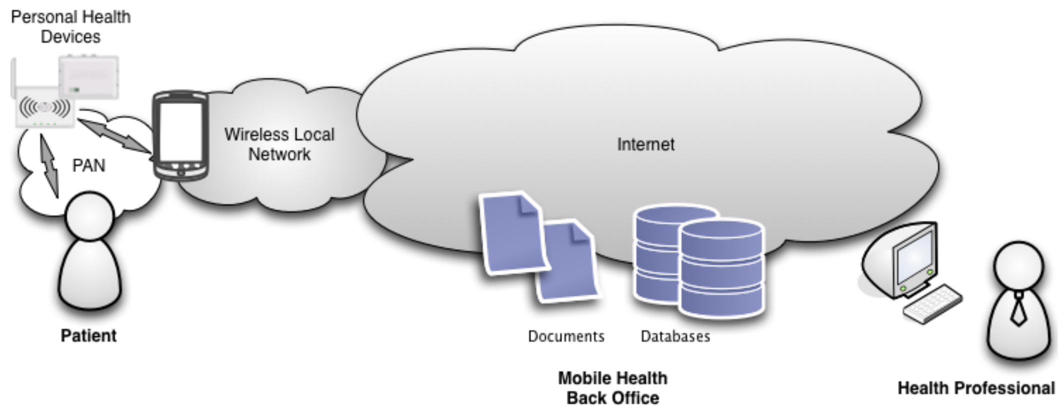


Figure 1. General mobile health system architecture.

The system contains one or more monitoring and/or surveillance devices, such as sensors and video cameras, forming a Personal Area Network (PAN) where information is carried through Bluetooth (BT), Infrared Data Association (IrDA) or WiFi modules. Those modules are wirelessly connected to the patient mobile device (e.g., a smartphone and/or a tablet), which should be connected to the Internet, in order to allow the information storage, which is retrieved from the modules. This information should be remotely stored and organized in databases and/or file systems, to allow its analysis by professional health care providers. Many similar architectural approaches were proposed over the years [36-39], and can be structured and summarized in four main components: (1) data acquisition modules; (2) the intelligent central node which is usually the patient mobile device and communicates with all modules through BT or Wi-Fi; (3) the health data center where all collected information is stored for (4) health providers. Thus, in [35] is emphasized that BT and Global System for Communications (GSM) and Code Division Multiple Access (CDMA) cellular networks should be explored to allow a greater mobility to the system. Hence, in [40] is presented a Remote Mobile Monitoring System (RMMS) for monitorization in motion through the referred mobile technologies.

As previously referred, after collecting patient information, its analysis is required by health professionals. In [41] is proposed a collaborative health model called Computer Supported Cooperative Work (CSCW) awareness-based, to realize human roles that are involved in mobile health monitoring activities.

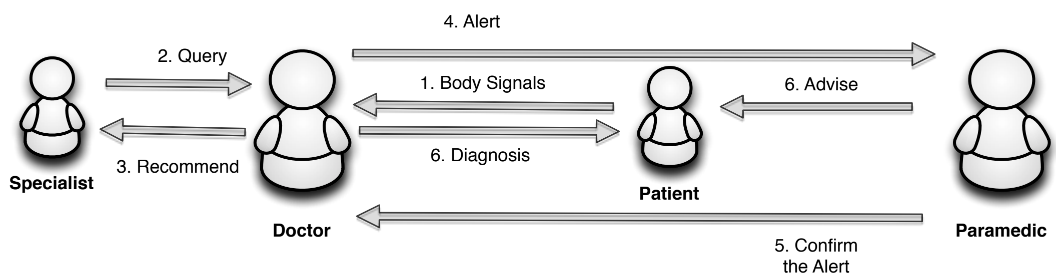


Figure 2. Human roles in a monitoring scenario.

In this model, patients and health professionals are considered as having cooperative roles that are geographical distributed and connected by mobile devices, where software agents are used in order to overcome the problem of different locations. A similar approach is also presented in

[39], and in the Figure 2 we could see the respective scenario. The objective of this model is to smooth integration difficulties in patient monitoring health approaches.

2.1.1. Limitations and challenges

There are some limitations and challenges on m-health systems, and they could be summarized as follows [42]:

- **Mobile devices limitations**, such as battery life consumption much associated with internet connections and its cost when there's no free Wi-Fi access points available as well as the lack of hardware sensors that some mobile e-health solutions requires;
- **User acceptance,** due to system privacy and security issues along with other limitations related to applications usability and reliability;
- **Unstable** data rates for 2.5G and 3.5G services, can cause some difficulties streaming videos in some e-health services, taking into account the actual 4G/LTE still limited worldwide coverage;
- The **lack of standards** can make it difficult to link telemedicine services to some mobile devices.

2.1.2. Electronic Health Record (EHR) and Personal Health Record (PHR)

Nowadays healthcare providers keep medical data in EHRs (Electronic Health Records) [43] to allow medical doctors easily access patient data. A typical EHR system is a structured repository of information regarding the patient medical history [44]. The main advantages of a EHR systems is the capacity to improve health providers efficiency, reducing costs, as well as promoting evidence-based medicine, increasing treatments effectiveness [45]. However, patients may want to obtain its personal health data, add or modify some information to his Personal Health Record (PHR). An Electronic Health Record (EHR) allows medical staff and patients electronically access that information, providing to the former improved access and enhanced ability to make improved decisions, at the same time they could increase the patient awareness to his health [46].

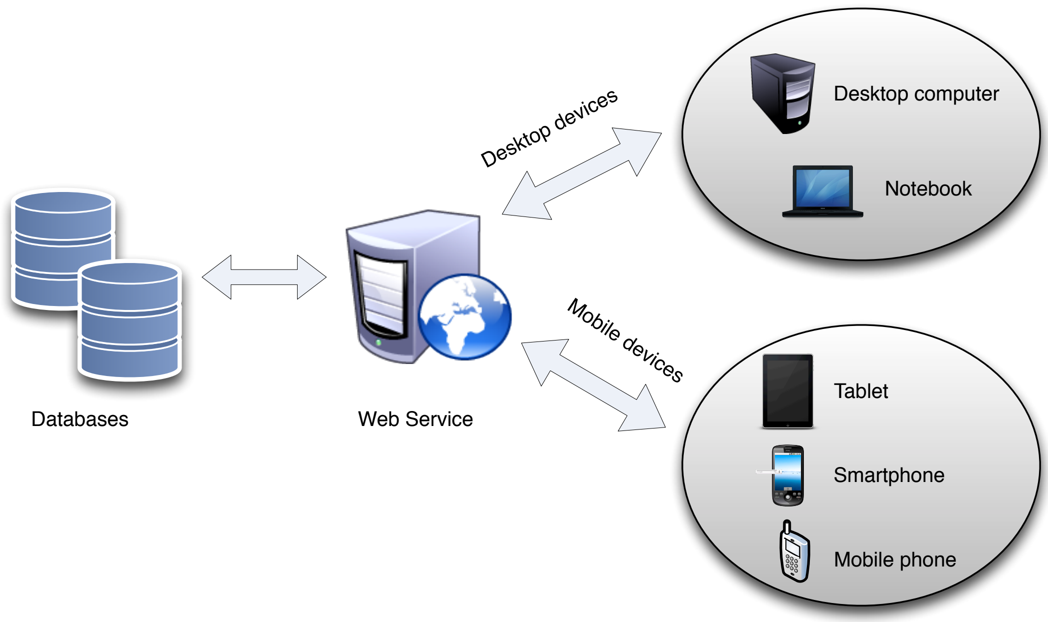


Figure 3. A typical EHR mobile system architecture.

This is much possible because EHR systems enables access to the information regardless of patient time and place [47]. The use of Web Services has an important role to mobile-EHR (m-EHR) systems, providing access to the data in any personal computer, tablet or smartphone that can access the Internet [48]. To provide a higher mobility to medical doctors, in [49] is presented an EHR system, structured by an PHR with six function modules (Prevention, Medical Treatment, Rehabilitation, Health Care, Health Education, Family Planning Guidance), running on a mobile application which connects to a database through a Web Server, where is logically stored all patient data. A typical EHR mobile system architecture [50] can may be seen in Figure 3. Although EHR-based mobile applications are becoming more common, as will be demonstrated, web-based EHR systems are becoming very popular and widely used because they provide users to access its health information through web, not constrained by space and time [51]. Two examples are present in [52], [53] where users can create and manage their PHRs.

Current barriers to PHR/EHR adoption among patients include cost, concerns about information privacy, inconvenience, and potential security issues [54]. Privacy and security are major concerns of the population, particularly if there is a stigma associated with the disease (e.g., HIV/AIDS). In [55] cryptographic mechanisms are proposed to approach these concerns, in order to ensure the confidentially of stored data. However, it is required to address some attention to web based services policies, regarding the user control over the stored data as well as legal issues. As an alternative to mobile applications and web-based PHRs, the MedicAlert Foundation proposes [56] an E-Health Key as a secure, portable and personal health record using USB (Universal Serial Bus) flash technology. The key detects if it's plugged in the patients personal computer or into an unknown computer. In the latter, the key assumes that is being inserted into a medical computer, and in that case is only available critical information and pre-authorized by the patient.

2.2. Ubiquitous Health (u-Health)

As previously referred, mobile devices have limited resources, such as their storage and memory capacity, along with their processing speed, much because of their smallness. MDs computational power makes them unsuitable to run heavy algorithms with many processing tasks [57]. The development of ubiquitous web-based systems releases small computers and mobile devices from these tasks, and provides a more natural embedding, allowing access to remote services and content regardless the time and place in a transparent manner. Ubiquitous computing, which could be present both on server and client side (i.e., on a Web Server and in a mobile device, respectively), provides invisible mechanisms, transparent to the end-user, where software and/or hardware interaction occurs without the user noticing it [58].

A good example of a ubiquitous system is the Internet itself, which allows access to Web Services and helps users maintaining information (e.g., medical records) and access its parameters anywhere in the globe [9]. Another important use of ubiquitous health resides in the use of body area networks (BANs) in patients homes to ubiquitously monitor physicals and physiological parameters [59]. These systems are also known as wireless body area networks (WBANs). Data is collected through sensors (forming the BAN), which is ubiquitously sent and remotely stored to be analysed by medical staff or eventually by the patient itself. Its access is made through a neutral platform (e.g., a web browser). A similar approach [60] uses a wireless local area network and cable television (CATV) network serving as a platform for monitoring patient signals. In [61] is presented the concept of a ubiquitous-bedroom (u-Bedroom) as a part of a ubiquitous-House (u-House), a ubiquitous health monitoring system to retrieve and measure biomedical signals without the individual's awareness.

Although the many possibilities that ubiquitous systems offer, the use of ubiquitous health systems and applications raises many ethical and privacy concerns [62]. Who owns the health information, how is stored and who is responsible for its management, how confidential it is, are all issues that concerns the patient and disincentive ubiquitous health systems use. In order to allow the natural grow of ubiquitous health systems and mobile applications is important to carefully approach this issue and provide an awareness to the user of the data treatment.

2.2.1. Ubiquitous Mobile Health

With the propagation of mobile devices [63], online markets have been growing with more health applications [64] that allows to its users many possibilities, such as health record registering, treatments alert, and health goals establishment. Those applications exist in many popular mobile platforms, such as *Google Android OS* [65], *iOS* [66] and *Symbian OS* [67], with theirs respective applications stores, such as the *Google Play* [68] (formerly *Google Android Market*), *App Store* [69] and *Ovi Store* [70], among others. For the first referred platform, *Stabilix PHR* [71] can be used to keep track of a personal health record, *Fast Food Calorie Counter* [72] allows users to keep track what should be eaten and *CardioTrainer* [73] uses the GPS to track the meters walked by the user and measure the calories burned. For *iOS, Capzule PHR* [74] works as a personal health record for all the family, along with *Health n Family* [75] for Symbian. However none of these applications offer suggestions for diet or exercise plans. On the other hand, SapoFit [76] is a *Google Android OS* application that intends to be a more complete solution for obesity prevention and treatment. Through the use of web services allows to the system to be used anytime and anywhere, at the same time that suggestions pulled back to the user are constantly improving over time. For integration and test of the cooperation mechanisms, this application was used, however more details will be properly approached in Chapter 5.

2.3. Cooperation Mechanisms

Cooperative mechanisms have proven to be a promising solution for several network constraints in wireless networks due to the overall characteristics of m-health architectures. This section will focus on wireless and mobile ad-hoc networks (MANETs), and will be referred the cooperation challenges, its advantages, some possible scenarios, along with important and relevant approaches and proposals presented in the literature.

2.3.1. Challenges in cooperative systems design

As referred in [16], there are many challenges to cooperation design in mobile environment due do the lack of standards and real static environments that ensure that all devices have similar specifications, as well as the fact that is not possible to guarantee the network homogeneity and guarantee its quality and stability. There are many constraints such as the mobiles devices resources, such as processor power, storage capacity, battery life, network connections with limited bandwidth and/or with high latency, which makes the cooperation mechanisms implementation in mobile environment a difficult task. Although those potential issues were enumerated in [16], [23], [77], they are still present in most cooperative systems and could be summarized as follows:

- **Low bandwidth and high latency issues**. Cooperation mechanisms could cause communication network issues jeopardizing network efficiency and effectiveness;

- **Synchronization and Security**. Cooperation systems require extra security and synchronization, which can be a difficult task.

- **Complex Schedulers**. Systems using multiple nodes relaying information between each other requires more sophisticated schedulers;

- **Node and route choice**. In cooperation systems is required to determinate the best node to cooperate to achieve a optimum relaying, which can be hard due to selfish and uncooperative nodes;

- **Mobile devices resources.** Low processor power, short amount of Random Access Memory (RAM), short battery life, and devices storage can comprehend limitations to mobile cooperation;

- **Node heterogeneity.** In systems where nodes have different hardware and/or software specifications, it is necessary to adapt and normalize node communication in order to achieve an optimal cooperation;

- **Fault-tolerance disconnection.** When a communication fault occurs in a relaying situation, it is necessary to identify the fault, recover the original message, and retransmit from the original node to the destiny node, which could not be possible in a mobile scenario, being required to decide a new route for the request.

It is necessary to give the necessary attention to all these parameters, in order to create cooperative systems that provide an optimal quality of service (QoS) and Quality of Experience (QoE), with potential performance gains or without compromising or deteriorating the network.

2.3.2. Cooperation benefits

A well-built cooperation system can produce many benefits, when comparing to traditional systems. The advantages [23], [78], [79] of using cooperative nodes in a system can be summarized as follows:

- **Performance gains**. A well constructed cooperation system could increase the network performance, due to higher achievable data rates and fewer retransmissions, increasing the network throughput;

- **Balanced QoS**. In cooperation systems that allow nodes without data connections access Internet services, other nodes relay packets in order to provide it. In the other hand those nodes had to sacrifice its resources (e.g., battery life) in order to relay that information;

- **Infrastructure-less deployment and reduced costs.** Relay node utilization decreases network infrastructure dependency, decreasing costs and allowing a cooperation system to be quickly build;

- In WLAN and cellular networks a suitable frequency management can **reduce interference** throughput.

Despite the existing challenges and difficulties in cooperative systems design, there are evident advantages, which should be properly approached.

2.3.3. Cooperative incentive methods

Cooperative incentive methods can be categorized in two major groups: reputation-based and pricing-based mechanisms [80]. In the former group, misbehaving nodes are isolated from other nodes and are usually deprived from receiving any services from them, punished with temporary or permanent sanctions. On the other hand, in the latter approach, cooperation is remunerated with virtual currency.

2.3.3.1 Reputation-based Systems

Node misbehaviour and selfishness is a matter has been discussed over many years. In [81] is emphasized that countermeasures for both are mandatory. Reputation mechanisms are applied to address node selfishness. They generally rely on neighbour monitoring to access its trustiness [82]. In order to decrease selfishness and stimulate cooperation, over the years many reputation systems have been proposed, which includes CONFIDANT, CORE and OCEAN [83-86] schemes. The CONFIDANT scheme compels nodes to cooperate, by detecting and isolating non-cooperative nodes. Each node has four main components: a monitor to locally detect any diverging monitor; a trust manager to take decisions about route information; a reputation system that is fundamentally the node reputation rating; and a path manager that defines the optimal path to avoid malicious nodes. In a CORE scheme nodes with good reputation can use network services while non-cooperative nodes with bad behaviour and therefore does not have access to network services. It has three types of reputation: subjective, calculated based on direct observation; indirect reputation calculated according to information provided by other nodes; functional reputation that is calculated through a given function. OCEAN also uses a monitoring and reputation system, dividing routing misbehaviour into misleading and selfish groups. If a node takes part in route finding but does not forward a packet is a misleading node, but if doesn't take part on route finding is a selfish node. When the node rating is lower than the pre-determined threshold is added to an avoid list and classified as problematic. It is given to the node a period time to cooperate and return to the network. While these three schemes above referred are the most common reputation-based schemes, most authors in the literature present proposals with combined and/or adapted characteristics of these schemes.

Anantvalee and Wu proposed in [87] a reputation based system for encouraging the cooperation of nodes on Mobile Ad Hoc Networks, under the principle that in a MANET, node cooperation in packet forwarding is required in order to avoid the network performance degradation. Unlike the model proposed in [5], to solve the selfishness problem where nodes choose to not forward packets to save their own resources, the authors proposes a selfish node detection system where nodes are presented with the benefits of being cooperative, and that being selfish does don't bring benefits to himself. It is also introduced the concept of suspicious node, as a partially cooperative node. The main purpose of the proposed system is to detect and punish selfish nodes through a Reputation Management System (RMS) as an extension of the Source Routing Protocol (SRP) [88], where each node monitors neighbours behaviours and assigns reputations values.

In [89] and [90] is proposed a routing protocol based on mobile agents where the best possible route between nodes is identified through selfish node isolation. Like the model proposed in [87], each node have a monitoring module of their behaviour in order to calculate its reputation.

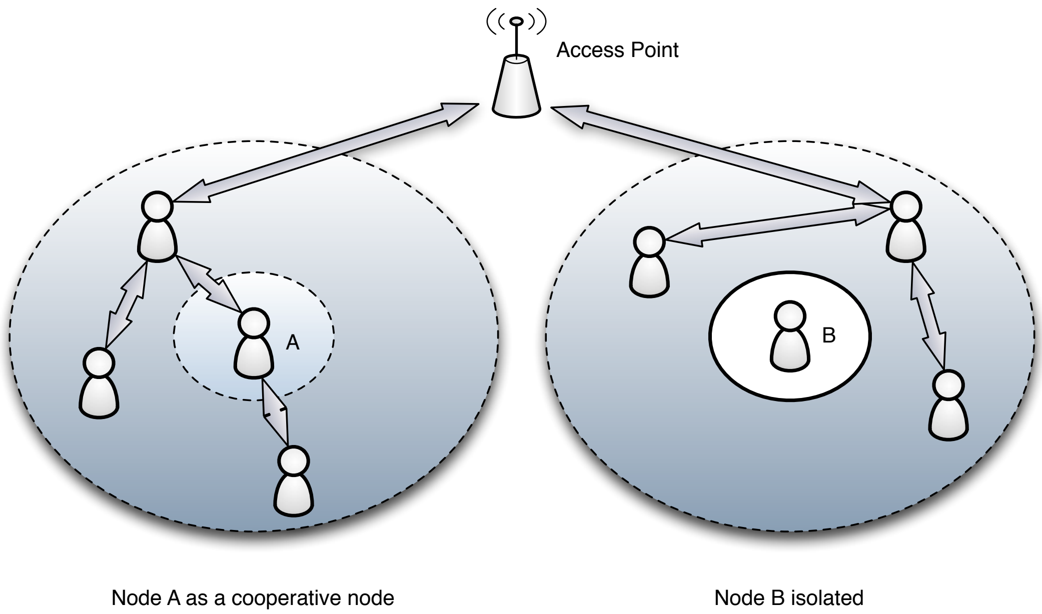


Figure 4. Node isolation scenario.

The calculation of the reputation value (RV) is made obtaining the number of packets forwarded along with the total of packets forwarded in the neighbourhood. When RV is lower than a pre-established value, nodes are isolated and deprived from network services, as it is possible to be seen in the Figure 4. Due to the mobile agents capacity of preserving bandwidth and its low latency [91], they are used to take part on the choice of the best route. They gather information about all neighbours including their reputation states, in order to establish reliable routers, finding optimal paths. There are other similar approaches such as [92] where once more is explored the dynamic source routing (DSR) protocol along with node behaviour monitoring and records [93] to calculate and address a reputation state. Many others reputation-based systems exists in the literature [94] [95].

2.3.3.2 Pricing-based incentives

As an alternative for reputation based systems, there are many other approaches using pricing based mechanisms. An example is the two-user cooperation strategy model proposed in [96], where a pricing policy serves as an incentive to encourage the user to cooperate to allow and guarantee the other user to benefit from cooperative help in order to minimize message delay. In this model every time a node choose to cooperate, receives currency that is paid from the user who asks for cooperation.

A dynamic pricing approach is presented in [97], where it is proposed a routing scheme where users (i.e., mobile nodes) have two options: a route with least virtual cost which does not guarantee the quality of service; or a route with QoS which demands an higher cost. In this model, the more options (i.e., routes) there are, lower will be the price to pay. Naturally, a more cooperative node will have more power of route choice. There are other similar approaches [98], [99] that proposes economical mechanisms to dynamically manage the cost and routes, showing that this technique increases network performance and in many cases can also decrease the node energy consumption.

Huang et al [100] proposes pricing strategies for resource allocation by taking account of factors like multiple transmission rates and nodes energy consumption in multi-hop MANETs. The objective of the proposed model is to achieve optimal wireless channels utilization by taking into account the interference and energy consumption of each node. Results shows that the proposed model can achieve optimal resource utilization and quick convergence under a multi-rate environment.

2.3.4. Cooperation-based approaches

In this section are presented cooperation-based approaches and mechanisms regardless their incentive methods. In [101] is investigated the use of cooperation between consumers and providers as an effective means to improve the consumer experience, the QoS of a system where mobile devices such as Personal Digital Assistants (PDAs) and mobile phones, regularly request services from the Web.

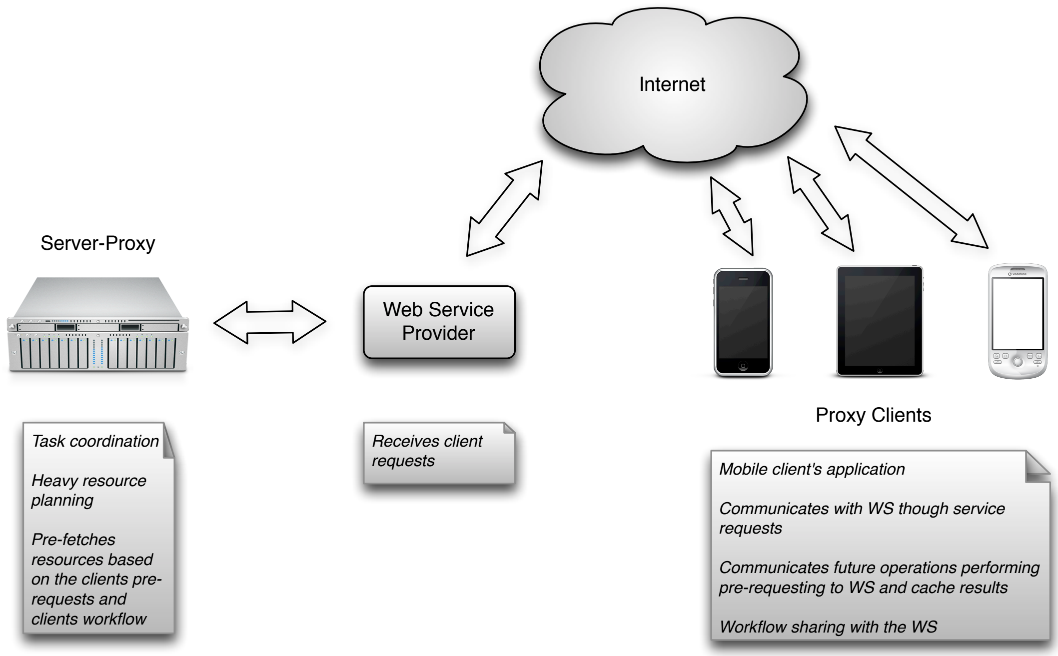


Figure 5. The cooperative approach through client and server proxies.

In order to allow a regular flow work, maintaining low latency values, it is proposed a cooperation model where two proxies are used: one in the server side the other one in the client side, as a software module in the user mobile device. The workflow is illustrated at Figure 5. The system is based on task prediction, to allow the server proxy to pre-fetch and pre-process necessary resources. To make this possible, the client side should make pre-requests to the Web Service (WS) communicating the intention for a specific future operation. The study concludes that cooperation through task prediction improves system performance and also provides the client side with choices and decisions rather than just provide stored information retrieval.

As previously referred, although WLAN have been widely used in cooperative systems, the energy required for WiFi communications in mobile devices can be a problem. In hand-held devices in idle mode, its energy consumption can achieve more than 50 percent of total energy [102], as can been seen in Figure 6.

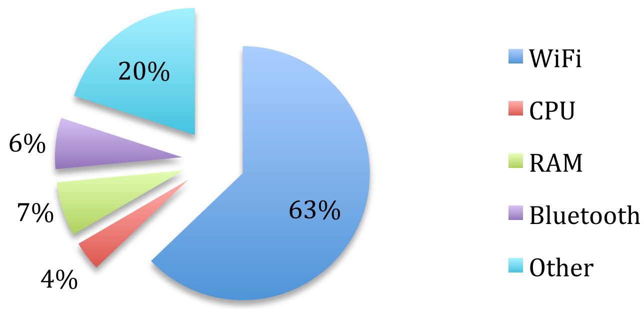


Figure 6. Consumed power for a connected mobile device in idle mode.

In an idle system, an active background data transfer rate consumes more than 60 percent of the total power, whereas Bluetooth consumes less than 10 percent energy when compared to WiFi consumption. This is explained due to the Bluetooth limited range, simpler radio architecture and lower rate transfer [103]. In [104] is explored the idea of using the high-power/high-bandwidth WLAN and low-power/low-bandwidth Bluetooth technology for multi-radio mobile networks, presenting a bandwidth-aware and energy-efficient cooperative networking clustering protocol. Depending on bandwidth requirements and on node activity, the protocol dynamically configures clusters, arranging nodes in a Bluetooth PAN with a common goal (i.e., in the same activity), as presented on Figure 7. For each cluster is elected a cluster head, which acts as a gateway between the PAN and the WLAN Access Point (AP), enabling regular nodes to access the WLAN infrastructure, at the same time they save energy, once they don't need to enable WiFi in their devices.

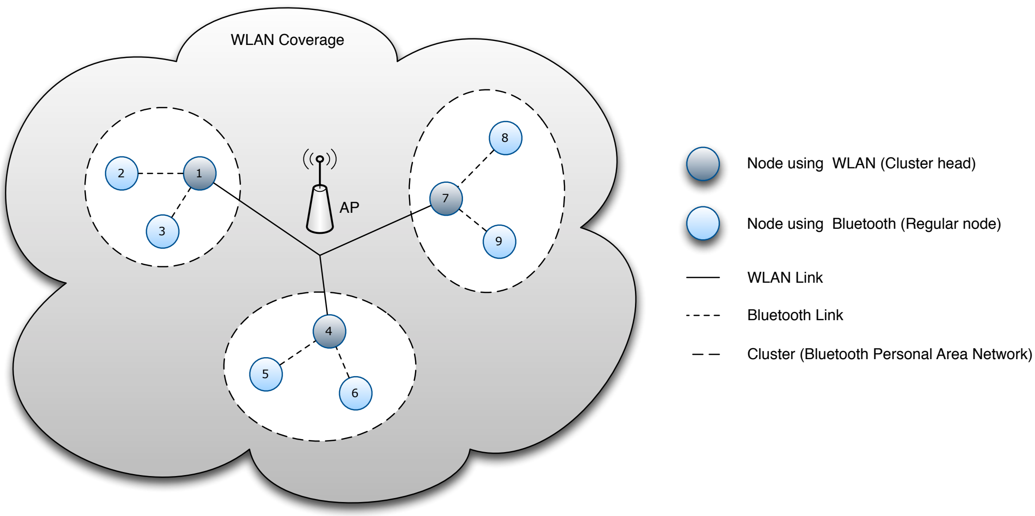


Figure 7. Nodes organized in clusters.

A similar group networking approach is presented in [105], where is proposed an optimal resource allocation solution for scalable video distribution over cooperative multihop networks to minimize the total energy consumption, in a real-time video broadcast scenario where multiple users are interested in the same content. The proposed system model consists in a base station capable of transmitting and relaying the video bit stream for mobile devices. The study shows that through the identification of optimized energy-efficient communication flows by using two low complexity approximation algorithms, it is possible to achieve great energy consumption gains. Similarly, a cooperative wireless network architecture with mobile devices that actively use two different wireless interfaces is presented in [25] in order to cooperatively distribute common content in the vicinity to node groups next to each other. A server holds the content, which have a wired connection to the base station. Depending on their position MDs connect to the BS through long-range connection such as 3G, LTE or WiMAX. Cooperation takes place by dividing content into multiple parts and distributing them to the MDs, and then each one will retransmit its received parts do other MDs using SRs links, such as WiFi or Bluetooth. That way each node does not need to download a full part of the content, saving battery power.

In [106] is presented a cooperative strategy for wireless networks which also uses a main base station for coordination. Rather than mobile relay nodes (RLNs) its strategy consists in the use of static relay stations (RSs) in order to optimize the network performance. The Figure 8 presents the scenario.

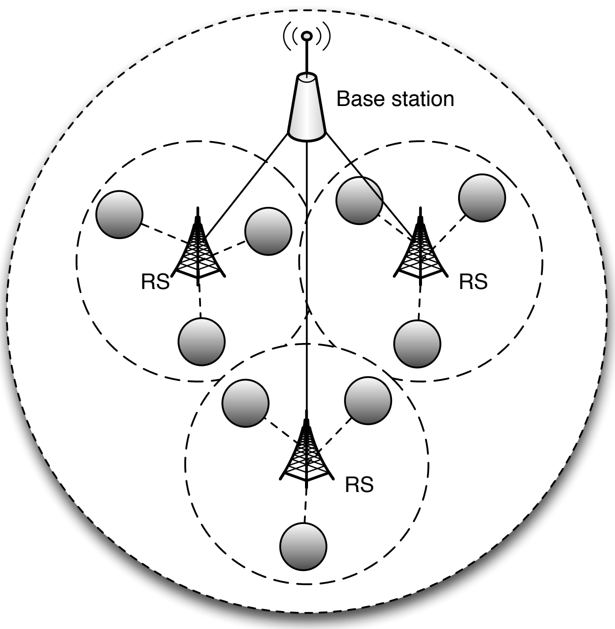


Figure 8. Cooperation through relay stations.

In the proposed model the main base station distributes the requested content to the multiple and organized RSs to form a virtual antenna array and cooperatively transmit to mobile devices.

2.3.4.1 Location-awareness

Location services for mobile devices were a much studied area in the last years. Network localization gives rise to a new paradigm in communications, enabling a variety of new applications, services and mechanisms that rely on position information of mobile nodes. The two main approaches [107] to obtain mobile devices localization is through cellular networks (GSM/CDMA) and through the Global Positioning System (GPS). The disadvantages of the latter are the outdoor limitations, the high energy consumption and the hardware cost factor.

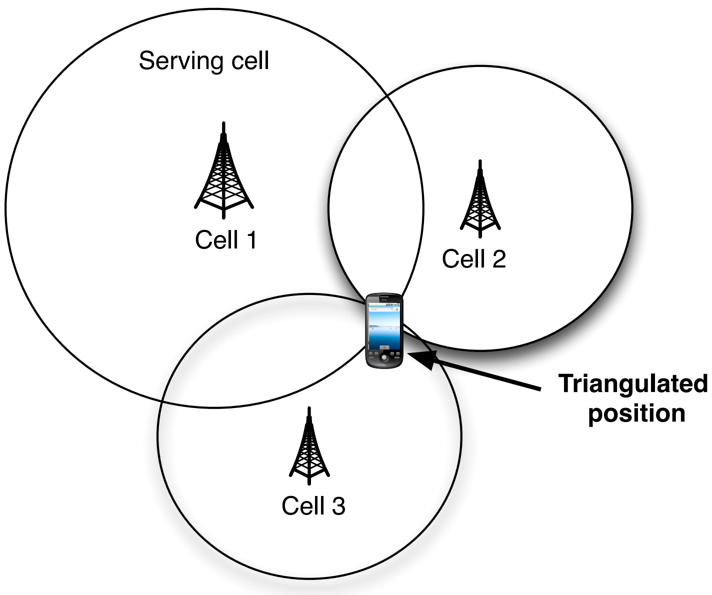


Figure 9. Triangulation scenario.

On the other hand a network oriented approach uses information obtained from the network [108], it has the advantage of working on most mobile devices using nearly no extra battery power, and it's not limited to the outdoor environment, although there are potential network coverage issues [109]. Most network-oriented approaches are using triangulation [110]. The problem with this approach is the cost factor for the end-user and the fact that is not accurate as GPS. Two location services that uses this technique and are widely used is *Google Latitude* [111], that performs triangulation through the three nearest cell towers, base transceiver stations (BTSs) in order to locate a user in real time, and the Find My Phone [112] tracking service from Apple. The triangulation scenario is presented at Figure 9. Both Google Latitude and Find My Phone from Apple can also track the user position scanning and using wireless networks in order the decrease the end cost to the user. The WLAN scanning technique to improve localization is adopted in many other services [113], [114].

A typical GSM BTS is usually subdivided in three sectors [115], 120 coverage degrees for each one, where, although it depends on the network carrier, is usually possible to retrieve the cell which identifies the sector within the cell area) where the mobile device is located. However, not its exact position, as may be seen on Figure 10.

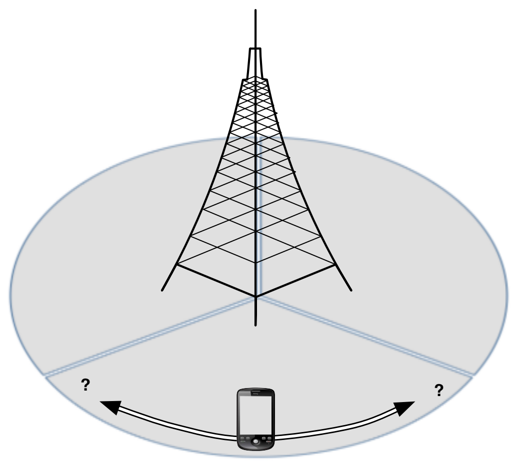


Figure 10. The trisector from the GSM architecture.

Due to GPS disadvantages, in [116] is presented an approach which is based on cooperation among mobile nodes to improve localization through the exploitment of the information retrieved from the cellular network.

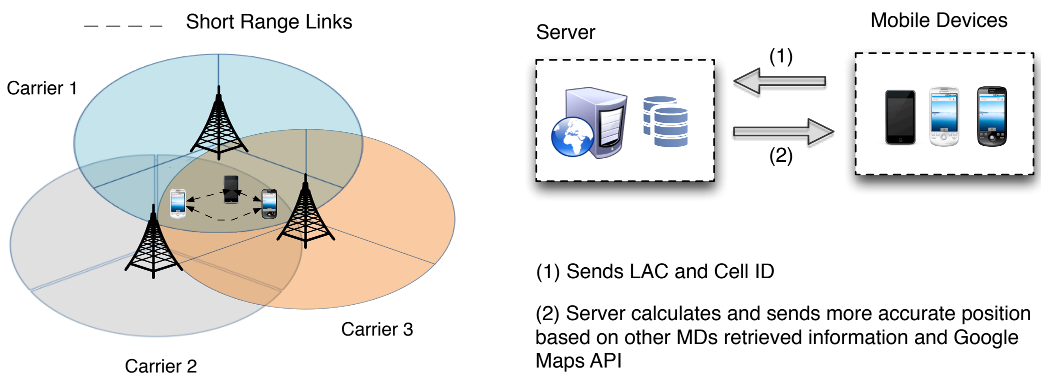


Figure 11. Localization improvement over cooperation.

In this proposal, first a cooperative node retrieves the location area code (LAC) and the cell ID from the network base station where it's connected. If there is any cooperative node within short links range (i.e., Bluetooth), it requests its cell and LAC information, and sends it to a server. The server compares the received information, and uses the *Google Maps* API [117] in order to calculate a more accurate position, retrieving back from the server geographical coordinates to the mobile device. A similar approach is presented in [118] to improve the accuracy of location information, where nodes share their position through wireless communications in order to disambiguate their positions in the network.

Location-aware cooperation plays an important role in other many situations [119]. With improved localization services medical staff could locate equipment in hospitals, workers can find merchandise in a warehouse, soldiers could easily determine each other's positions in harsh environments and fire fighters can track each other in smoke-filled buildings.

2.4. Summary

This chapter presented the literature review concerning mobile health, ubiquitous health and cooperation mechanisms. Thus, after a brief introduction, Section 2.1 presented the mobile health architecture along with some existing approaches, as well as its limitations, its challenges, and a review on electronic and personal health records. Section 2.2 approached the ubiquitous health regarding monitoring systems as well as mobile devices applications for common users. Last, Section 2.3 approached the cooperation mechanisms, its challenges and advantages, its incentive methods, and the existing approaches in the literature. The use of cooperation mechanisms is presented as a much possible solution to many constraints and limitations of mobile health architectures.

3. Requirements Analysis

Requirements analysis, also called requirements engineering, is an essential process in software development since it contains all specifications of the system. Its existence is mandatory in order to fully identify all system features and behaviours.

The Unified Modeling Language (UML) is the most used modelling specification, because it provides suitable standard methods to model not only application and data structures, but also its behaviour, architecture, and business process [120]. It is managed by the Object Management Group (OMG) and is an industry standard for graphical description. UML is neither a software methodology nor a programming language. It's a language with semantic notation that allows developers to view, specify, build and document the objects of a system. Through UML is possible to design models, which are representations in small scale of a particularly perspective. They can be applied to existing systems or systems to be created. A model consists in a set of diagrams with textual description that are consistent with each other.

The system features and behaviours will be addressed in this chapter in a quantifiable and detailed manner, along with UML diagrams in order to demonstrate behaviours, interactions and the system structure.

Section 3.1 will approach the system essentials requirements, Section 3.2 will address used technologies in this work and Sections 3.3 to 3.5 will present behavioural, interaction and structural diagrams. Last, Section 3.6 summarizes the chapter.

3.1. Essential requirements

Determining essential requirements is one the most important initial steps in requirements analysis. They can be features or constraints, allowing to have primary ground rules where is established the requirements that are mandatory to be present in the system. Defining essential requirements can be a difficult task, because it is necessary to have a global and complete vision of the vision in order to fully define these requirements. Thus, the following essential requirements were defined:

- Android API level should equal or above 10 (i.e., Google Android version equal or above 2.3.3), which represents 74.4% of the active Android devices across the globe [121];
- Bluetooth hardware should be present;
- Wi-Fi or Edge/3.5G/4G modules are required;
- Cooperation mechanisms should work ubiquitously in the system, and thus, completely invisible and transparent to the end user;
- Security mechanisms should be manually integrated if Bluetooth core version is below 4.0;
- A pervasive Web Service is required in order to provide reputation and access management;
- If a third party application for Bluetooth transmissions control exists (e.g., a Bluetooth firewall), it should be properly configured.

In order to create and integrate the mobile cooperation mechanisms, the above defined essential requirements are required.

3.2. Used Technologies

The mobile cooperation architecture aims the Google Android Operating System [65]. However, the cooperation mechanisms could also be applied to other mobile OSs, such as iOS [66] and Windows Phone [122]. Thus, in order to implement the referred mechanisms, the Android Software Development Kit (SDK) [123] was used. This SDK provides a set of tools and necessary APIs to the Android platform, and it uses the Java programming language. This platform and its architecture will be approached later in more detail.

The creation of the Cooperative Web Service (CWS) was accomplished through the Java Server Pages (JSP) technology [124], using the REST architecture. This choice was made due to the simplified, fast and dynamic possibilities to create Web Services that JSP provides. It was also used the Apache Tomcat Web Server [125] to serve the Web Service.

To hold the user cooperation information in the server-side, a MySQL database was required. For query processing it was used the MySQL Workbench tool [126]. However, it is important to refer that another Data Base Management System (DBMS), such as Microsoft SQL Server, could also be easily applied to the system. At client-side, the SQLite DBMS was used to temporarily hold the nodes reputation information.

For Java development in order to integrate the mechanisms in the m-health application (i.e., in SapoFit), the Eclipse Integration Development Environment (IDE) was used, combined with the Android Development Tools (ADT), an Eclipse Plugin, that extends the program capabilities, providing test emulators, direct deployment and useful debugging options. Last, for Web Service creation, the NetBeans IDE was used, combined with JSP and the referred Tomcat Web Server.

3.3. Behavioural Diagrams

Behavioural diagrams are used to show the functionality of the system, which includes use case and activity diagrams.

3.3.1. Use Case Diagrams

Use case diagrams provide an overview of the global functionalities existing in the system, displaying the actors and their associations with the use case. In a use case diagram actors are drawn as stick figures, and they can be a person, organization or external system that plays a role in the system. The user case diagram for the m-health application is presented at Figure 12.

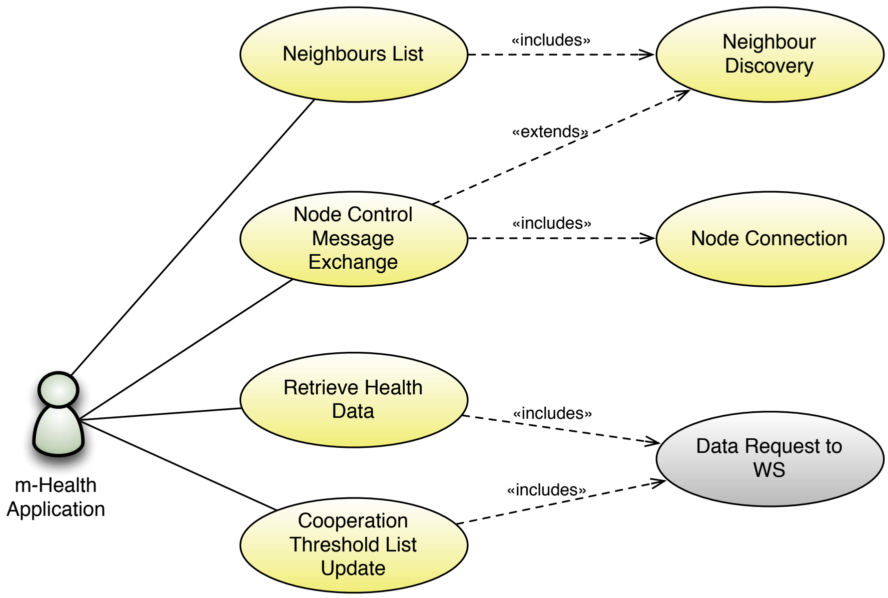


Figure 12. Application user case diagram.

The user case diagram for the Web Service is presented in the following Figure 13.

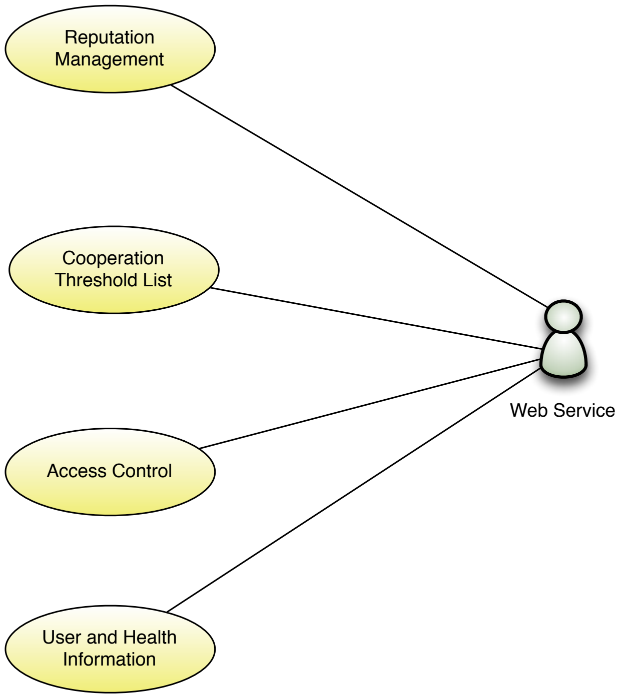


Figure 13. Web Service user case diagram.

3.3.2. Activity Diagrams

Activity Diagrams are widely used to provide a visualization of the system workflow. Two activity diagrams are defined regarding the request packet route path and the response path. In Figure 14 is presented the activity diagram that shows the cooperation workflow between mobile devices and the WS when a node makes a service request.

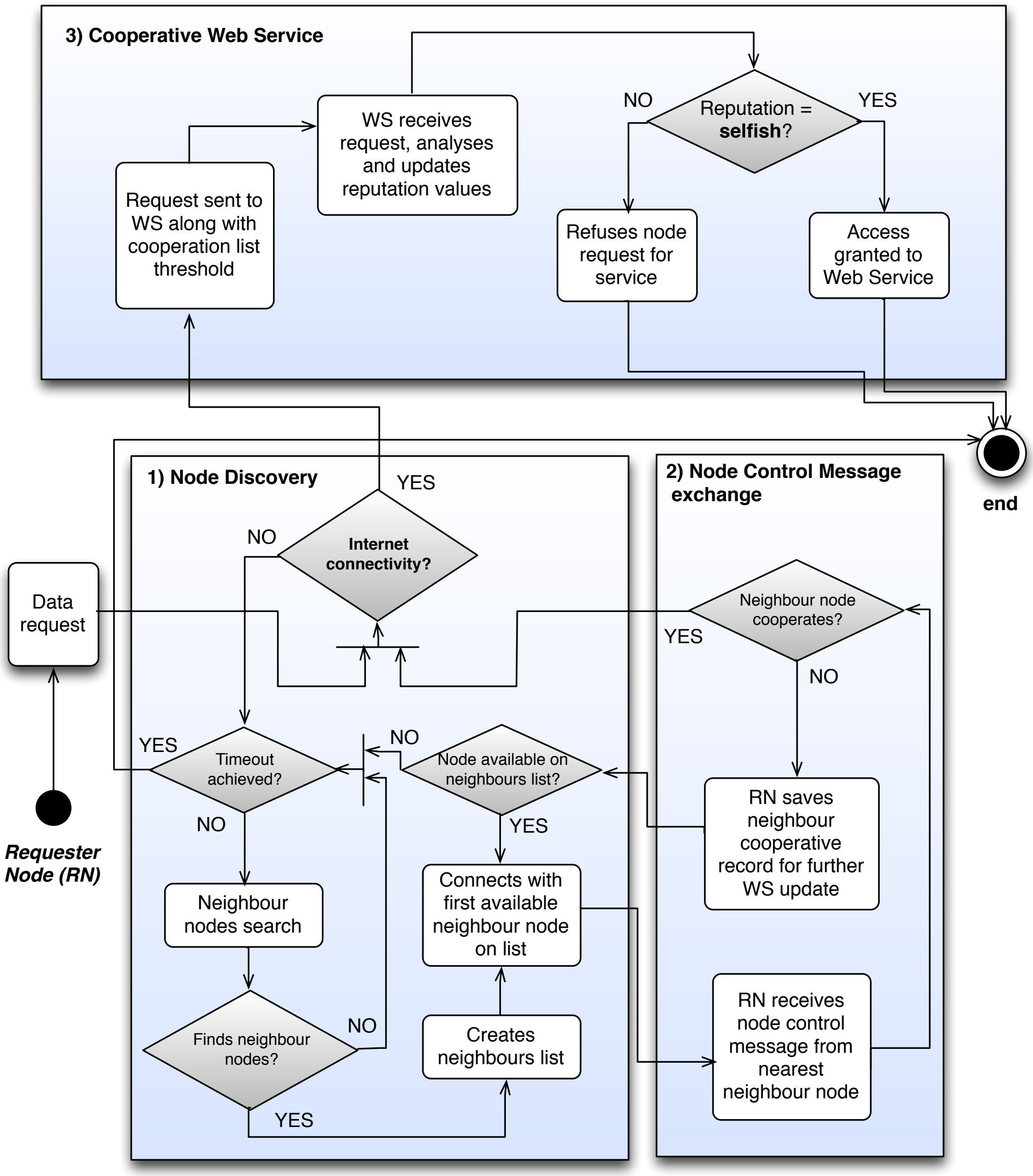


Figure 14. Request path activity diagram.

In the following Figure 15 is presented the activity diagram that regards the response path that originates from the Web Service, which could be the same route path as the request or an alternative path.

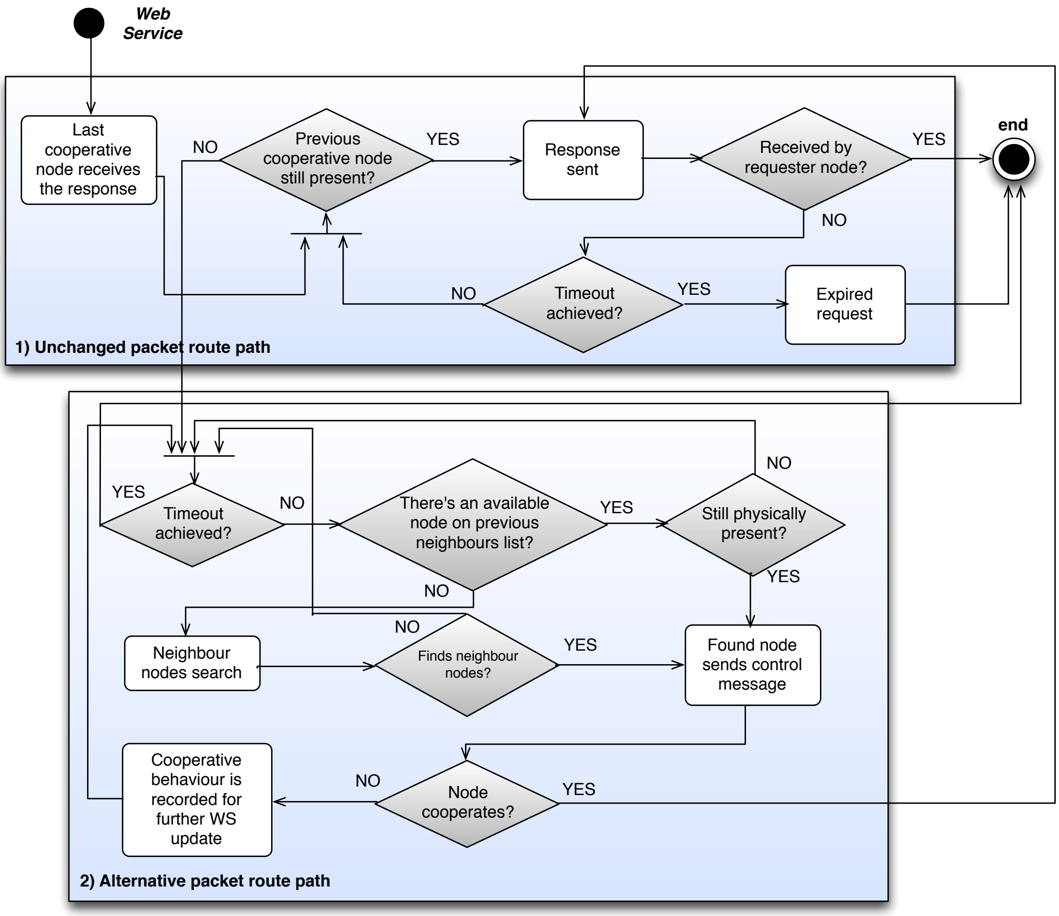


Figure 15. Response path route activity diagram.

3.4. Interaction Diagrams

As the name implies, interaction diagrams are used to describe some interactions among elements in the system. The sequence and collaboration diagrams are the two existing interaction diagrams. The former will be approached in the following Section 3.4.1.

3.4.1. Sequence Diagrams

Sequence diagrams are useful to model the logic flow within a system perspective. They focus on identifying the system behaviour. In this work, the system flow was divided in three relevant parts. The first is presented at Figure 16, presents the first cooperation phase, i.e., the node discovery process and the node connection flow regarding Bluetooth transmissions.

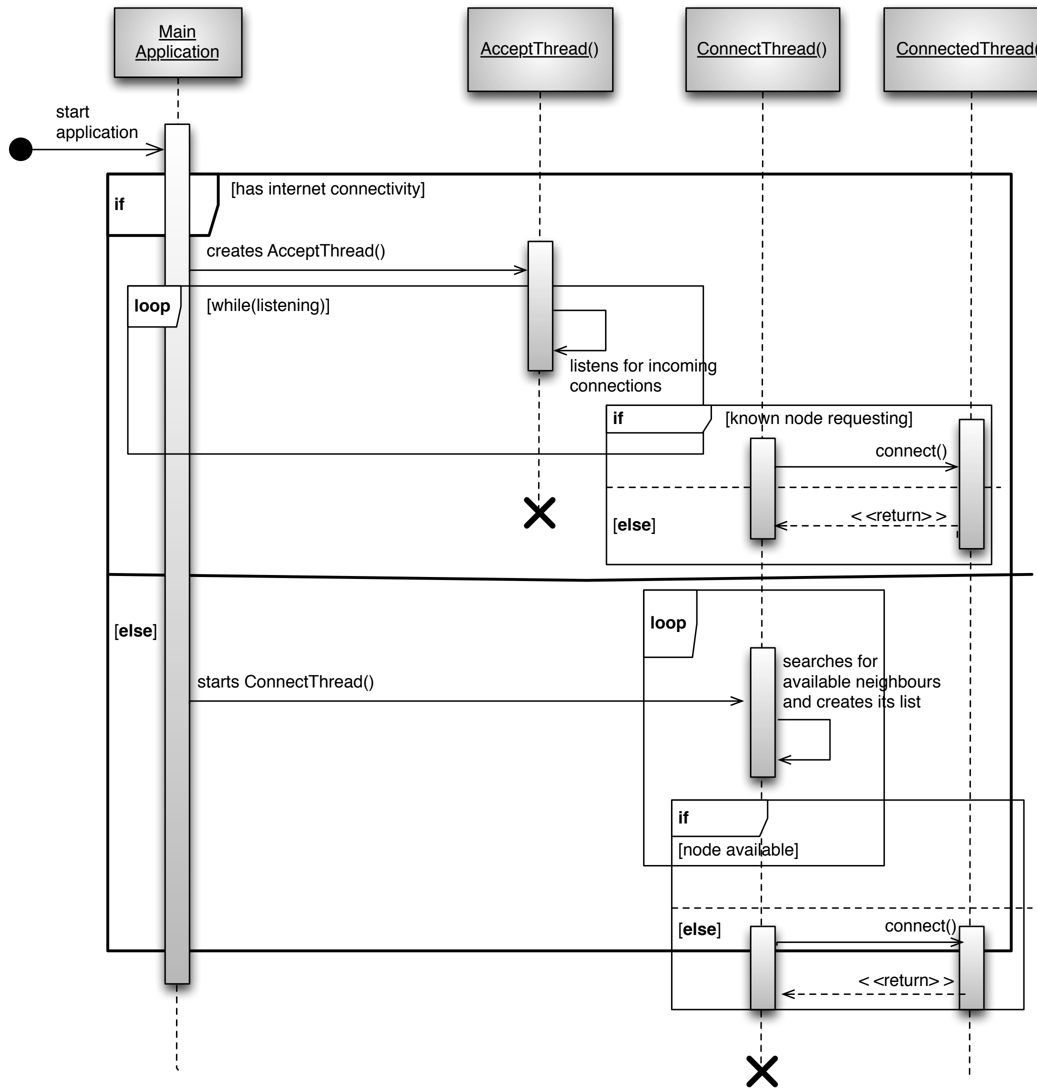


Figure 16. Node bluetooth discovery and connection processes.

The second phase, which is presented in the sequence diagram at Figure 17, it represents the sequence that occurs after the connection between a requester node (the node requesting for a service) and the requested relay node A (the first found relay node). It is also present a relay node B, which is the node found by relay node A. It demonstrates the transmission of the node and requester control messages.

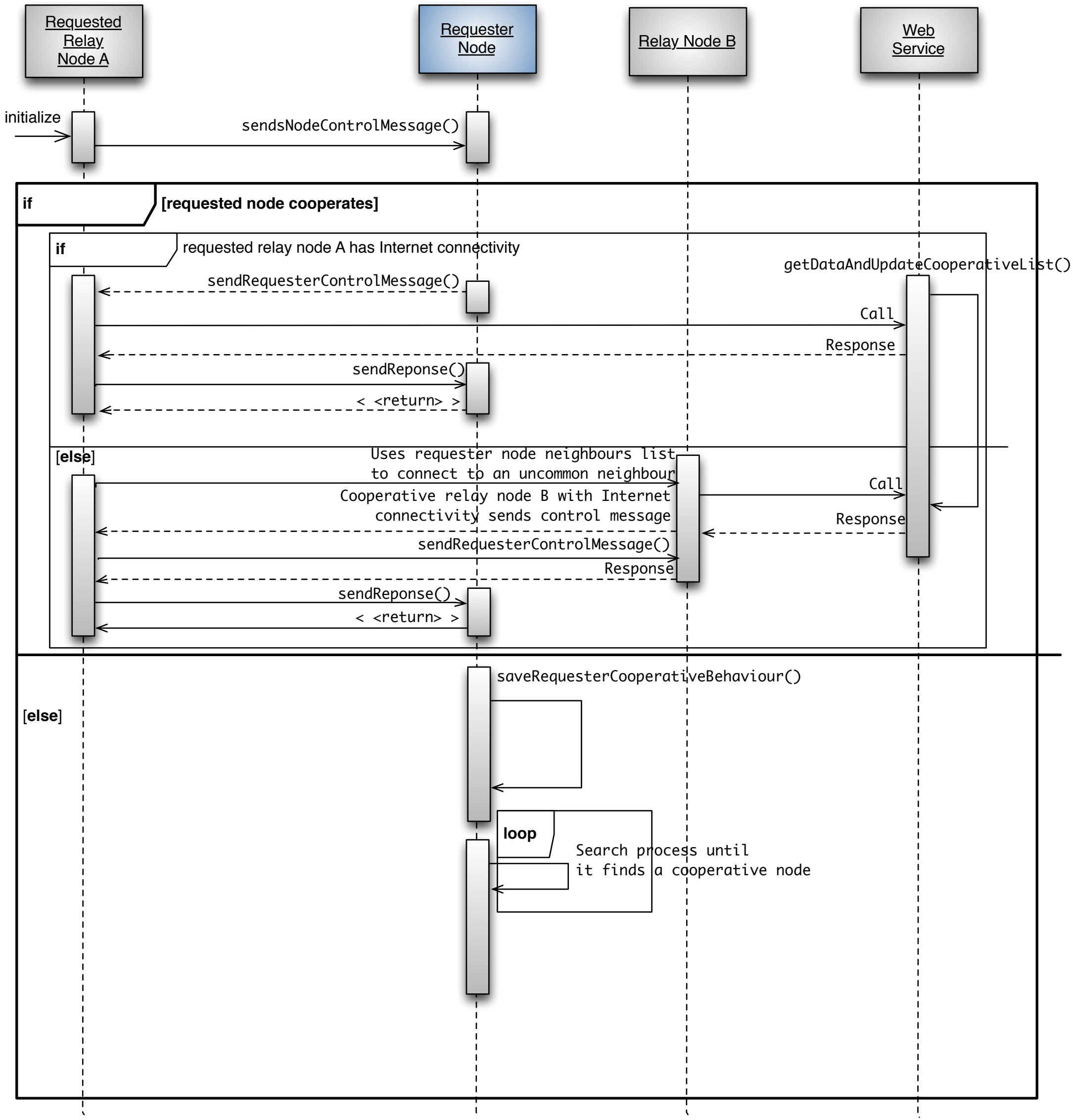


Figure 17. Exchange of the node control and request control messages.

The third and final phase of cooperation consists on the request handling by the Web Service and sending the response back to the requester node, which in this diagram, can be Node A or Node B. This diagram is presented below in the Figure 18.

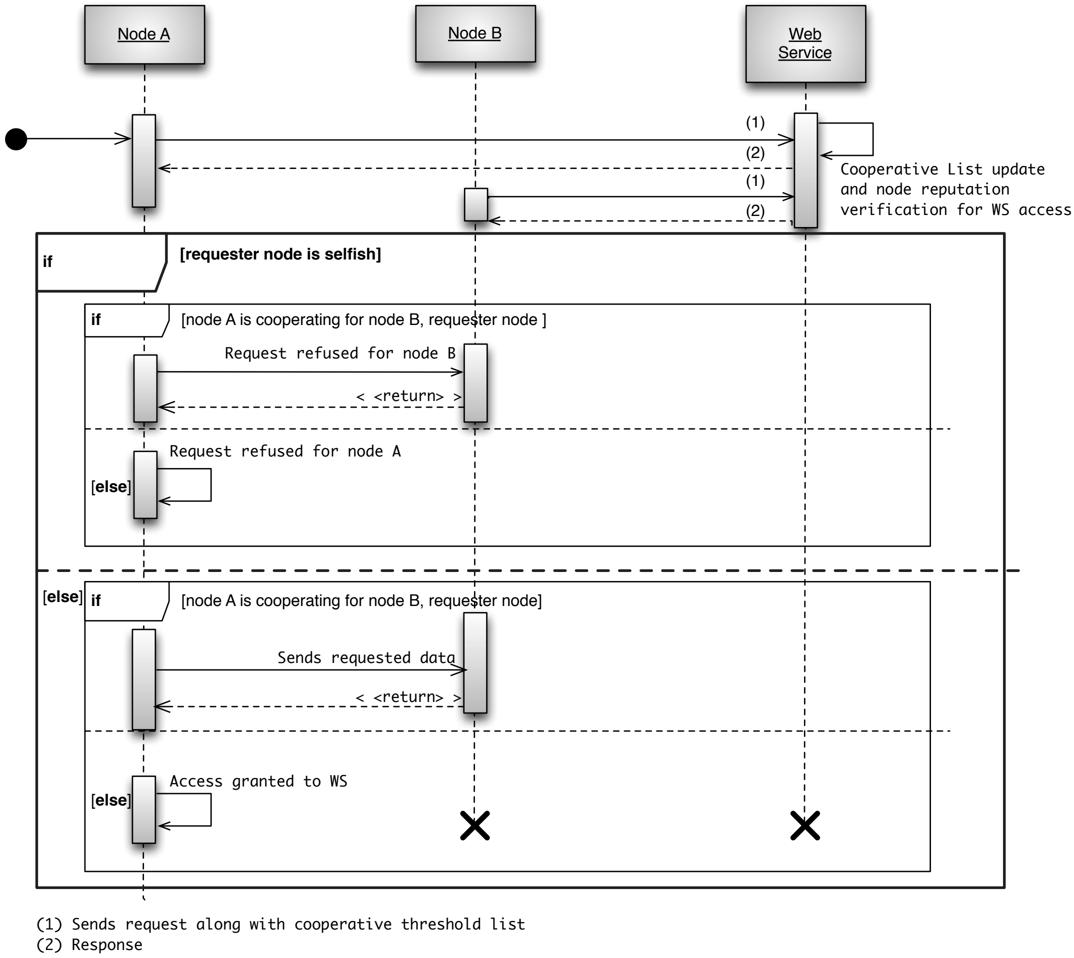


Figure 18. Web Service request management.

3.5. Structural Diagrams

Structural diagrams present the elements of a system regardless the time. One example of a structural diagram is the class diagram.

3.5.1. Class Diagrams

Class diagrams show statically the collection of model elements such as classes, their types, and their relationships. The class diagram that represents the static elements of the cooperation system is presented at Figure 19.

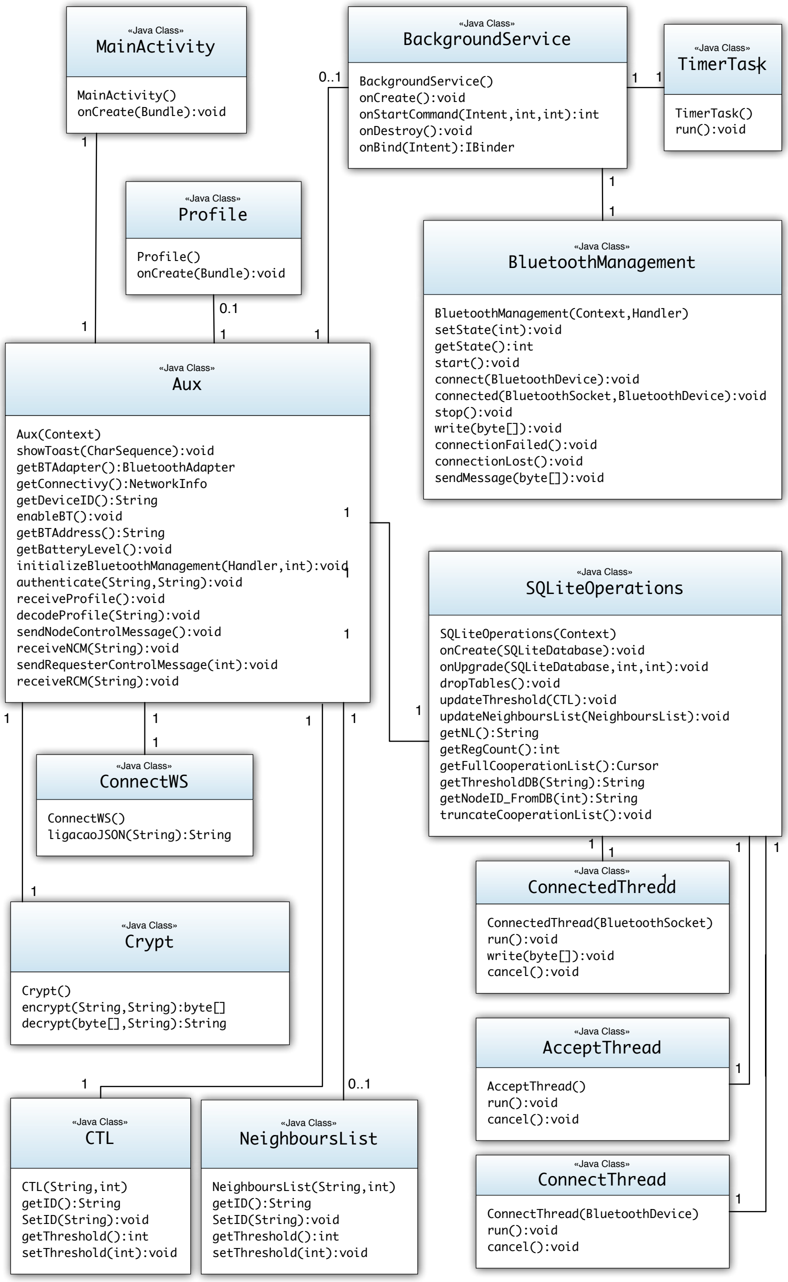


Figure 19. Class diagram of the application cooperation mechanisms.

3.6. Summary

In this chapter the requirements analysis was approached, in order to address all system behaviours and necessary features to the system. Thus, after a brief introduction, Section 3.1 presented the essentials system requirements, Section 3.2 shortly presented the used technologies in this work, and Section 3.3 to Section 3.5 approached and presented the behavioural, interaction and sequence diagrams, respectively, which included use case, activity, sequence and class diagrams.

4. Ubiquitous Cooperation Mechanisms

In this chapter will be introduced some details regarding the aimed Google Android platform in order to understand the system functionality, which is presented in Section 4.1. Taking into account that the created cooperation mechanisms are targeted specifically to this mobile operating system, it is necessary to be aware of its features as well as its limitations. Thus, Section 4.2 will focus the cooperation system architecture, regarding the integrated mobile mechanisms, along with the cooperative Web Service. Nevertheless, will be approached the created ubiquitous Android service, and the reputation-based strategy, which includes the node and requester control messages, the neighbours and reputation lists, in Sections 4.2.1 and 4.2.2, respectively.

4.1. Android Platform

In this section will be approached some details regarding the Google Android platform, that are important to understand due to the importance of the system intended ubiquity.

4.1.1. Android Architecture

Google Android can be defined as a software stack for mobile devices that includes an operating system, middleware and key applications [65]. Despite the fact that the Android SDK provides a set of official tools and APIs for application development, is it possible to use and create alternative tools and APIs in order to develop mechanisms and applications. This much possible due to the open-sourciness of the Google OS. The following Figure 20 shows the main system components of the Android OS.

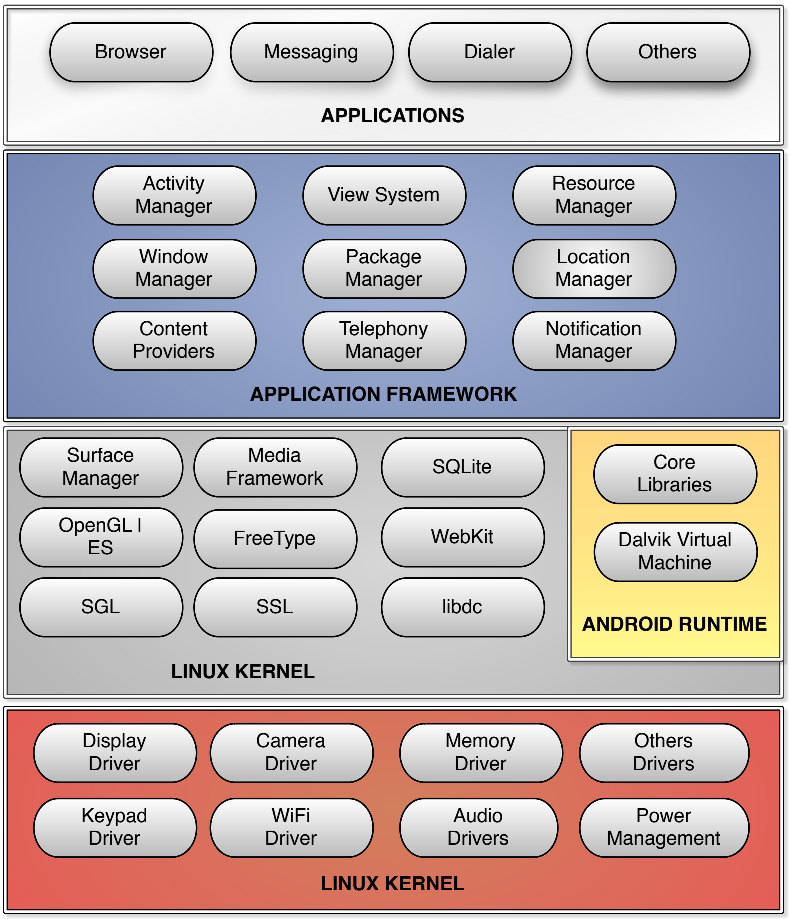


Figure 20. Android OS system architecture.

These main components could be summarized in the following manner:

- **Applications.** Android systems by default are provided with a set of core applications, which includes the email client, phone dialer, messaging app, calendar, maps, browser, among other applications;
- **Application Framework.** This framework provides the access to manage the device hardware, access to the location information, background services, notifications and other embebed android features;
- **Libraries and Android Runtime.** Android includes a set of libraries that are used by various components of the OS and are explored through the application framework, as well as the Android runtime, which comprises the core libraries and the Dalvik Virtual Machine, that relies on the Linux kernel for underlying functionality such as threading and low-level memory management;
- **Linux Kernel**. The kernel handles core system services such as memory and process management, and works as an abstract layer between the hardware and the software stack.

4.1.2. Activity Stack

Although a typical Android application runs through one activity, is possible to create an application that runs more activities at the same time, which are managed in the system as an activity stack. When a new activity is started, it is placed on the top of the stack and becomes the running activity, running in the foreground. Therefore, an Android activity has fundamentally four states:

1. **Active** or **running.** As referred, if the activity is in the top of stack, running in foreground.

2. **Paused**. If the activity has lost focus but is still visible (for example, if a message popup appears above the running application.
3. **Stopped**. In an activity is completely obfuscated by the system, it is stopped, retaining all information and stop being visible to the user. It could be restarted or destroyed, depending on the user requests and system needs.
4. **Destroyed**. If an activity is paused or stopped, the android system can drop the activity from memory. If the user requests the activity again, it has to be completely and manually restarted and restored to its previous state.

The possibility of an activity process to be easily terminated by the system or user represents a limitation to a cooperation process, because it could be unexpectedly or intentionally interrupted, originating problems in packet forwarding and node communication. In order to overcome this problem, a **foreground service** can be used, which will be detailed presented in Section 4.2.1.

4.2. System Architecture

In this section will be approached the cooperation architecture for service oriented m-health applications. Two main modules essentially compose it: the mobile cooperation mechanisms existing in the main application, and the Web Service for remote reputation management and access control, which may be seen in Figure 21. The main application is comprised by activities and the service. The former comprehends the original activities of the mobile application, where login, profiles and other original applicational components are presented. The latter possesses the mobile and ubiquitous cooperation mechanisms, namely the node control and requester control messages, as well as the neighbours and reputation lists. The cooperative web service comprises the remote methods called by remote devices, the final node reputation list and the access control module. The database at the server-side holds all user information, as well as reputation records and cooperative behaviours, while a temporary SQLite database at the client-side holds the temporary reputation information resulted from nodes behaviour.

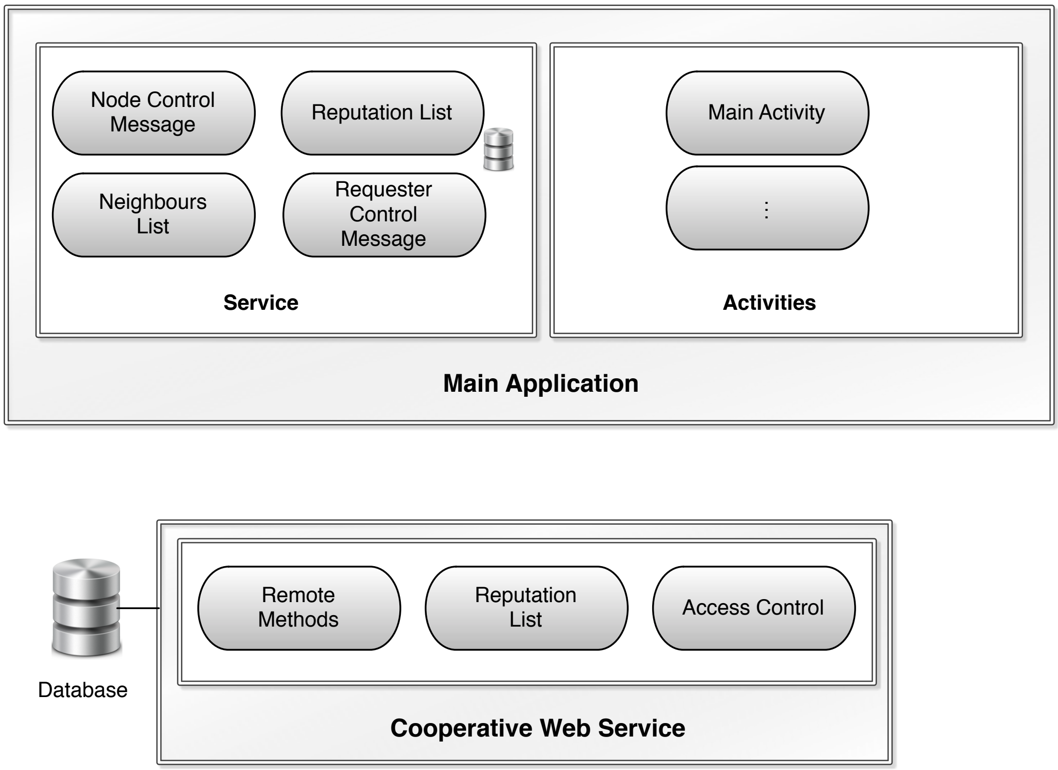


Figure 21. System architecture.

The following Section 4.2.1 presents the ubiquitous service where cooperation mechanisms are integrated, where its importance to the system ubiquity and usability are approached.

4.2.1. Ubiquitous Service

Nowadays, mobile applications and services are used in a daily life basis to support the need for information, communications or leisure. However, the user acceptance of a certain application, mechanism or system highly depends on the provided quality of experience and usability [127]. Thus, in this work a very important matter that is necessary to take into account is the ubiquity and pervasiveness of the cooperation system. The user experience of a cooperating device should not be jeopardized due to the cooperation process. Cooperation mechanisms were therefore integrated in an Android Service in order to allow the pervasiveness of the solution.

Although activities can be easily terminated by the mobile operating system or by the user itself (accidentally or purposely), and have to be manually restarted, cooperation mechanisms were integrated in an Android service, due to its capabilities to perform longer-running operations in background without interacting directly with the user. The lifecycle of an Android Service is shown on the Figure 22.

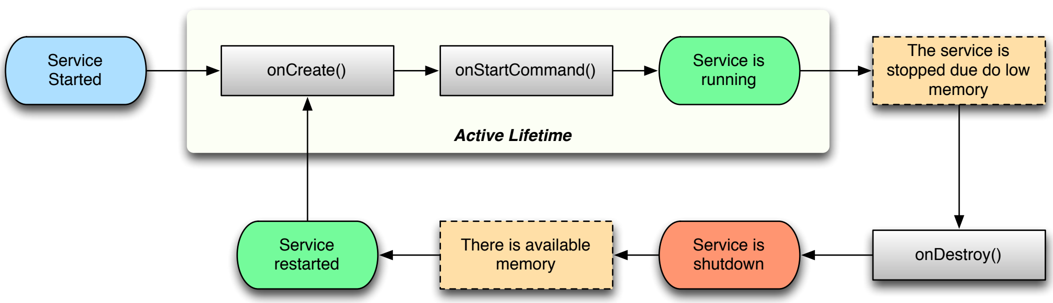


Figure 22. Android service lifecycle.

By default, services run in background processes, running transparently to the user, without notifying it of the execution, performing operations while there is enough memory RAM in the mobile device. However, a background service can be easily killed by the system, because it is assumed as having secondarily priority to the user. If this case, the service is stopped and destroyed, which can interrupt an on going cooperation process. However, unlike a common activity, an Android service is automatically restarted as soon as possible, returning to its original state as soon as possible. Another advantage of services is that they could run with different priorities than activities, which allow them to run for longer running times without being interrupted.

In order to assure that even a service is not killed by the system, a foreground service was used for cooperation mechanisms integration. Putting the service in a foreground state (i.e., similarly to running activities), the system considers the background service as an application that the user is actively aware of and thus is not a candidate for killing when low on memory. Still, has the advantage of automatically restart if for some motive the user stops the main application, as may be seen in Figure 23.

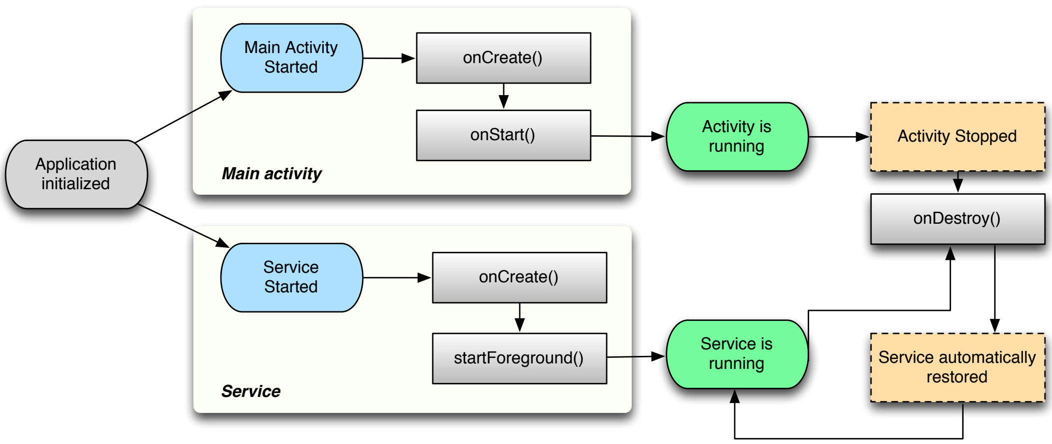


Figure 23. Main activity and service main states in a cooperative mobile health application.

In the above Figure, the main activity that provides to the user getting its health information, food plans and other functionalities, runs separately than the Android Service, where the cooperation mechanisms are present. This allows the user to freely stop and start the main m-health application, freeing memory on the device, without stopping the foreground service and therefore allowing the cooperation process. The objective is to allow nodes (i.e., mobile devices) to automatically and transparently cooperate, regardless the m-health application state.

4.2.2. Reputation-Based Strategy

The main objective of the created cooperation strategy is to provide an infrastructure independent alternative and **ensure global connectivity** to the Internet across specific m-health applications, at the same time it aims to optimize the overall network performance. Thus, in order to deal with the selfishness issue and ensure packet forwarding, three options were considered, while maintaining the system ubiquity:

1. Nodes could freely choose its cooperation state, without motivation to cooperate and forward packets and no punishment if they choose not to assist a node without network access.

2. Enforce cooperation (i.e., packet forwarding) at application level at all times, which means that all nodes are obligated to cooperate with other nodes, regardless of the available resources (e.g., battery power).

3. Applying an incentive method in order to give mobile nodes a motivation to cooperate, using a reputation-based system to punish selfish nodes, while taking into account nodes with critical resources.

Although the first two considered options are completely valid to specific scenarios, it is necessary to take into account that the created cooperation system aims mobile health systems, which in practice represents applications with critical purposes. While the first option cannot guarantee the packet forwarding to requester nodes, the second option can jeopardize an enforced cooperating node, due to the lack of resources. Thus, it was created a reputation-based system in order to overcome those two problems, which is essentially formed by Node Control Messages (NCMs), Requester Control Messages (RCMs) that includes Reputation Lists (RLs) and Neighbours Lists (NLs), and a Cooperative Web Service (CWS) to handle global cooperation and reputation management. In short, the created reputation system words under the following main specifications:

1. When the m-health application is firstly initiated, it is automatically established a predetermined and **unique identifier** which is assigned to the Bluetooth device name in order to allow requester nodes in discovery process to identify nodes with cooperation mechanisms.

2. A requester node that initiates a discovery process should connect to the **first relevant found node**, in order to optimize the discovery process.

3. When a requester node finds and connects to a neighbour node (through Bluetooth scanning), **receives a node control message** from it;

4. All nodes **should maintain a neighbours list** and if necessary, a **reputation list**, being responsible to calculate the **reputation value** (RV) based on the received information through the NCM. These lists **should be forwarded** through the relay nodes, within requester control messages.

5. When a requester node initiates a request to receive data through cooperation, it will wait for a response **until the timeout is achieved**. If the timeout is achieved and the response has not been received, the

request **expires** and initiates another request through another neighbour node;

6. Based on the received behaviour information by cooperative nodes, the **Web Service** verifies and updates the reputation states, managing the access control, refusing or providing access to the data.

These are the summarized pillars of the reputation-based cooperation system, and will be detailed approached in the following Sections, from Section 4.2.2.1 to 4.2.2.4. In Figure 24 is presented a possible cooperation scenario, involving two node groups using the same m-health Android application.

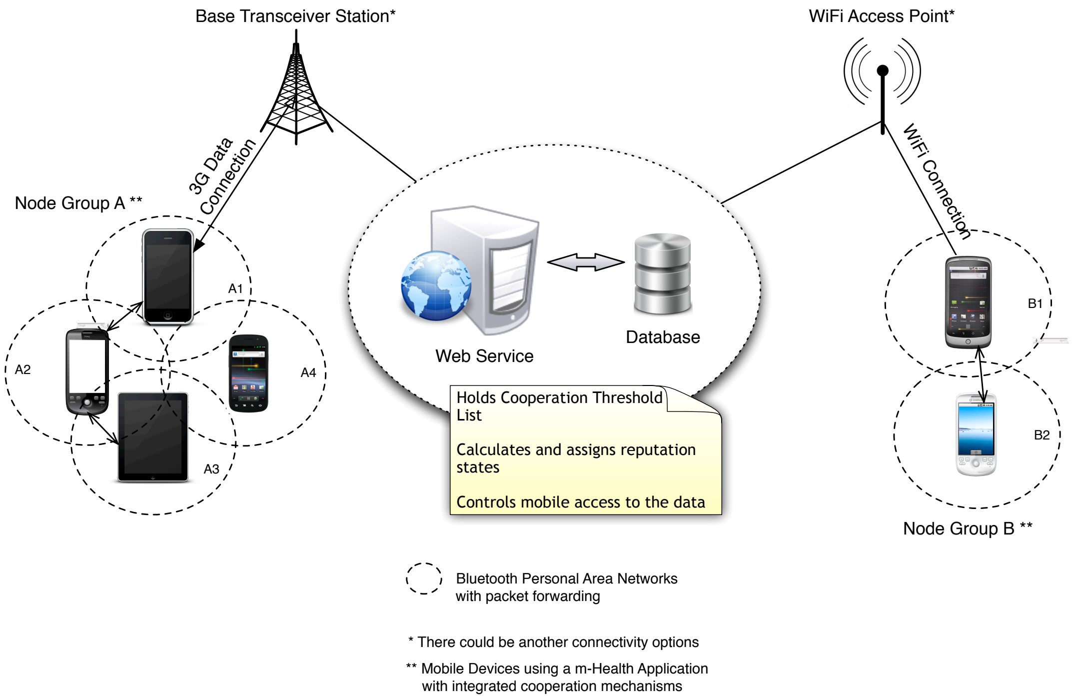


Figure 24. Cooperation scenario.

In the presented scenario there are a total of five nodes using the m-health application with integrated cooperation mechanisms, where only two (nodes A1 and B1) have Internet connectivity. Most mobile devices have Bluetooth class 2 modules, which means they can search for nodes within a ten meter range, approximatelly. In group B, node B1 and B2 are the only nodes available within their ranges, so node discovery, node choice and packet forwarding occurs directly. In the group A, node A3, which is defined as the requester node, will search and connect for the first available node it founds, which in the presented scenario, is the node A2. However, if A2 does not have Internet connectivity and node A1 is not achieveable by A3, it has to request to A2 to request to node A1 to retrieve data from the Web Service in behalf of A3. Considering a mobile scenario where nodes can change their positions in a few seconds, the response will preferably follow the same path, however, if that is not possible (for instance, node A2 could not be available anymore), node A1 will try to communicate with a node which is a neighbour both from A2 and A3, in order to increase the probability of the fourth node be also a neighbour from the requester node (i.e., from node A3), which in this case is the node A4. The necessary information to anticipate this situation is available on the neighbour list (NL), which was sent along with the request, as will be approached later.

4.2.2.1 Node Control Message (NCM)

Node Control Messages are sent from requested nodes to requester nodes and aim to provide an awareness of the node state, i.e., if the node is willing to cooperate and in what conditions. It contains the established node unique identifier, the battery state, the Internet connectivity status and the cooperation status. The NCM is presented at Figure 25, along with the size of each component.

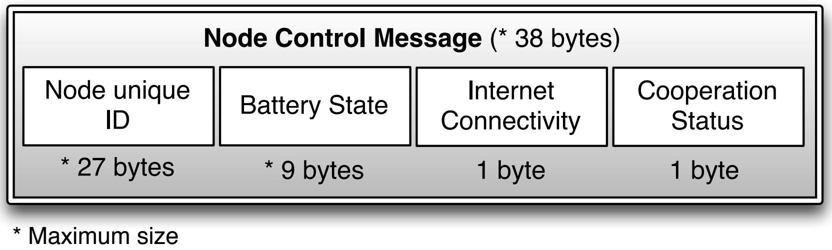


Figure 25. Node Control Message.

The node control message has a maximum size of 38 bytes, and the four components could be described in following manner:

1. **Node unique ID.** This identifier, which will be saved and stored on the first contact with the Web Service, it is arranged through an aggregation of the mobile device Bluetooth mac address and the user unique identifier.
2. **Battery State.** To every mobile node is assigned a battery classification based on its remaining power in percentage.
3. **Internet Connectivity.** In this element will be returned a 0 or 1, where the first means that the node has no Internet Connectivity and 1 stands for the opposite.
4. **Cooperation Status.** This module also returns a 0 or 1, where 0 stands for not cooperatively available, and 1 for cooperatively available. This status is achieved in the following manner: the application validates all necessary requirements at application level in order to forward packets (e.g., a third-party application that represents a Bluetooth firewall, can jeopardize the cooperation blocking Bluetooth communications). If all requirements for packet forwarding are met but the application still cannot forward packets or accept a connection from a requester node, it is assumed that the user is deliberately avoiding cooperation.

These four elements comprise the node control message, providing enough data to the requested node in order to calculate the reputation value (RV), as shown on Table 1. The *critical* status represents a battery power of less than 15%. In this case, the node becomes unavailable for cooperation. Thus, it is possible to avoid nodes with critical battery power being punished by not sacrificing its last battery resources. The *poor* status occurs when the battery power is between 15% and 35%. Between 35% and 70% is achieved the *regular* battery status and above the 70% the node is classified as having an *excellent* status. The reputation value is achieved through a correlation between the battery status, the Internet connectivity and the node cooperation state. In Table 1 is possible to verify that the worst punishment occurs when a node with *excellent* battery state has Internet connectivity but it is not willing to cooperate, and the better-rewarded node happens when the cooperation occurs from a node with *poor* battery state and Internet connectivity.

Table 1. Reputation Value calculation.

Battery State		Internet Connectivity	Cooperation State	Reputation Value (RV)
Classification	0%-100%			
Critical	<15%	-	-	-
Poor	>=15% and < 35%	0	0	-1
Poor		0	1	+3
Poor		1	0	-2
Poor		1	1	+4
Regular	>= 35% and < 70%	0	0	-2
Regular		0	1	+2
Regular		1	0	-3
Regular		1	1	+3
Excellent	>= 70%	0	0	-3
Excellent		0	1	+1
Excellent		1	0	-4
Excellent		1	1	+2

It is important to note that cooperative nodes without Internet connectivity could also increase its reputation, due to the eventuality of relaying packets in behalf of requester nodes. These intervals are assumed to avoid selfishness among nodes with good conditions to cooperate, while nodes with very low resources are not extremely punished if they do not cooperate.

4.2.2.2 Neighbours List (NL)

When a node makes a request to another node, which does not have Internet connectivity, it is suitable that the intermediary node does not relay information (i.e., the requester control message as will be approached in Section 4.3.2.4), connect to a common neighbour of both, in order to provide a better node discovery scope. Also, in cases involving more than two nodes and at least one intermediary is necessary, it is possible that the response has to follow an alternative path due to the unavailability of nodes that provided the original request path. During the request, in order to the required provide information about the actual neighbours nodes, and in the response in order to assure the best possible return path, it is necessary to maintain a list of neighbours, which is presented in Figure 26.

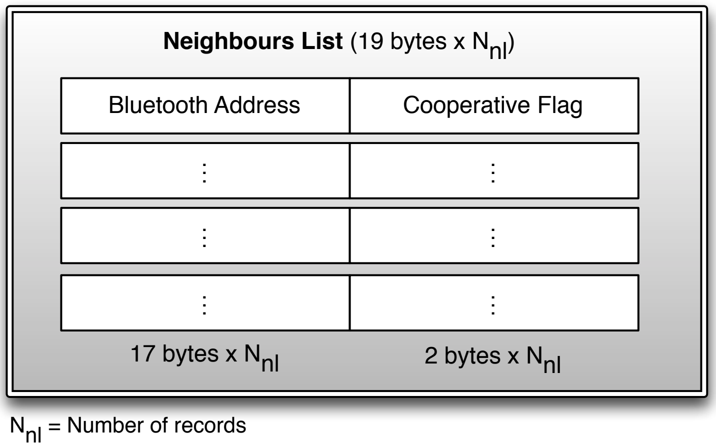


Figure 26. Neighbours List.

For example, in a situation involving five nodes, N_1, N_2, N_3, N_4 and N_5, where although N_1 has three neighbours in the vicinity, N_2, N_4 and

N_5, it finds first N_2. If N_2 finds first N_3 in the discovery process, make a request for data retrieval in behalf of the requester node. Thus, in this case the other remaining two nodes are not necessary to intervene in the cooperation process (i.e., in packet forwarding) in a first phase, as presented in Figure 27. In the presented scenario, before connecting to N_2, N_1 retrieves all the remaining node IDs and Bluetooth addresses from its neighbours, aggregating the information on a neighbours list. This list is then sent along with the service request to N_2 in the requester control message. N_2 will then compare the received neighbours list in order to search for neighbours that are not known for N_1.

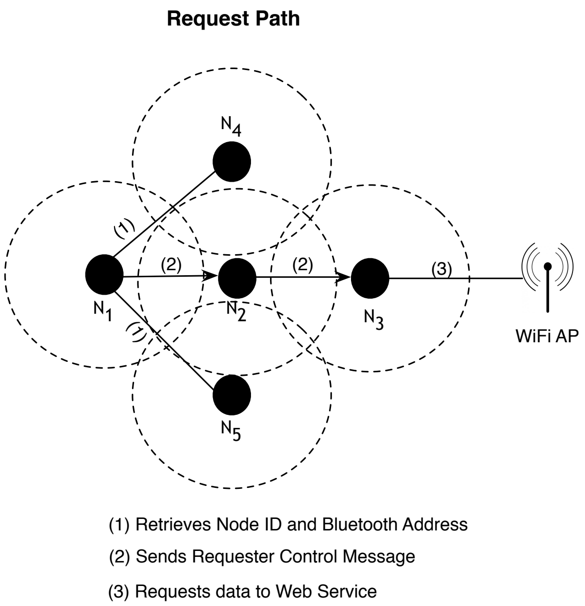


Figure 27. Request path.

If node N_2, the intermediary relay node, is not available for the response, N_3 has to resort to N_4 or N_5, both common neighbours, in order to forward packets to N_1. It will then use the received information regarding the neighbours list and compare it with the available nodes within its range. If it finds a common neighbour, it will request packet forwarding to the requester node, ignoring the presence of the remaining nodes, as illustrated in Figure 28.

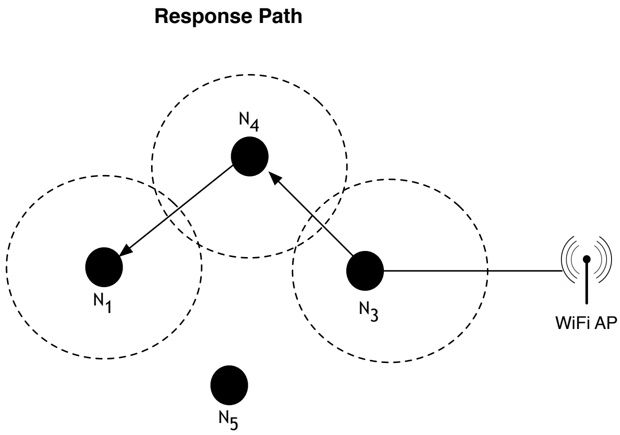


Figure 28. Response path.

Although mobile nodes have to perform a discovery process in order to verify if nodes remain within the Bluetooth range, the objective of this solution is to avoid direct connections to absent nodes. This results in failed connections and therefore in time losses far worse when comparing with the required time of discovery processes, as will be later demonstrated. More important, a neighbours list allows nodes in the response to avoid the uncooperative nodes found in the request path. This specific situation will be approached in Section 5.2, where the experimented cooperation scenario is addressed.

A neighbour list has a size of 19 bytes for each record, i.e., for each neighbour.

4.2.2.3 Reputation List (RL) and Cooperative Web Service (CWS)

Although the node reputation value is locally and temporary stored, it is exchanged by mobile nodes and aggregated with previously existing reputation lists until a cooperative node with Internet connectivity is found, in order to update the final reputation list in the WS. When this occurs, the result of the aggregation of all RLs is sent and updated in the

Web Service when a node with cooperative node with Internet connectivity is found.

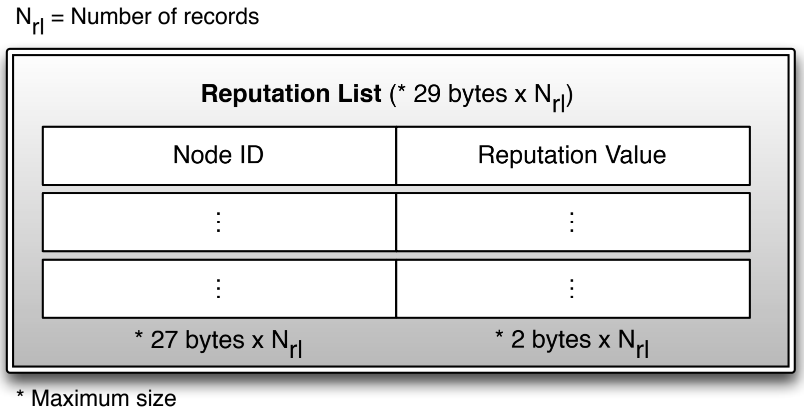


Figure 29. Reputation List.

A reputation list has a maximum size of 29 bytes for each record and its structure is presented at Figure 29. The RL is simply comprised by the node unique identifier and the reputation value (RV) value (calculated as presented in Table 1 of Section 4.2.2.1). The total number of records that exists on the server-side database is equal to the number of registered nodes in the m-health application, while in the client-side the number of records is changeable and varies through time, being emptied every time is forwarded to a relay node, but updated when its sent by a requester node. Each *node ID* is associated with the application user identifier, which means that when a user uses different mobile devices, it is maintained its reputation.

Based on node reputation, the CWS is responsible to decide if a requester node can or cannot access the remote data. Therefore, three reputation states are assumed: selfish, neutral and cooperative. The intervals that define the node reputation state are defined in Equation 4.1.

$$Rep(N)=\begin{cases} \text{Selfish}, & R_V \in\ ]-\infty, -1] \\ \text{Neutral}, & R_V \in 0 \\ \text{Cooperative}, & R_V \in [1, +\infty[\end{cases} \quad (4.1)$$

Nodes with zero reputation value are considered neutral. Neutral nodes have direct access to the Web Service, but they are not allowed to receive packets through cooperation until its RV is equal or greater than 1, achieving a convenient cooperative reputation state. Thus, nodes with negative reputation value are considered selfish, and their access to the WS is refused until they reach the cooperative state, except for packet forwarding requests, where selfish nodes can retrieve remote data for a cooperative requester node.

Communications with the Web Service, requests and responses, occurs using the JavaScript Object Notation (JSON), due to its language independence, its standard lightweight notation and its data structures and associative arrays that provides mechanisms to easily organize and pass information. At application level, all temporary and local cooperation reputation lists are logical stored on a SQLite database, which is emptied once the information is sent and updated in the WS.

Due to the packet forwarding implications, it is necessary to take into account security issues in related to data privacy, which is a major concern in health systems. Thus, it is necessary to protect the transported information in Bluetooth transmissions, in order to safeguard personal information concerning users health. Cryptographic mechanisms is seen as a solution in order to present security methods in packet forwarding [55]. Although the latest Bluetooth core 4.0 version was officially adopted in 2010 supports packet encryption, and it uses Advanced Encryption Standard (AES) and a 128-bit block cypher algorithm [128], there are few mobile devices that supports this version, where most mobile devices are actually using the core 2.1 version, which dates from 2007. Therefore, packet encryption was manually applied to the cooperation system to secure

Bluetooth communications, using AES algorithm in Cipher Feedback (CFB) mode with a key size of 128 bits [129].

4.2.2.4 Requester Control Message (RCM)

The requester control message is first sent by the initial requester node, and it comprises five main components: (1) the **requester ID**, (2) the **service request**, (3) the **neighbours list**, (4) the **reputation list** and (5) the **achieved cooperation time** (ACT). An illustration of the RCM is presented at Figure 30. Its size can greatly vary because it depends in the number of aggregated neighbours and reputation lists, as well as the size of the service response and the ACT.

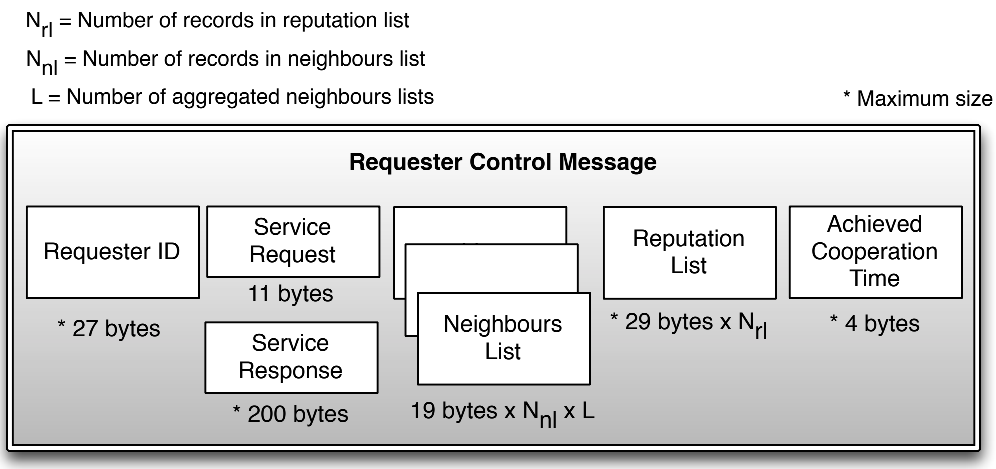


Figure 30. Requester Control Message.

The five main components of the requester control message can be described as follows:

1. **Requester ID**. As previously referred, the requester ID results from the aggregation of the mobile device Bluetooth mac address and the user unique identifier.

2. The **Service request** represents the information that exactly the requester node is requesting, namely the authentication or logout tokens, its health profile, or other remotely stored information.

3. The **Service Response** contains the specific requested data (e.g., the health profile) or the service denial.

4. **Neighbours List**. Although the first requester control message contains only one NL, depending on the number of used relay nodes, will result in the same number of neighbours lists.

5. **Reputation List**. The RL will contain all reputation values calculated in the cooperation process, and can be updated for any node, being the values updated depending on the relay nodes behaviour, until it reaches the WS, where the stored information is pervasively stored.

6. **Achieved cooperation time**. To prevent a request node to indefinitely wait for a request, it was defined a maximum *waiting period* (MWP). Therefore, when a node initiates a request and sends the requester control message, it will wait for the response until the MWP is lesser than 30 seconds. This value is defined in order to control the user QoE. If the response is not received then MWP is achieved, the requester node cancels its request and starts searching and requesting cooperation to a different initial node. The ACT provides to all nodes intervening in the cooperation process an awareness, of when they should stop cooperating and wasting resources finding a cooperative node with Internet connectivity. When the RCM is exchanged through nodes, the ACT should pass in order to provide an awareness of the achieved cooperation time.

The requester control message is exchanged between nodes using JSON (encrypted using AES algorithm) during requests and responses.

Although in this work the cooperation mechanisms aim a specific mobile Operating System, this independent notation provides a quicker expansion of these mechanisms to other mobile platforms.

4.3. Summary

In this chapter it was presented in Section 4.1 some important aspects regarding the Google Android platform, in order to understand the ubiquitous mechanisms. In Section 4.2 it was approached the cooperation system architecture, as well as the reputation-based cooperation strategy. Thus, the main objective of this chapter was to present the importance of the system ubiquity through the created cooperation mechanisms in order to achieve a global network connectivity while approaching selfishness issues and the choice of the request and response paths. This is achieved through the reputation-based strategy, which is fundamentally possible through the application foreground service comprised by four cooperation mechanisms: the node and requester control messages, the neighbours and reputation lists, along with the Web Service. An illustration of the message exchange sequence is presented in the Figure 31.

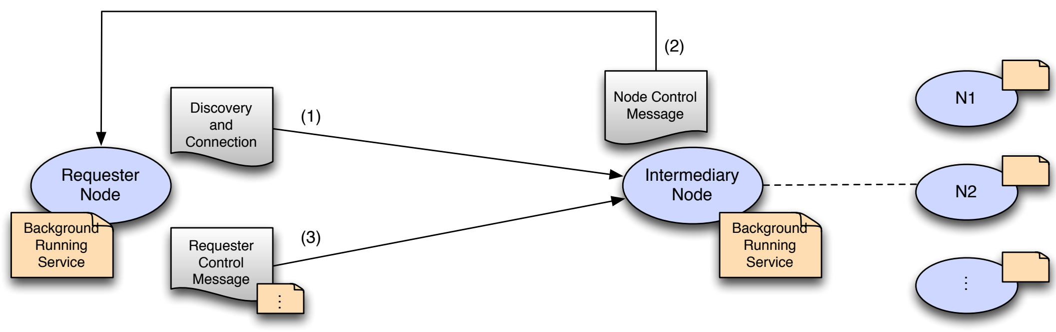


Figure 31. Data exchange sequence.

In this Figure it is possible to perceive the following message exchange sequence: (1) First it occurs the node discovery and connection by the requester node; (2) the intermediary relay node responds with the node control message; (3) The requester node sends all necessary information for cooperation process, using a requester control message.

All these mechanisms contribute to a fully operational ubiquitous cooperation reputation-based system, which aim to improve the global Internet connectivity and remote data access.

5. Performance Evaluation and System Validation

This chapter focus on the system validation and in the performance evaluation of the ubiquitous cooperation mechanisms, which were integrated in an existing m-health application, presented in the following Section 5.1. Section 5.2 presents the created cooperation scenario and necessary assumptions for performance experiment purposes. In Section 5.3 is approached the performance evaluation of the ubiquitous cooperation mechanisms taking into account the experimented scenario, where performance metrics and its analysis are addressed. Last, Section 5.4 summarizes this chapter.

5.1. SapoFit, a m-health Android Application

This section shortly presents SapoFit, an m-health application, developed for Google Android OS and carried out with SAPO (Portugal Telecom) and Next Generation Networks and Applications Group (NetGNA). This mobile health application focus on obesity prevention and treatment, retrieving user information and returning the actual Body Mass Index (BMI) along with the calculated ideal BMI for a specific person, while giving constants and improved treatments over time to achieve a certain weight objective, as may be seen in Figure 32.

Figure 32. User login, food treatment plans and user profile screenshots of SapoFit mobile application.

All cooperation mechanisms were integrated in this Android application, as previously referred, through a foreground service, in order to allow cooperation regardless the application state. The application originally uses a Web Service in order to remotely store all user information along with treatments information, which was modified in this work in order to provide the Cooperation framework to the WS.

5.2. Cooperation Scenario

A cooperation scenario was created and used for performance evaluation purposes, residing on the requester node (RN), three cooperative relay nodes (C_1, C_2 and C_3), which include one node with Internet connectivity, and *Un*, the uncooperative node. There are also three invalid nodes. These nodes are not within the Bluetooth range of the remaining nodes or they are not applicable (i.e., they do not have integrated cooperation mechanisms). The scenario is presented in Figure 33.

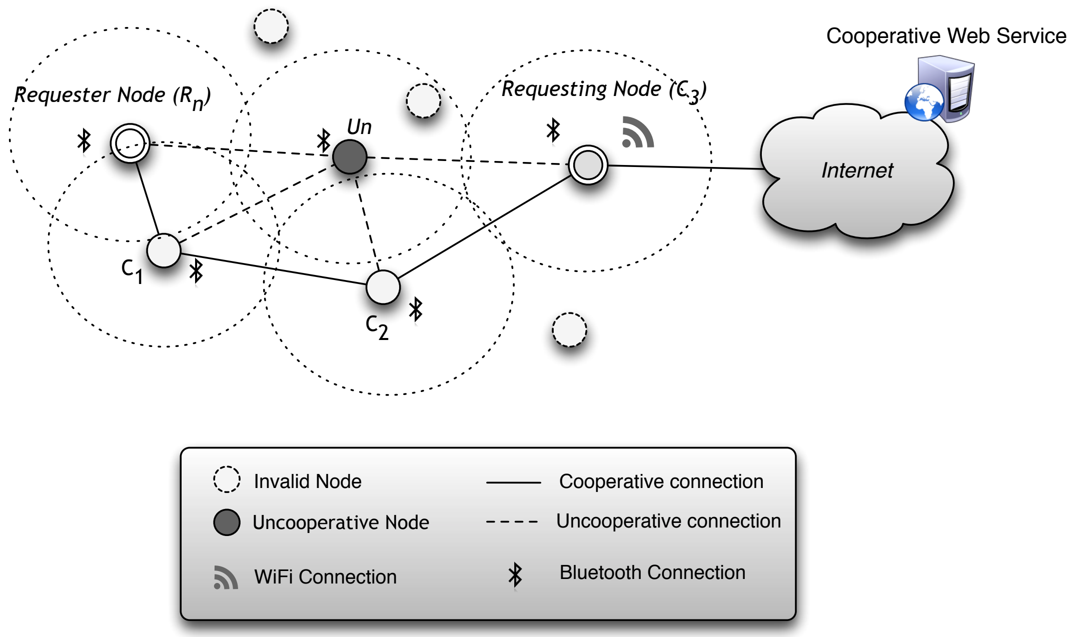


Figure 33. Network scenario for performance evaluation.

In a first sight it is possible to verify that the optimal path for both the request and the response would be as presented in the following Figure 34, where only one relay node is required.

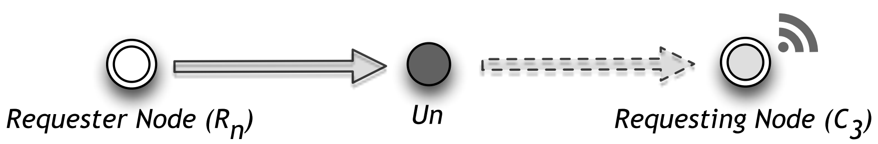


Figure 34. Request optimal path.

However, *Un* is an uncooperative node, which means that an alternative optimal path needs to be defined, as presented in Figure 35.

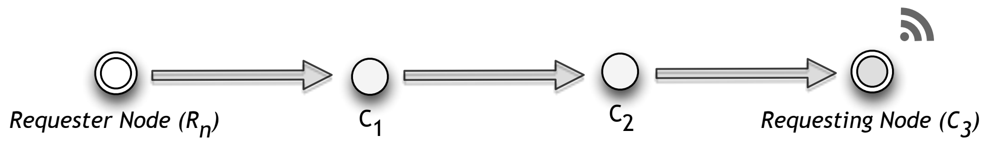


Figure 35. Alternative request path.

However, for experiment purposes, the uncooperative node was intentionally placed in order to be detected first than C_1 from the node R_n perspective, purposely resulting in a time loss, as presented in Figure 36.

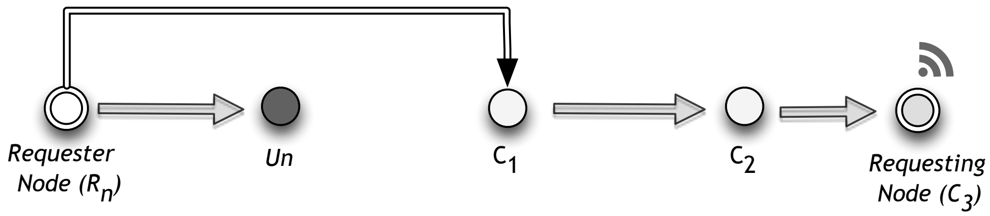


Figure 36. Established request path.

Thus, through R_n neighbours list, remaining nodes are informed that *Un* has an uncooperative state, so all can avoid the node in the response path, as presented in Figure 37.

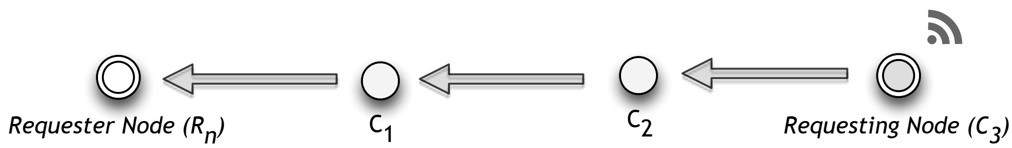


Figure 37. Response path.

Before approaching the performance evaluation, it is important to address the number of processes that occurs in the cooperation flow of the created scenario, which is presented at Table 2.

Table 2. Number of required processes.

Processes		**Request Path**	**Response Path**
A	Discovery	3	3
B	Connection Establishment	4	2
C	Node Control Message	4	-
D	Requester Control Message	3	3

These processes are described as follows.

A) **Discovery**. It is necessary three necessary discovery processes. Two to find C_1 and C_2 nodes, and one to find Un_1 and C_3. In the response path, three discovery processes are required in order to confirm the presence of the original intermediary nodes.

B) **Connection**. It is required a total of six connection processes. The response path has two less connections that the request, because the uncooperative node is avoided, and the requested node, C_3, does not need to connect again to node C_2.

C) **Node Control Message.** The node control message is sent during the request path three times. The NCM is not exchanged during the response due to the fact that the original nodes remain in the same position and cooperative state.

D) The **Requester Control Message** is aggregated and sent a total of six times, during the request and after the Web Service response.

The performance tests took place with four real mobile devices as may be seen in Figure 38, and three simulated devices to serve as uncooperative nodes. These tests were performed on both indoor and outdoor environments.

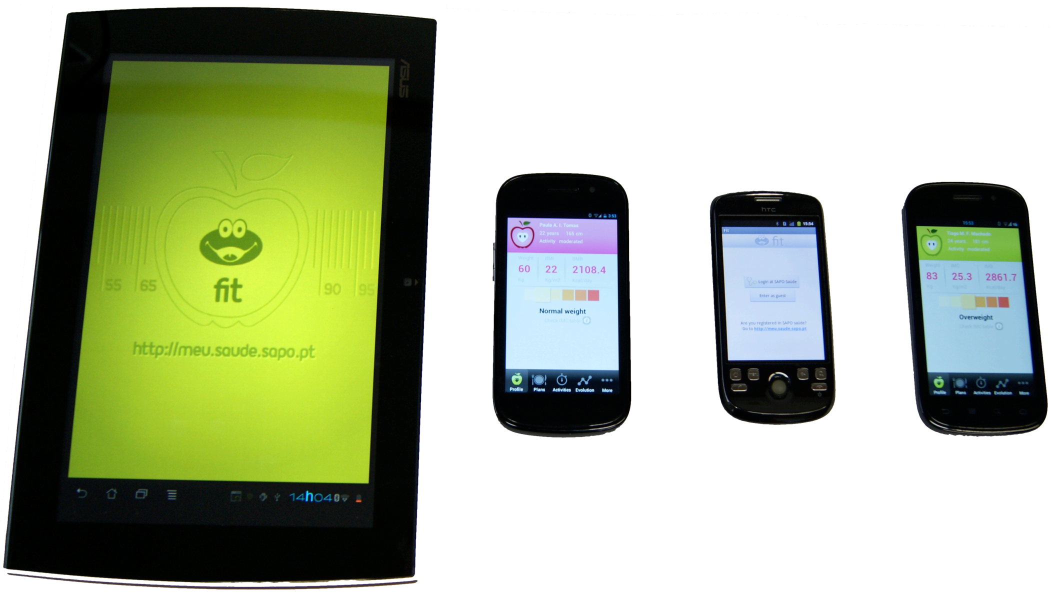


Figure 38. Used mobile devices.

The four mobile devices, one tablet and three smartphones, have the Google Android Operating System, with the 4.0.3 version in the tablet, version 4.0.4 in both Samsung Nexus S, and 2.3.3 in the HTC Magic. These devices possess Bluetooth class 2 modules, as most of the common mobile devices [103], and the 2.1 core version. Having Bluetooth class 2 means they have an approximate maximum range of ten meters. Thus, indoor and outdoor tests were performed at a distance of approximately eight meters between each mobile node, in order to avoid failed connections.

In the next Section 5.3 is performed the performance evaluation of all measured and retrieved data, taking into account this specific scenario.

5.3. Performance Evaluation of Ubiquitous Cooperation Mechanisms

This section performs the performance evaluation of the cooperation mechanisms, and will address the performance metrics in Section 5.3.1, which will be used in the Section 5.3.2 in order to retrieve and calculate the necessary data to provide the system performance analysis.

5.3.1. Performance Metrics

This section presents the two performance metrics that were considered in this study, namely the request delay and the response delay.

Request Delay (RQD): the RQD metric measures the average time that it takes in order to make a service request, i.e., until the requester node initiates a the discovery process and until it is received by a node with Internet connectivity or the request expires. Equation 5.1 presents how RQD is calculated.

$$RQD = Cn_1(\beta + \alpha + \sigma + \varphi) + Un_1(\beta + \alpha + \sigma) + Cn_2(\alpha + \sigma + \varphi) + \delta \quad (5.1)$$

Where,

- Cn_1= Total number of cooperative nodes, not in neighbours list (i.e., found nodes through discovery process), during the request;
- Cn_2 = Total number of cooperative nodes, in neighbours list (i.e., a node already been discovered), during the request;
- Un_1= Total number of uncooperative nodes, during the request;

- β = Average node discovery time;
- α = Average Bluetooth connection establishment time;
- σ = Average node control message time transfer between two nodes;
- φ = Average time transfer of the requester control message, between two nodes;
- δ = Time loss due to a failed connection;

Response Delay (RPD): the *RPD* metric measures the average time that is required to send the response from the node with Internet connectivity to the requester node. Equation 5.2 presents the formula in order to calculate the RPD. In case that a node with WS connectivity is not found, it measures the delay that it takes to carry that information back to the requester node.

$$RPD = \varphi + Cn_3(\beta + \alpha + \sigma + \varphi) + Un_2(\beta + \alpha + \sigma) + (Cn_4 - 1)(\alpha + \varphi) + \delta \quad (5.2)$$

Where,

- Cn_3 = Total number of cooperative nodes found through discovery procedure, during the response;
- Cn_4 = Total number of cooperative nodes, used through neighbours list, during the response;
- Un_2 = Total number of uncooperative nodes, during the response;
- β = Average node discovery time;

- α = Average Bluetooth connection establishment time;
- σ = Average node control message time transfer between two nodes;
- φ = Average time transfer of the response through the RCM.
- δ = Time loss due to a failed connection;

Thus, in order to calculate the necessary average total time (ATT) required to make a full request and to receive the response, it is calculated through the following Equation 5.3, which is basically the sum between *RQD* and *RPD*.

$$ATT = RQD + RPD \tag{5.3}$$

5.3.2. Performance Analysis

This section presents the performance analysis of the achieved cooperation system in this work. As previous referred, when a requester node requires cooperation from a node, there are processes involved, namely the discovery procedure, the connection establishment, the transfer time of the NCM and in a case involving a cooperative node the RCM as well. Eventually, it can also occur a failed connection. All these processes were individually and collectively timed in exhaustive tests, obtaining its average values after thirty experiments. The results are presented at Table 3. The discovery procedure starts and finishes in an average of 1732 milliseconds, a connection establishment is performed in an average of 2475 milliseconds, the NCM is sent in approximately 87 milliseconds and the RCM is sent in about 165 milliseconds. A specific test was also performed in order to test the time loss due to a failed connection, and therefore the time loss in an average of 5146 milliseconds was measured. However, all other experiments went free of failed and problematic Bluetooth connections.

Table 3. Processes periods in milliseconds.

Processes \ Environment		Indoor (10 m)	Outdoor (10 m)	
α	Discovery	2221	1243	1732
β	Connection Establishment	2670	2280	2475
σ	Node Control Message	102	71	87
φ	Requester Control Message	195	134	165
δ	Failed Connection	5146		

The request delay always result in a different value when comparing to the response delay, due to the fact that even the return path route remains the same, the discovery process will not be necessary. In the case that the response has to follow an alternative route, there is the probability of finding and spending time with uncooperative nodes. Experiments were conducted in order to calculate both request and response delays, i.e., the RQD and RPD metrics, as presented at Figure 39. As may be seen, the created scenario with one uncooperative node resulted in a request delay of approximately 16 seconds. Simulated experiments with two and three uncooperative nodes have resulted in an RQD in an average of 20 and 24.5 seconds, respectively. The experiment conducted without uncooperative nodes have provided the lowest RQD value of approximately 13,4 seconds. The value of the persistent RPD value, about 5.5 seconds, is explained due to the fact that in the conducted tests the neighbours list was used in order to avoid the uncooperative nodes found during the request, which resulted in a response path free of not cooperative nodes.

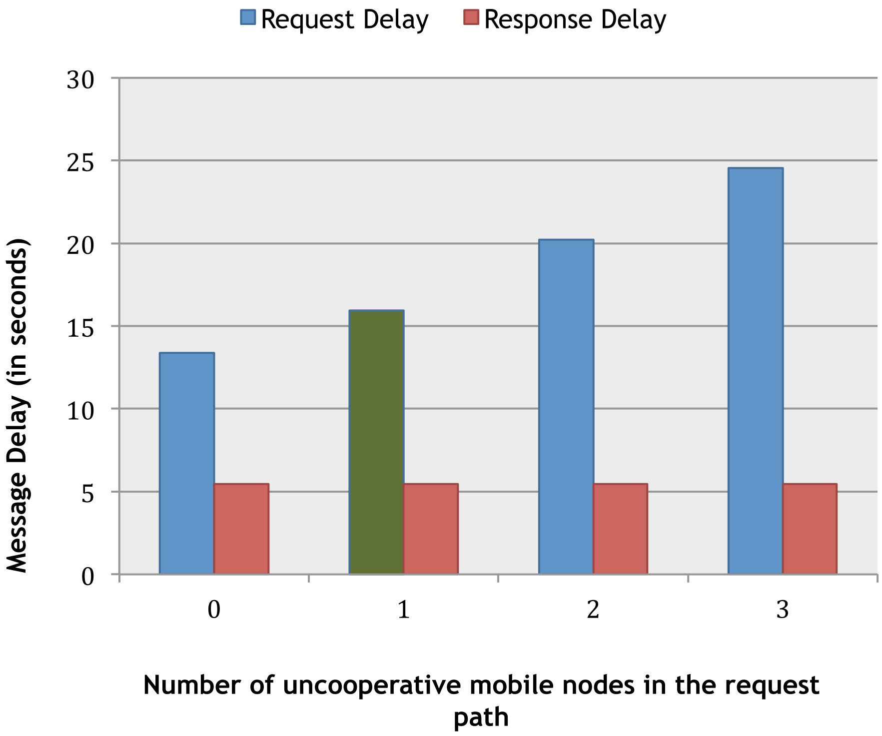


Figure 39. Measuring of the request and response delays

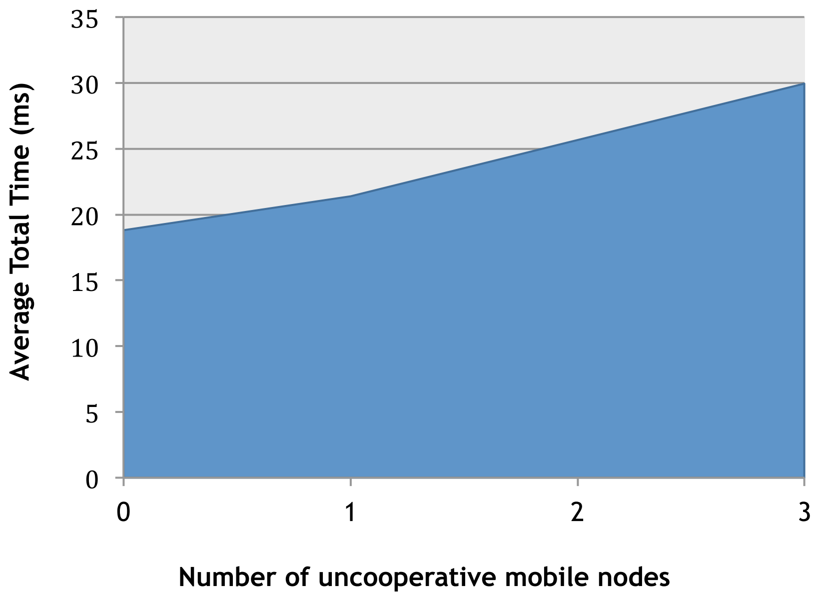


Figure 40. Average Total Time.

In the above Figure 40, the ATT value is shown, which as previously mentioned, have resulted from the total delay from both the request and the response, taking into account from 0 to 3 uncooperative nodes. It is clearly visible that the increase of uncooperative nodes truly affects the cooperation performance. For a scenario without uncooperative nodes, the ATT is approximately 18.8 seconds, consisting on the lowest value. For one and two uncooperative nodes the ATT is about 21.4 and 25.7, approximately. The worst situation occurred when three uncooperative nodes were found in the request path, which caused a final ATT value of about the double of the lowest value, approximately 30 seconds. Thus, in this work this value defines the maximum waiting period (MWP), as previously mentioned in Section 4.3.2.4.

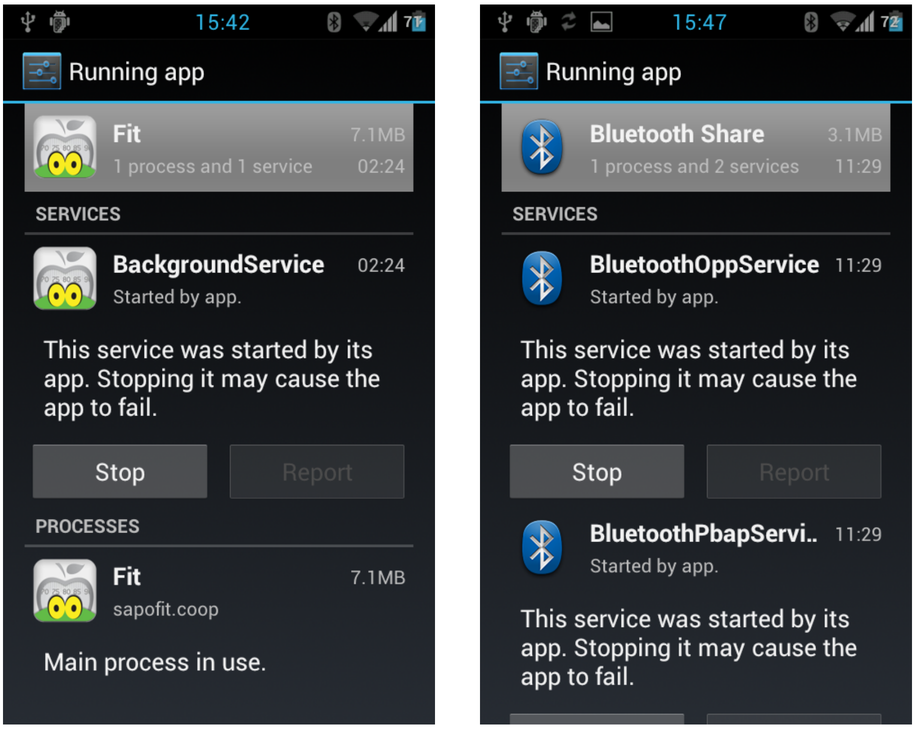


Figure 41. Cooperation memory RAM consumption.

Therefore, when ATT is greater than MWP, relay nodes will stop cooperating for that specific request and the requester node will initiate a new request by searching for different nodes from those found during the previous cooperation process.

As mentioned before, cooperation mechanisms were integrated in a foreground service that runs at the same time that the main activity (i.e., the mobile application itself), however with a background behaviour. In the performed experiments, the revealed memory footprint resulted from the cooperation process never jeopardized the system, and the packet forwarding never failed due to lack of resources. This service was individually tested aside the main process, and the required RAM memory for the service was measured, as may be seen in the above Figure 41. The retrieved value of 7.1 megabytes (MBs) was measure with the service in listen mode, waiting for incoming connections. The maximum value of 8.3 MB was verified when the service was in full operation, exchanging data through Bluetooth with another mobile device. During the packet forwarding, it was also verified a 3.1 mb of memory RAM consumption for the native Bluetooth process of the operating system.

5.4. Summary

This chapter presented in Section 5.1 the m-health application where the cooperation mechanisms were integrated. This application, which was carried out by SAPO and NetGNA, aims the obesity prevention and treatment through a service oriented architecture. In Section 5.2, the cooperation scenario was presented in order to provide an awareness of how the tests were performed, including the information flow, i.e., what information was exactly transmitted between nodes, and in which order; Section 5.3 presented the performance metrics and the performance analysis. Two specific metrics, RQP and RPD, were defined in Section 5.3.1 in order to quantify the delay of the request as well as the delay of the response. In Section 5.3.2 the performance analysis of all collected and calculated data was performed. Tests were performed individually to measure required Bluetooth processes time, and more important, the efficiency of the system. Results clearly show that the greater the number of uncooperative nodes on the packet route path, greater will naturally be the time that the requester node needs to wait for the response. Thus, based on the tests results, a maximum waiting period was defined in order to guarantee the quality of the service, and to avoid a request to run indefinitely until a cooperative node with WS connectivity is found. Last but not least, the consumed amount of memory RAM by the foreground service was measured, and it was revealed a low memory footprint.

6. Conclusions and Future Work

6.1. Conclusions

This chapter presents a synthesis of this dissertation along with the main achievements and important conclusions that result from this work and points some directions for future work. The main objective of this dissertation was to study and develop cooperation mechanisms, creating an integrated pervasive cooperation system for service oriented mobile health applications with Internet connectivity dependency. Fundamentally, these mechanisms aimed to assure that users of a m-health system without WiFi or cellular network data connectivity can access remote data through cooperation, requesting packet forwarding from nearby nodes and receiving data through Bluetooth. This work was carried out with SAPO (Portugal Telecom), for integration with the m-health Google Android application SapoFit. Thus, all the dissertation objectives were successful accomplished and all intermediate objectives were achieved.

After introducing and presenting the topic of this dissertation, define its objectives and main contributions, chapter two presented the cooperation mechanisms state-of-the-art, which included the challenges to its design, its advantages, incentive methods and existing approaches in the literature. It was also approached important related work in mobile health as well as some important insights in ubiquitous health and applications.

Chapter three presented the requirements analysis taken before the cooperation mechanisms development and integration process. First, the essential requirements were defined. Next, the used technologies from the software perspective were described in to provide an awareness of the required tools for the referred processes. Last, user case, activity, sequence and class diagrams were presented.

Chapter four approached the developed ubiquitous cooperation mechanisms for mobile application integration. It was firstly introduced some important details regarding the Google Android mobile platform, such as the ubiquitous foreground service, in order provide the required ubiquitous context to the cooperation system architecture, which is also presented in the referred chapter. Next, the cooperation system architecture is presented, in order to provide an a global perspective of the system. For the proposed reputation-based strategy, a node and requester control messages along with neighbours and reputation lists and a cooperative web service were presented. Besides the potential constraints in service-oriented mobile applications, these mechanisms can also solve some several issues in existing cooperation frameworks, such as the system need for ubiquity, the choice of the optimal route path in packet forwarding as well as the choice for the mobile candidate to serve as a relay node, along with an reputation-based incentive method in order to decrease selfishness and motivate cooperation. It is important to note that this strategy, although defined for mobile health systems, was created taking into account the portability to other types of systems and mobile platforms. This means that this solution can be easily applied in systems with different categories (e.g., social networking services) as well as the use of JSON (both for WS and node communications) and Bluetooth provides common software and hardware interfaces that can be used in other mobile platforms allowing cross-platform interaction.

Chapter five performs the system validation and performance evaluation. After a brief introduction about the m-health application (i.e., SapoFit) where the cooperation mechanisms were integrated, the network scenario for test purposes was presented. Next, two performance metrics, the request delay and the response delay were defined, and were applied in the performance analysis. Experiments were conducted in order to verify the behaviour and efficiency of the system with a various number of uncooperative nodes. Last, the consumed amount of memory RAM by the foreground service was measured.

A major concern during the cooperation system development was the fact that cooperation process would run on mobile devices with limited processor and memory resources, along with the need for ubiquity. Through the use of an Android service, if for some motive (e.g., lack of memory resources) the m-health application is stopped by the operating system or by the user, without user interaction the service restarts as soon as memory resources are restored, allowing the cooperation process to occur in background, transparently to the user. As the performance analysis revealed, the memory footprint resulted from this persistent process never jeopardized the system, and the packet forwarding always occurred without issues. Ultimately, through the conducted experiments the ubiquitous foreground service allowed mobile devices to be exploited at the same time that other functions occurred, such as texting, writing an email or make a phone call, without disturbing the user or jeopardizing packet forwarding. Although, there were some fluctuations on Bluetooth transfer speeds, much because of processor utilization in those different processes.

In terms of energy consumption, performed tests have shown that Bluetooth transmissions spend imperceptible amounts of battery power, with the predictable exception of the unique node with WiFi data connection, where a perceptible decrease of battery power occurred after some dozens of tests, due to the amount of received requests.

The cooperation strategy in this work applied to a particular m-health system clearly presents advantages when comparing to similar systems without cooperative solutions, providing a suitable and free of charge alternative for remote access, as well as performance gains in the server side, due to the less concurrency access. Also, this system allows reducing costs in existing cooperation solutions using specific infrastructures (e.g., relay base stations), due to its infrastructural independency. There are however, some potential downsides. Mobile devices resources, if very low through the various nodes in a request, can possibly affect an entire cooperation process, eventually causing a request to expire. As shown in the performance analysis, selfish or malicious nodes can significantly increase the message delay. While a request with a path with three cooperative intermediate nodes can take approximately 15 seconds, if other three nodes are found before the node with WS access, the delay can reach the 30 seconds approximately, which represents a time loss of 50 percent in that scenario. Thus, it is necessary to take into account the predictable user acceptance issue in terms of the increased energy consumption, which ultimately at some point is required in order to maintain a positive reputation value. It is important that future works provide awareness to the end user that although cooperation usually translates into short-term losses they are often translated into long-term gains.

From this work, it was accepted a paper for an international conference, as well as a submission with extended contributions for a major international journal. This work was also presented in the 15th Seminar of the Rede Temática de Telecomunicações Móveis, University of Minho, Guimarães, Portugal, in June 2012.

6.2. Future Work

To conclude this work, it just remains to suggest future research directions based on current work:

- The development of APIs for other mobile platforms, such as iOS and Windows Phone, could greatly increase the value and usefulness of cooperation mechanisms, for mobile applications that already are multi-platform.

- The use of a location-aware service could provide an alternative to node discovery through Bluetooth.

- Test other routing mechanisms and incentive methods.

- Performance evaluation in larger scale with real users in a dynamic scenario to allow testing the system efficiency and effectiveness in a more reliable manner, as well as its user acceptance to the cooperation system. Real scenario tests would also allow retrieving more accurate data about energy consumption that results from cooperation.

References

[1] L. Gyarmati and T. A. Trinh, "Cooperative Strategies of Wireless Access Technologies: a Game-Theoretic Analysis," *Pervasive and Mobile Computing*, vol. 7, no. 5, pp. 545–568, Oct. 2011.

[2] J. Black, F. Koch, L. Sonenberg, R. Scheepers, A. Khandoker, E. Charry, B. Walker, and N. L. Soe, "Mobile Solutions for Front-Line Health Workers in Developing Countries," presented at the *11th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Melbourne, Australia, 2009, pp. 89–93.

[3] D. Vatsalan, S. Arunatileka, K. Chapman, G. Senaviratne, S. Sudahar, D. Wijetileka, and Y. Wickramasinghe, "Mobile Technologies for Enhancing eHealth Solutions in *Developing Countries," Second International Conference on eHealth, Telemedicine, and Social Medicine (ETELEMED 2010)*, St. Maarten, Netherlands, pp. 84–89, 2010.

[4] C. Doukas, T. Pliakas, and I. Maglogiannis, "Mobile Healthcare Information Management Utilizing Cloud Computing and Android OS," *Conference Proceedings of IEEE Engineering in Medicine and Biology Society (IEEE EMBC 2010)*, Buenos Aires, Argentina, pp. 1037–1040, Jan. 2010.

[5] J. Valarmathi, R. Preethi, N. Bhuvaneshwari, and V. Karthick, "A Novel Trust Management Scheme in Pervasive Healthcare," presented at the *International Conference on Recent Trends in Information Technology (ICRTIT 2011)*, Chennai, India, 2011, pp. 503–508.

[6] M. Weiser, "The Computer for the 21st Century," *IEEE Pervasive Computing*, vol. 99, no. 1, pp. 19–25, 2002.

[7] J. Cheng, "Testing and Debugging Persistent Computing Systems: A New Challenge in Ubiquitous Computing," presented at the *IEEE/IFIP International Conference on Embedded and*

Ubiquitous Computing (IEEE/IFIP 2008), Saitama, Japan, 2008, vol. 1, pp. 408–414.

[8] J. Zhou, E. Gilman, M. Ylianttila, and J. Riekki, "Pervasive Service Computing: Visions and Challenges," presented at the *IEEE 10th International Conference on Computer and Information Technology (CIT 2010)*, Oulu, Finland, 2010, pp. 1335–1339.

[9] Z. Rashid, U. Farooq, J. Jang, and S.-H. Park, "Cloud Computing Aware Ubiquitous Health Care System," presented at the *E-Health and Bioengineering Conference (EHB 2011)*, Suwon, South Korea, 2011, pp. 1–4.

[10] M. Nkosi and F. Mekuria, "Cloud Computing for Enhanced Mobile Health Applications," *IEEE Second International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2010)*, Pretoria, South Africa, pp. 629–633, 2010.

[11] R. Steele and K. Min, "Role-Based Access to Portable Personal Health Records," *International Conference on Management and Service Science (MASS 2009)*, Sidney, Australia, pp. 1–4, 2009.

[12] M. Shanmugam, S. Thiruvengadam, A. Khurat, and I. Maglogiannis, "Enabling Secure Mobile Access for Electronic Health Care Applications," *IEEE Pervasive Health Conference and Workshops*, pp. 1–8, 2006.

[13] W. D. Yu, B. Joshi, and P. Chandola, "A Service Modeling Approach to Service Requirements in SOA and Cloud Computing — Using a u-Healthcare System Case," *IEEE 13th International Conference on e-Health Networking, Applications and Services (IEEE Healthcom 2011)*, Innsbruck, Austria, pp. 233–236, May 2011.

[14] S. van der Burg, M. de Jonge, E. Dolstra, and E. Visser, "Software Deployment in a Dynamic Cloud: From Device to Service Orientation in a Hospital Environment," *Proceedings of theWorkshop on Software Engineering Challenges of Cloud Computing (ICSE 2009)*, Vancouver, Canada, pp. 61–66, 2009.

[15] N. R. Suri, Y. Narahari, and D. Manjunath, "An Efficient Pricing Based Protocol for Broadcasting in Wireless Ad Hoc Networks," *First International Conference on Communication System Software and Middleware, Comsware*, Delhi, India, pp. 1–7, 2006.

[16] D. Zhang, M. Li, and L. Hu, “Challenges to Mobile Ad Hoc Cooperation Design,” presented at the *Proceedings of the 8th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2004)*, 2004, vol. 1, pp. 517–520.

[17] S. Ziane and A. Mellouk, “A QoS Adaptive Multi-path Reinforcement Learning Routing Algorithm for MANET,” *IEEE/ACS International Conference on Computer Systems and Applications (IEEE AICCSA 2007)*, Amman, Jordan 2007, pp. 659-664,

[18] S. S. Manvia, L. B. Bhajantrib, and V. K. Vaggac, “Routing Misbehavior Detection in MANETs Using 2ACK,” *Journal of Telecommunications and Information Technology*, no. 4, pp. 105–111, 2010.

[19] S. Hashmi and J. Brooke, “Authentication Mechanisms for Mobile Ad-Hoc Networks and Resistance to Sybil Attack,” presented at the *Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2008)*, Cap Esterel, France, 2008, pp. 120–126.

[20] L. Tamilselvan and V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET,” *Journal of networks*, vol. 3, no. 5, pp. 13–20, 2008.

[21] E. Hernandez-Orallo, M. Serrat, J. Cano, C. Calafate, and P. Manzoni, “Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog,” *IEEE Communications Letters*, no. 99, pp. 1–4, 2012.

[22] Z. Li and H. Shen, “Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks,” *IEEE Transactions on Mobile Computing*, 2011.

[23] M. Dohler and Y. Li, "Cooperative Communications: Hardware, Channel and PHY", *1st ed. Wiley*, 2010, p. 464.

[24] H. Shan, W. Zhuang, and Z. Wang, “Cooperation or Not in Mobile Ad Hoc Networks: a MAC Perspective,” *IEEE International Conference on Communications (ICC 2009)*, Dresden, Germany, pp. 1–6, 2009.

[25] L. Al-Kanj and Z. Dawy, “Optimized Energy Efficient Content Distribution Over Wireless Networks with Mobile-to-Mobile Cooperation,” presented at the *IEEE 17th International Conference on Telecommunications (ICT 2010)*, Doha, Quatar,

2010, pp. 471–475.

[26] S. Mazuelas, Y. Shen, and M. Z. Win, “Information Coupling in Cooperative Localization,” *IEEE Communications Letters*, vol. 15, no. 7, pp. 737–739.

[27] M. Castillo-EffenUniversity of South Florida, "Cooperative Localization in Wireless Networked Systems," *ProQuest*, 2007, p. 178.

[28] A. Conti, M. Guerra, D. Dardari, N. Decarli, and M. Z. Win, “Network Experimentation for Cooperative Localization,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 467–475, 2012.

[29] T. M. F. Machado, I. M. Lopes, B. M. Silva, and J. J. P. C. Rodrigues, “Performance Evaluation of Cooperation Mechanisms for mHealth Applications,” *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2012) on Communications QoS, Reliability and Modeling Symposium (CQRM)*, Anaheim, USA, December 3-7, 2012.

[30] C. Nøhr and J. Aarts, "*Information Technology in Health Care,*" *IOS Press Incorporated*, 2010, p. 215.

[31] R. Haux, “Health Information Systems - Past, Present, Future,” *International Journal of Medical Informatics*, vol. 75, pp. 268-281, 2006.

[32] P. J. McCullagh, M. Beattie, and C. D. Nugent, “Pervasive Technology to Facilitate Wellness,” presented at the *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA 2010)*, Samos, Greece, 2010.

[33] Y. Zhang, H. Chen, and M. Guizani, "Cooperative Wireless Communications", *1st ed. Auerbach Pub*, 2009, p. 528.

[34] R. Istepanian, S. Laxminarayan, and C. S. Pattichis, "M-Health: Emerging Mobile Health Systems", *1st ed. Springer*, 2006, p. 653.

[35] I. Cubic, I. Markota, and I. Benc, “Application of Session Initiation Protocol in Mobile Health Systems,” presented at the *MIPRO Proceedings of the 33rd International Convention*, Opatija, Croatia, 2010, pp. 367–371.

[36] J. Le Boudec, M. Feham, A. Bouchachia, and A. Bourouis,

"Ubiquitous Mobile Health Monitoring System for Elderly (UMHMSE)," *International Journal of Computer Science & Information Technology (IJCSIT 2011)*, vol. 3, no. 3, pp. 74–82, Jun. 2011.

[37] M. A. Al-Taee, N. A. Jaradat, and D. M. A. Ali, "Mobile Phone-Based Health Data Acquisition System Using Bluetooth Technology," presented at the *IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (IEEE AEECT 2011)*, Amman, Jordan, 2011, pp. 1–6.

[38] A. Alahmadi and B. Soh, "A Smart Approach Towards a Mobile E-Health Monitoring System Architecture," presented at the *International Conference on Network-Based Information Systems (NBIS 2009)*, Indianapolis, USA, 2009, 2011, pp. 1–5.

[39] V. Chan, P. Ray, and N. Parameswaran, "Mobile E-Health Monitoring: an Agent-Based Approach," *IET Communications*, vol. 2, no. 2, p. 223, 2008.

[40] W. Walker, A. L. Praveen Aroul, and D. Bhatia, "Mobile Health Monitoring Systems," presented at the *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE EMBC 2009)*, Minneapolis, USA, 2009, pp. 5199–5202.

[41] A. Talaei-Khoei, P. Ray, and N. Parameswaran, "An Awareness Framework for Agent-Based Mobile Health Monitoring," presented at the *third International Conference on Next Generation Mobile Applications (NGMAST 2009), Services and Technologies*, Cardiff, UK, 2009, pp. 108–113.

[42] B. Kumar, S. P. Singh, and A. Mohan, "Emerging Mobile Communication Technologies for Health," presented at the *International Conference on Computer and Communication Technology (ICCCT 2010)*, Allahabad, India, 2010, pp. 828–832.

[43] J. H. Li, Land, L.P.W., P. Ray, and S. Chattopadhyaya, "E-Health Readiness Framework from Electronic Health Records Perspective," *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, pp. 326–348, 2010.

[44] "ISO/TR 20514, Health informatics - Electronic health record - Definition, scope and context," *American National Standards Institute (ANSI)*, 2005, p. 34.

[45] W. Yina, "Application of EHR in Health Care," *Second*

International Conference on Multimedia and Information Technology, vol. 1, pp. 60–63, 2010.

[46] C. Noteboom and D. Bastola, "Cycles of Electronic Health Records Adaptation by Physicians: How Do the Positive and Negative Experiences with the EHR System Affect Physicians' EHR Adaptation Process?," *45th Hawaii International Conference on System Sciences*, Grand Wailea, USA, 2012.

[47] I. M. Lopes, B. M. Silva, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proenca, "A Mobile Health Monitoring Solution for Weight Control," presented at the I*nternational Conference on Wireless Communications and Signal Processing (WCSP 2011),* Nanjing, China, 2011, pp. 1–5.

[48] J. B. Oladosu, F. A. Ajala, and O. O. Popoola, "On the use of use of Web Services technology in e-health applications," *Journal of Theoretical and Applied Information Technology*, 2009.

[49] T. Shen and Z. Yan, "The Design of Community EHR System Based on PDA," presented at the *International Conference on Complex Medical Engineering (IEEE/ICME 2007)*, Beijing, China, 2007, pp. 398–401.

[50] I. de la Torre Díez, M. Antón-Rodríguez, and F. J. Díaz-Pernas, "Mobile Web Application Development to Access to Psychiatric Electronic Health Records," *Telemedicine Techniques and Applications*, 2011.

[51] D. Patra, S. Ray, J. Mukhopadhyay, B. Majumdar, and A. Majumdar, "Achieving e-Health Care in a Distributed EHR System," *11th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sidney, Australia, 2009, pp. 101–107.

[52] SAPO, "*Meu Sapo Saúde,"* [Online]. Available: https://meu.saude.sapo.pt/ [Accessed: April, 2012].

[53] Intuit Health, "*Medem iHealthRecord,"* [Online]. Available: http://medemphr.mymedfusion.com/ [Accessed: April, 2012].

[54] P. R. Marupally, V. Paruchuri, and S. Chellappan, "Privacy Preserving Portable Health Record (P^3HR)," *International Conference on Network-Based Information Systems (NBIS 2009)*, Indianapolis, USA, 2009. pp. 310–315.

[55] K. Raychaudhuri, "Privacy Challenges in the Use of eHealth

Systems for Public Health Management," *International Journal of E-Health and Medical Communications*, 2010.

[56] MedicAlert Foundation, "MedicAlert E-HealthKEY," [Online]. Available: http://www.medicalert.org/ [Accessed: April, 2012].

[57] S. Sano, T. Yoshihisa, and M. Tsukamoto, "Design and Implementation of Device with Alterable Functions for Ubiquitous Computing," *International Symposium on Ubiquitous Multimedia Computing (UMC 2008)*, Hobart, Australia, 2008, pp. 226–231

[58] S. Yoo, S. Jung, J. Choi, and D. Rho, "Development of Ubiquitous Health Monitoring System," *International Conference on Convergence Information Technology*, Gyeongju, South Korea, 2007, pp. 1116–1120.

[59] A. Bourouis, M. Feham and A. Bouchachia, "A New Architecture of a Ubiquitous Health Monitoring System: A Prototype of Cloud Mobile Health Monitoring System," *International Journal of Computer Science Issues (IJCSI 2012),* Vol. 9, Issue 2, No 2, March 2012.

[60] C. Lin, R. Lee, and C Hsiao, "A pervasive health monitoring service system based on ubiquitous network technology," *International Journal of Medical Informatics*, vol. 77, no. 7, pp. 461–469, Jun. 2008.

[61] J. Choi, B. Choi, J. Seo, R. Sohn, M. Ryu, W. Yi, and K. Park, "A System for Ubiquitous Health Monitoring in the Bedroom via a Bluetooth Network and Wireless LAN," *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE IEMBS 2004)*, vol. 2, pp. 3362–3365, San Francisco, USA, 2004.

[62] I. Brown and A. A. Adams, "The ethical challenges of ubiquitous healthcare," *International Review of Information Ethics*, vol. 8, no. 12, pp. 53–60, 2007.

[63] J. Rodrigues, M. Oliveira, and B. Vaidya, "New Trends on Ubiquitous Mobile Multimedia Applications," *Journal on Wireless Communications and Networking (EURASIP 2010)*, vol. 2010, no. 1, p. 689517, 2010.

[64] C. Z. Qiang, M. Yamamichi, V. Hausman, D. Altman, and I. C. T. S. Unit, "Mobile Applications for the Health Sector," *World Bank ICT Sector Unit*, 2011.

[65] Google, "*Google Android Operating System,"* [Online]. Available: http://www.android.com/ [Accessed: April, 2012].

[66] Apple, "*Apple iOS,"* [Online]. Available: http://www.apple.com/ios/.[Accessed: April, 2012].

[67] Symbian Foundation, "*Symbian Operating System,"* [Online]. Available: http://licensing.symbian.org/ [Accessed: April, 2012].

[68] Google, "*Google Play,"* [Online]. Available: https://play.google.com/ [Accessed: April, 2012].

[69] Apple, *"Apple Store - iTunes,"* [Online]. Available: http://itunes.apple.com/ [Accessed: Apr.-2012].

[70] Nokia, "*Ovi Store*," [Online]. Available: http://store.ovi.com/. [Accessed: April, 2012].

[71] Stabilix Corporation, "*Stabilix PHR*," [Online]. Available: https://play.google.com/store/apps/details?id=com.stabilix.phr.professional.activity [Accessed: April, 2012].

[72] AimX Labs, "*Fast Food Calorie Counter,"* [Online]. Available: https://play.google.com/store/apps/details?id=com.concretesoftware.caloriecounter_full [Accessed: April, 2012].

[73] Noom Inc, "*CardioTrainer*," [Online]. Available: https://play.google.com/store/apps/details?id=com.wsl.CardioTrainer.pro_feature [Accessed: April, 2012].

[74] Capzure, "*Capzule PHR*," [Online]. Available: http://capzule.com/ [Accessed: April, 2012].

[75] PurpleTalk Inc, "*Health and Family*," [Online]. Available: http://store.ovi.com/content/100498 [Accessed: April, 2012].

[76] B. M. Silva, I. M. Lopes, J. J. P. C. Rodrigues, and P. Ray, "SapoFitness: A Mobile Health Application for Dietary Evaluation," *13th IEEE International Conference on e-Health Networking Applications and Services (IEEE Healthcom 2011)*, pp. 375–380, Columbia, USA, 2011.

[77] A. Hinze and G. Buchanan, "The Challenge of Creating Cooperating Mobile Services: Experiences and Lessons Learned," *Proceedings of the 29th Australasian Computer Science Conference, vol. 48*, pp. 207–215, Darlinghurst, Australia, 2006.

[78] P. Liu, Z. Tao, Z. Lin, E. Erkip, and S. Panwar, "Cooperative

Wireless Communications: a Cross-Layer Approach," *IEEE Wireless Communications*, vol. 13, no. 4, pp. 84–92, 2006.

[79] G. Kramer, I. Marić, and R. D. Yates, *Cooperative Communications. Now Pub*, 2007, p. 160.

[80] M. H. L. Froushani, B. H. Khalaj, and S. Vakilinia, "A Novel Approach to Incentive-Cased Cooperation in Wireless Ad Hoc Networks," *18th International Conference on Telecommunications*, pp. 78–83, Ayia Napa, Cyprus, 2011.

[81] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, pp. 107–121, Canterbury, UK, 2002.

[82] J. Hu, "Cooperation in Mobile Ad Hoc Networks," *Computer Science Department. Florida State Universit*, 2005.

[83] Z. Safaei, M. Sabaei, and F. Torgheh, "An Efficient Reputation-Based Nechanism to Enforce Cooperation in MANETs," presented at the *International Conference on Application of Information and Communication Technologies (AICT 2009)*, Azerbaijan, Baku, 2009, pp. 1–6.

[84] J. Sen, "A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks," *International Journal HIT Transaction on ECCN (Electronics, Communication, Computers and Networking)*, Dec. 2010.

[85] S. Misra, I. Woungang, and S. C. Misra, "Guide to Wireless Ad Hoc Networks," *Springer*, 2009.

[86] S. Shivshankar, Y. Ma, and A. Jamalipour, "A Correlative Study of Cooperation Enforcement Mechanisms," presented at the *Australasian Telecommunication Networks and Applications Conference (ATNAC 2011)*, Melbourne, Australia, 2011, pp. 1–6.

[87] T. Anantvalee and J. Wu, "Reputation-Based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks," *IEEE International Conference on Communications (IEEE ICC 2009)*, Glasgow, Scotland, 2007, pp. 3383–3388.

[88] Z. G. Al-Mekhlafi and R. Hassan, "Evaluation Study on Routing Information Protocol and Dynamic Source Routing in Ad-Hoc

Network," presented at the *7th International Conference on Information Technology in Asia (CITA 2011)*, Sarawak, Asia, 2011, pp. 1–4.

[89] S. Sukumaran and V. Jaganathan, "Reputation Based on Demand Routing Protocol Using Mobile Agent in Mobile Ad-Hoc Networks," presented at the *International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010)*, Chennai, India, 2010, pp. 1–4.

[90] S. Sukumaran and E. Blessing, "Reputation Based Localized Access Control for Mobile Ad-hoc Networks," presented at the P*roceedings of the 5th international conference on Ad-Hoc, Mobile, and Wireless Networks*, Ottawa, Canada, 2006, vol. 4104, pp. 197–210.

[91] C. Chowdhury and S. Neogy, "Estimating Reliability of Mobile Agent System for Mobile Ad hoc Networks," *Third International Conference on Dependability (DEPEND 2010)*, Venice/Mestre, Italy, 2010, pp. 45–50.

[92] V. Balakrishnan, V. Varadharajan, U. Tupakula, and P. Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks," *4th International Symposium on Wireless Communication Systems (ISWCS 2007)*, Oct. 2007, Trondheim, Norway, pp. 592–596.

[93] T. Suzuki, M. Kobayashi, A. Khan, and M. Morita, "Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad Hoc Networks," *IEEE International Conference on Communications (IEE ICC 2006)*, Istanbul, Turkey, 2006, vol. 8, pp. 3729–3734.

[94] A. M. Raafat, M. Fathy, A. Yehia, and M. A. Azer, "Cooperation Incentives in Wireless Ad Hoc Networks," presented at the *2nd International Conference on Education Technology and Computer (ICETC 2010)*, Shanghai, China, 2010, vol. 5.

[95] S. Buchegger and J. Le Boudec, "Self-Policing Mobile Ad Hoc Networks by Reputation Systems," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101–107, 2005.

[96] C. Chen and S. Kishore, "Making Cooperation Valuable: a Delay-Centric, Pricing-Based User Cooperation Strategy," presented at the *45th Annual Conference on Information Sciences and Systems (CISS 2011)*, Baltimore, USA, 2011, pp. 1–6.

[97] D. Mathews, K. Ananda, and S. Radha, “Dynamic Pricing Approach for Cooperation Stimulation and QoS in Mobile Ad Hoc Networks,” *11th IEEE International Conference on Computational Science and Engineering (IEEE CSE 2008)*, São Paulo, Brazil, 2008, pp. 388–393.

[98] Z. M. Nezhad and S. Khorsandi, “Cooperation enforcement based on dynamic pricing in multi-domain sensor network,” *IEEE Consumer Communications and Networking Conference (IEEE CCNC 2011)*, 2011, Las Vegas, USA, pp. 1055–1060.

[99] Z. MohammadNejad, M. Ahmadian, and S. Khorsandi, “Providing a Hybrid Algorithm for Routing and Cooperation Based on Dynamic Pricing in Wireless Sensor Networks,” *International Conference on Application of Information and Communication Technologies (AICT 2009)*, Venice/Mestre, Italy, 2009, pp. 143-148.

[100] J.-H. Huang and Y.-F. Kao, “Price-Based Resource Allocation Strategies for Wireless Ad Hoc Networks with Transmission Rate and Energy Constraints,” presented at the *Proceedings of 16th International Conference on Computer Communications and Networks*, Honolulu, USA, 2007, pp. 1065–1070.

[101] Y. Luo and R. Deters, “Using Cooperation to Improve the Experience of Mobile Web Services Consumers,” presented at the *IEEE Asia-Pacific Services Computing Conference (IEEE APSCC 2009)*, Guilin, China, 2009, pp. 213–218.

[102] T. Pering, Y. Agarwal, R. Gupta, and R. Want, “CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Rnterfaces,” in *Proceedings of the 4th international conference on Mobile systems, applications and services (MobiSys 2006)*, Uppsala, Sweden, 2006.

[103] Bluetooth SIG Inc, "*Bluetooth Technical Information*," [Online]. Available: http://www.bluetooth.com [Accessed: May, 2012].

[104] J. Yoo and K. H. Park, “A Cooperative Clustering Protocol for Energy Saving of Mobile Devices with WLAN and Bluetooth Interfaces,” *IEEE Transactions on Mobile Computing*, 2011, vol. 10, no. 4, pp. 491–504.

[105] A. Abdel Khalek and Z. Dawy, “Energy-Efficient Cooperative Video Distribution with Statistical QoS Provisions Over Wireless Networks,” *IEEE Transactions on Mobile Computing*, no. 99, pp.

1-1, 2011.

[106] H. Lu and W. Liao, “Cooperative Strategies in Wireless Relay Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 323-330, 2012.

[107] F. H. P. Fitzek and M. D. Katz, Eds., *Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications*, 1st ed. Springer, 2007, p. 750.

[108] T. Z. T. Zhu, C. W. C. Wang, G. J. G. Jia, and J. H. J. Huang, “Toward Context-Aware Location Based Services,” *International Conference on Electronics and Information Engineering (ICEIE 2010)*, Kyoto, Japan, 2010, vol. 1, pp. 1-413.

[109] J. Zhou, Z. Lu, J. Lu, and S. Huang, “Location Service for Mobile Ad Hoc Networks with Holes,” presented at the *International Conference on Networking and Information Technology (ICNIT 2010)*, 2010, pp. 91-96.

[110] Navizon Inc, "*Navizon*," [Online]. Available: http://www.navizon.com/ [Accessed: February, 2012].

[111] Google, "*Google Latitude*," [Online]. Available: http://www.google.com/latitude [Accessed: February, 2012].

[112] Apple Inc., *"Find My Phone*," [Online]. Available: http://www.apple.com/iphone/built-in-apps/find-my-iphone.html. [Accessed: April, 2012].

[113] Koozyt, Inc, "*PlaceEngine*," [Online]. Available: http://www.placeengine.com/en [Accessed: February, 2012].

[114] Skyhook, Inc, "*Skyhook*," [Online]. Available: http://www.skyhookwireless.com/ [Accessed: February, 2012].

[115] J. Eberspächer, H. Vögel, C. Bettstetter, and C. Hartmann, *GSM - Architecture, Protocols and Services*, 3rd ed. Wiley, 2009, p. 338.

[116] C. Sammarco, F. H. P. Fitzek, G. P. Perrucci, A. Iera, and A. Molinaro, “Localization Information Retrieval Exploiting Cooperation Among Mobile Devices,” *IEEE International Conference on Communications Workshops (IEEE ICC Workshops 2008)*, pp. 1-5, Beijing, China, 2008.

[117] Google, "*Google Maps API,"* [Online]. Available: https://developers.google.com/maps/ [Accessed: May, 2012].

[118] H. Wymeersch, J. Lien, and M. Z. Win, “Cooperative Localization in Wireless Networks,” presented at the Proceedings of the IEEE, 2009, vol. 97, no. 2, pp. 427–450.

[119] M. Z. Win, A. Conti, S. Mazuelas, Y. Shen, W. M. Gifford, D. Dardari, and M. Chiani, “Network Localization and Navigation via Cooperation,” *IEEE Communications Magazine*, vol. 49, no. 5, pp. 56–62, 2011.

[120] Object Management Group, "*UML*," [Online]. Available: http://www.uml.org/ [Accessed: April, 2012].

[121] Google, "*Android versions distribution,*" [Online]. Available: http://developer.android.com/resources/dashboard/platform-versions.html [Accessed: June, 2012].

[122] Microsoft, "*Windows Phone*," [Online]. Available: http://www.microsoft.com/windowsphone/ [Accessed: April, 2012].

[123] Google, "*Android Software Development Kit*," [Online]. Available: http://developer.android.com/sdk/index.html [Accessed: April, 2012].

[124] Oracle Corporation, "*Java Server Pages*," [Online]. Available: http://www.oracle.com/technetwork/java/javaee/jsp/index.html [Accessed: April, 2012].

[125] The Apache Software Foundation, "*Apache Tomcat Web Server,*" [Online]. Available: http://tomcat.apache.org/ [Accessed: April, 2012].

[126] Oracle Corporation, "*MySQL Workbench*," [Online]. Available: http://www.mysql.com/products/workbench/ [Accessed: April, 2012].

[127] S. Ickin, K. Wac, M. Fiedler, and L. Janowski, “Factors Influencing Quality of Experience of Commonly Used Mobile Applications,” *IEEE Communications Magazine*, 2012.

[128] Bluetooth SIG, Inc, “Specification of The Bluetooth System,” pp. 1–2302, [Online]. Available: http://www.bluetooth.com/Pages/about-technology.aspx Accessed: May, 2012].

[129] U. Blumenthal, F. Maino, and K. McCloghrie, “The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-Based Security Model,” *in RFC*, vol. 3826, 2004.

Appendix

In this appendix, the paper entitled "Performance Evaluation of Cooperation Mechanisms for mHealth Applications" accepted for an international conference is presented in the following pages, as well as the submitted international journal paper entitled "A Novel Cooperation Strategy for Mobile Health Applications.

Performance Evaluation of Cooperation Mechanisms for mHealth Applications

Tiago M. F. Machado[1], Ivo M. Lopes[1], Bruno M. Silva[1], Joel J.P.C. Rodrigues[1], and Jaime Lloret[2]
[1]Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal
[2]Universidad Politécnica de Valencia, Spain
{tiago.machado; ivo.lopes; bruno.silva}@it.ubi.pt; joeljr@ieee.org; jlloret@dcom.upv.es

Abstract— **Mobile health (m-Health) includes the use of mobile applications to deliver healthcare services anytime and anywhere. This paradigm benefits with the advent of Web services based systems, since they allow health applications available for users with mobility support. This paper presents a novel cooperation strategy for m-Health services and applications. It consists in a reputation-based strategy for Web services oriented architectures that includes a cooperative Web service for managing all the network cooperation and nodes reputation. The cooperation strategy is divided in two modules for mobile nodes, one for verifying the cooperation status of neighbor nodes and another for classifying the neighbor nodes in function of their reputation. The performance of the proposal is evaluated in a real scenario, using an m-Health application, called *SapoFit*.**

***Keywords*- Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Healthcare Application.**

I. Introduction

Mobile health (m-Health) is considered the next generation of e-Health systems and it is already changing typical healthcare services [1-2]. Figure 1 illustrates a typical m-Health service architecture supported by Web services (WS). These WS are hosted on Web servers and can be used through network connectivity, including the Internet. These types of architectures based on mobile devices and wireless communications presents challenged issues, such as, battery and storage capacity, broadcast constrains, interferences, disconnections, noises, limited bandwidths, and network delays.

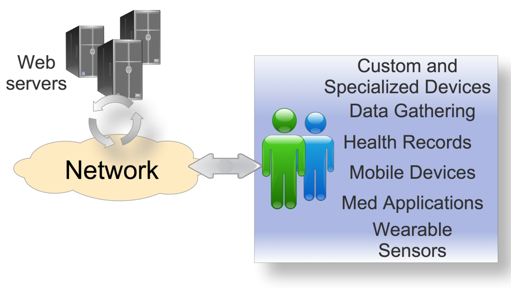


Figure 1. Illustration of an m-Health application framework based on Web services.

Cooperation-based strategies have been presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability. Furthermore, in the last years several cooperation mechanisms and algorithms have been proposed to improve wireless networks performance, where mobile nodes cooperate with each other performing all networking functionalities [3-4]. This paper presents a novel cooperation strategy for m-Health applications focusing on forwarding and retrieving data to/from nodes that have no direct connection to an m-Health service. For instance, devices without Internet connection can use their m-Health applications without problems. This m-Health cooperation proposal is a reputation-based strategy where a Web service manages all the cooperation among nodes and their reputation. It is based on three main components: a *node control message*, a *network cooperative list*, and a *cooperative Web service* (*CWS*). The *control message* and the *cooperative list* are included in the mobile nodes requests for services, and record all cooperative and non-cooperative actions. The *CWS* includes a reputation table for all nodes and decides which nodes can have access to the requested services. The performance assessment and validation of the proposal is also presented. This evaluation studies the impact of the cooperation strategy on the performance of an m-Health application taking into account different number of uncooperative nodes. The cooperation proposal is deployed and evaluated in an m-Health application for obesity prevention and control, called *SapoFit* [5-7]. Results show that mobile nodes without Internet connectivity can use the application continuously with success. It also shows the improvement of the service delivery probability and service average delay, increasing the overall network performance.

The remainder of this paper is organized as follows. Section II elaborates on related work about the topic focusing on cooperation techniques that contribute to the proposed cooperation solution. Section III describes the proposed m-Health cooperation strategy. A performance evaluation and validation through a prototype with an m-Health application is presented in Section IV. Finally, Section V concludes the paper and points out further research works.

II. Related Work

Cooperation is expected to play a central role in the evolution of pervasive mobile health applications towards mobile wireless networks. In wireless networks, energy saving is one of the biggest concerns in mobile devices due to its limited resources. In [8] it is demonstrated that the energy consumed by Wi-Fi transmissions in idle hand-held devices can achieve more than 50% of the total energy. Thus, it is proposed the use of short links (e.g., Bluetooth) in order to save energy since it is estimated that Bluetooth consumes less than 10% battery power. In [9], an optimized energy efficient content distribution strategy for wireless ad-hoc networks is presented. The proposal consists in a centralized base station for network optimization management in order to reduce overall mobile devices energy consumption. A similar cooperative approach is presented in [10] for wireless networks which also uses a main base station for coordination, and rather than relay nodes proposes the use of relay stations in order to optimize the network performance and decrease overall node battery consumption. In order to improve the responsiveness of a Web Service to consumers, it is presented an approach in [11] that uses two proxies in order to arrange the cooperation strategy. The server-proxy aims to improve the server-side responsiveness. The client-proxy exists as a software module in the mobile application to allow cooperation with the service provider by sharing workflow for pre-processing. Furthermore, to improve mobile clients performance a server-side caching component and a prediction model are also included.

In cooperative systems, neither all nodes forward other nodes messages – they are called *uncooperative nodes*. Uncooperative nodes can be *faulty* or *malicious,* and/or *selfish* [12]. In order to mitigate the selfishness problem, many cooperation schemes have been proposed for stimulate cooperation and mitigate the detrimental effect of non-cooperative nodes. Basically, two types of strategies were classified, *virtual currency based schemes (also known as pricing-based strategies)* and *reputation based schemes*.

Pricing-based schemes use incentives to inflict nodes cooperation. These incentives are given to nodes that cooperate and use them in order to gain privileged services from the network, such as faster and/or routes more reliable. Non-cooperative nodes that have no currency cannot choose the route or do not have access to the service. Therefore, pricing-based schemes assume that forwarding a message incurs in a cost to a node. A dynamic pricing approach is presented in [13]. It proposes a routing scheme where users (i.e., nodes) could choose a route with least cost, which does not guarantee the quality of service (QoS) or a route with desired QoS guarantees but demands a higher cost.

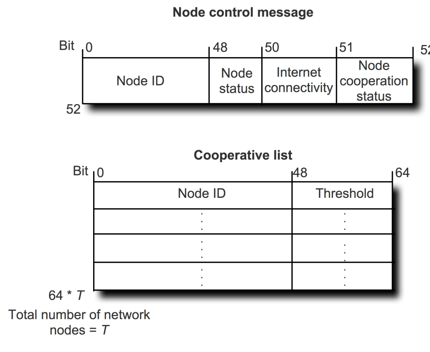
Reputation schemes use the node reputation to cutback selfish behavior. Generally, its calculation is assessed by neighbor monitoring or through the exchange of reputation information between nodes. The three main reputation-based cooperation systems are CONFIDANT [14], CORE [15], and OCEAN [16]. CONFIDANT uses a monitoring module to directly detect and isolate non-cooperative nodes in the network. CONFIDANT scheme assents on four components per node: a monitor module, so nodes can locally monitor any deviating behavior; a trust manager to make decisions about providing or accepting route information; a reputation system that holds all information about node reputation values; and a path manager which according to reputation values defines paths to avoid malicious nodes. Similarly, CORE schemes uses monitoring to stimulate cooperation among nodes and to detect and isolate non-cooperative nodes, but it defines three types of reputation: *subjective reputation,* based on direct observation; *indirect reputation,* according to information provided by other nodes; and *functional reputation* which is calculated through a function that uses a weight in function of its importance. Unlike CONFIDANT and CORE, OCEAN divides misbehavior nodes into misleading and selfish groups. If a node takes part in route finding but does not forward a packet is a misleading node, but if doesn't take part on route finding is a selfish node. When the node rating is lower than the pre-determined threshold is added to an avoid list and classified as problematic. It is given to the node a period time to cooperate and return to the network. Although CONFIDANT, CORE and OCEAN are the three main reputation-based cooperation systems, many authors and existing approaches choose to adapt and create reputation systems with combined and/or different specifications from these schemes. Our proposed reputation-based system is based on CONFIDANT and CORE schemes, because it possesses characteristics from both, as it will be demonstrated later.

I. COOPERATION MECHANISMS FOR MOBILE HEALTH APPLICATIONS

This section describes, the cooperation approach for m-Healh applications. It is based on the following three modules: *i*) a node control message, *ii*) a cooperative list, and *iii*) a cooperative Web service (CWS).

a. Nodes control message and network cooperative list

The control message is exchanged when a node makes contact with a neighboring node. This message attempts to provide a control consciousness control of neighbors nodes know if they are willing to cooperate and under what conditions. It contains a node ID, node status (storage capacity, power and Internet connectivity), and the status of cooperation (cooperative or uncooperative). An illustration of a control message and a list of cooperative nodes can be seen in Figure 2.



The cooperative list records all cooperative nodes and uncooperative during a service request. This list ranks all the neighboring cooperative actions. It saves the node ID and adds or subtracts a threshold for classification according to the state of node cooperation. Each node updates the list of co-operation each time a service is requested from a single node (a node without Internet connectivity).

The cooperative threshold list (CT) starts at 0 (zero) and a unit (1) is added or subtracted in accordance with the state of cooperation node and node status. The CT has a direct influence on the reputation of the node. Table I shows the correlation between the node co-operation status, the node status, its Internet connectivity and the resulting CT. The node status is based on its capacity to store and energy lifetime. A node has three types of status: poor, regular and excellent. It is assumed that a node is poor when the storage capacity of the device is 95% or more, or its power energy available is less than 20%. The regular state occurs when a storage capacity of the node is less than 95% and its power supply is between 20% and 80%. A node is an excellent state when the storage capacity of the node is less than 95% and energy power available is greater than 80%. The CT varies between -2 and +3. This interval is taken to ensure that non-cooperative nodes with a low number of nodes are punished. Nodes with co-operative in a poor state has the highest value of CT (+3). Furthermore, nodes in a poor state, with or without storage capacity or low battery, have a plausible justification for not cooperating, so they are not punished in their CT (0).

The worst scenario for a cooperative node is one that is in excellent condition, with connectivity to the Internet and still refuses to cooperation. This node is punished with the worst CT value (equal to -2).

TABLE I. CORRELATION BETWEEN THE NODE COOPERATION STATUS, THE NODE STATUS, ITS INTERNET CONNECTIVITY, AND THE RESULTANT CT CLASSIFICATION.

Node Status	**Internet Connectivity**	**Cooperation State**	**CT**
Poor	0	0	**0**
Poor	0	1	**+3**
Poor	1	0	**0**
Poor	1	1	**+3**
Regular	0	0	**-1**
Regular	0	1	**+2**
Regular	1	0	**-2**
Regular	1	1	**+2**
Excellent	0	0	**-2**
Excellent	0	1	**+1**
Excellent	1	0	**-3**
Excellent	1	1	**+1**

a. Cooperative Web service and reputation table

The cooperative Web service (CWS) includes the table of node reputation. To calculate the reputation, the CWS uses the node cooperation lists. Based on node reputation, it decides if the requesting node must have access to the Web service m-health application or not. The reputation table lists all the network nodes with its reputation and its current cooperative threshold. The threshold value on the reputation table for the node N is represented by Cn. After the CWS receives a request and the corresponding cooperative list, the service adds the CT value into the threshold in the reputation table for nodes listed in the cooperative list, i.e., $C_N = C_N + CT$. The reputation table considers three states of Reputation: selfish, cooperative or super-cooperative. As can be seen by (1), these states are calculated using the node, and an optimum interval of time that is based on the total number of network nodes (t). For networks with few nodes, it is extremely important that uncooperative nodes receive worst CT, punishing and motivating them to cooperate. Therefore, half the number of network nodes to limit the range to the states reputation (*t*/2) is used.

$$Rep(N) = \begin{cases} Selfish,\ C_N \in \left]-\infty, -\frac{t}{2}\right[\\ Cooperative,\ C_N \in \left[-\frac{t}{2}, +\frac{t}{2}\right[\\ Super-Cooperative,\ C_N \in \left[+\frac{t}{2}, +\infty\right[\end{cases} \quad (1)$$

Based on the nodes reputation, the CWS will not grant access and release any resources of the Web services for selfish nodes. Selfish nodes are punished by CWS with an order to cooperate until it reaches a cooperative state. The CWS releases resources for cooperative, however, super-cooperative nodes have a first priority over application resources in case of simultaneous requests.

The CWS also stores a list of all requests that were positively answered. These requests are stored until their time-to-live (TTL) expires. The TTL is the average delay that receives a request to be answered by the Web service. This list prevents that earlier requests are answered from the same node a second time.

A major concern in the proposal is the issue of privacy of all data transmitted and retrieved. Privacy is a matter of priority in m-health services that deal with sensitive user information. On m-Health applications diverse security issues must be considered, such as personal information management, secondary use of personal information, misuse of personal information, and errors with the personal information stored. Therefore, cryptographic mechanisms can be seen as a solution to guarantee data confidentiality and protection [17]. The cooperation strategy presented assumes secure transactions of data between nodes using the Advanced Encryption Standard (AES) encryption algorithm used in Cipher Feedback Mode (CFB), with a key size of 128 bits [18].

IV. DEMONSTRATION AND VALIDATION

This section focuses on the performance evaluation and validation of the m-Health cooperation proposal. First, the m-Health application where the cooperation mechanisms were evaluated along with the respective network scenario and node expected behaviours is presented. Later, the validation and feasibility of the proposal and the performance evaluation results are shown. This study focuses on nodes service requests delivery probability and service average delay. These are the network challenges that the presented cooperation proposal aims to resolve and improve.

a. SapoFit Application

SapoFit application allows users their weight control, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility of following food plans based on the calories that user need in a healthy way. The entire communications pass through a Web service. Values such as name, height, sex, age, weight, and general physical activity level are used to calculate the user ideal weight, BMI, and BMR. Figure 3 shows three application activities, *Login*, *Plans*, and *Profile*. At the *Login* a user inserts is credentials. The Web service responds with the user data to populate the Profile window, which is the main window of SapoFit. The *Plans* activity displays the daily calories depending on the weight that the user wants to obtain, also presents daily meals with calories. For the performance evaluation of the m-Health cooperation proposal, it was considered a user without network availability, using the nodes cooperation to request access to the *Login*, *Profile* and *Plans* services.

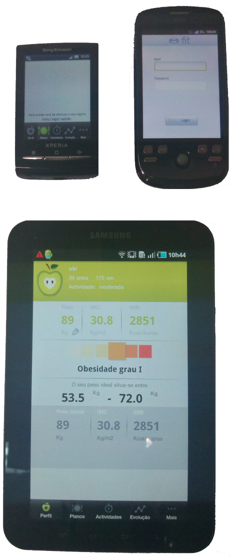


Figure 3. Three real activities of SapoFit with *Login*, *Food Plans*, and *User Profile* Screenshots.

b. M-Health network scenario

The real m-Health network scenario used for the performance evaluation study of the cooperative proposal may be seen in Figure 4. It includes eight mobile nodes (using SapoFit), assuming that three of them are uncooperative nodes. Node M is the single node with connection to the SapoFit Web services. Although an m-Health scenario presents high node mobility, for evaluation purposes, it is assumed the node positioned according to the presented network scenario.

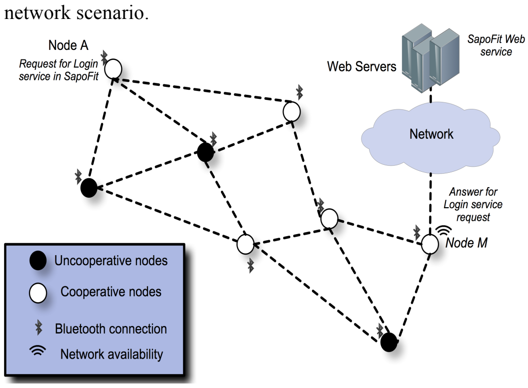


Figure 4. Illustration of the m-Health network scenario used for performance evaluation of the cooperation strategy.

The activity diagram of a mobile node is presented in Figure 5. It is subdivided into three logical parts: (1) Node Discovery; (2) Node Control Message Exchange; and (3) Cooperative Web Service. The objective is to connect to the Web Service and get its data. First, a node without Internet connectivity starts searching for neighbor nodes using Bluetooth connection.

Second, if it finds a known and available node, it receives the *node control message* from it, where the Requester Node (RN) is informed if the requested node (i.e., the found and chosen neighbor node) is in cooperative mode or not. If it does not cooperate, it saves the neighbor cooperative behavior for further update in the WS. Otherwise, the requested node sends the request to the WS along with its cooperative list records. The WS processes the received information updating reputation values according to the received cooperation list, and determines if the requester node is selfish or not selfish. If it is a selfish node, it is sent to the requester node that its reputation is not enough in order to access its data, which means it must cooperate in the future in order to increase its reputation and regain access to the WS. If the *cooperation threshold* status is equal or great than zero, the requested data is sent to the requested node, forwarding the information to the requester. In other hand, a node with Internet connectivity that tries to access the Web Service directly, it also needs to see its reputation verified by the Web Service, in order to determine if it is allowed or not to access the service.

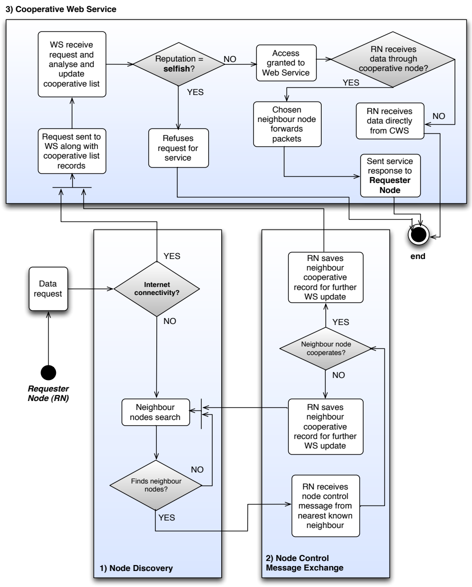


Figure 5. Activity diagram of a mobile node representing a mobile device with SapoFit and its cooperation mechanisms.

c. Performance Analysis

This section focuses on the performance analysis of the proposed cooperative strategy and its impact on the overall network performance. In order to generate this analysis, each demonstrated result is achieved through an average of 30 experiments. In a first analysis, it is possible to realize that the m-Health application cannot access the Web Service if the mobile terminal does not have Internet connectivity and cooperation mechanisms are not integrated. Through these mechanisms all mobile devices, with or without Internet connectivity, gain access to the remote services. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). The service delay is measured as the time between the request for the application service and its delivery. In our demonstrated scenario, it was considered from zero to three uncooperative nodes. The service delivery probability and the service average delay as function of the number of uncooperative mobile nodes are presented in Figure 6. As can be seen, when the number of uncooperative nodes increases, the service delivery probability decreases about 95, 88, 71, and 57 percent, respectively. As expected and present the in Figure 7, the service average delay presents the same behavior. Increasing the number of uncooperative nodes the service average delay increases 17.32, 26.1, 36.5, and 54.7 seconds, respectively. The maximum service delay observed of about 68.7 seconds happened in our experiments with three uncooperative nodes.

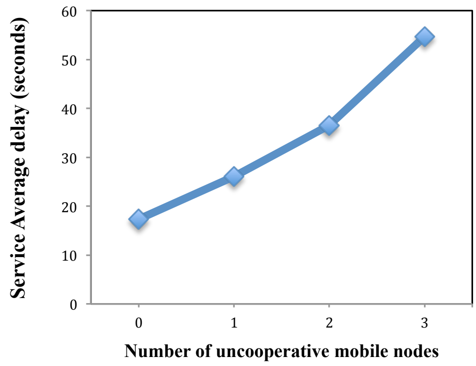


Figure 6. Service average delay as function of the umber of uncooperative mobile nodes.

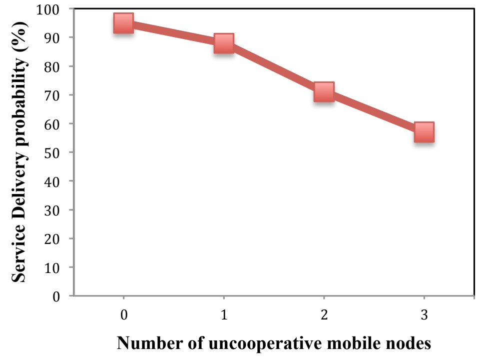


Figure 7. Service delivery probability as function of the umber of uncooperative mobile nodes.

V. CONCLUSIONS AND FUTURE WORK

This paper presented a cooperation strategy for m-Health architectures using a Web service oriented approach. This proposal presents a reputation-based strategy were a Web service manages all the network cooperation. It is based on three cooperation mechanisms: a node control message; a network cooperative list; and a cooperation Web service (CWS). Based on the paradigm of m-Health services, anytime and anywhere, the main objective of this proposal was to raise the quality of the m-health service by forwarding requests in case of network unavailability. Therefore this proposal focuses on the probability of a success service request and its average delay. Furthermore, this work presented the performance assessment and validation of the cooperation proposal. The proposed cooperation mechanisms for m-health applications were deployed and evaluated in a mobile application for obesity control and prevention, called SapoFit.

Through the network performance evaluation and its metrics comparisons, it was concluded that cooperation solution improved significantly the overall performance and the m-Health application. Despite of some results variations due to high mobility patterns and limited laboratory environment, cooperation mechanisms have shown significantly improvements on the service quality, namely on the request for services probability and its average delay.

There are a number of extensions of this work planned to undertake in the future. Many of these involve refining the treatment of sensitive and priority medical information that is handled in m-Health applications. Furthermore, it is important to evaluate the cooperation proposal in more applications scenarios.

ACKNOWLEDGMENTS

This work has been partially supported by the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT – *Fundação para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2011 Project, and by Portugal Telecom - SAPO, Portugal.

REFERENCES

[1] S. Akter and P. Ray, "mHealth - an Ultimate Platform to Serve the Unserved," in IMIA Yearbook of Medical Informatics, Schattauer, Germany, 2010, pp. 94-10.

[2] S. Tachakra, X. Wang, R. Istepanian, and Y. Song, "Mobile e-Health: the Unwired Evolution of Telemedicine," in Telemedicine Journal and e-Health, Vol. 9, pp. 247-257, 2003.

[3] G. Kramer, I. Maric, and R. D. Yates, "Cooperative communications (Foundations and Trends in Networking)," Now Publishers Inc., June, 2007.

[4] L. Buttyán and J-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," in Mobile Networks and Applications, Vol. 8, pp. 579-592, 2003.

[5] Bruno M. Silva, Ivo M. Lopes, Pradeep Ray, and Joel J.P.C. Rodrigues, "SapoFitness: A Mobile Health Application for Continuous Monitoring Dietary Evaluation", in IEEE HEALTHCOM 2011, Columbia, MO, USA, June 13-15, 2011.

[6] Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Bruno M. C. Silva, and Isabel de la Torre, "A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit", in Informatics for Health and Social Care, Informa Healthcare, 2012 (accepted for publication).

[7] SapoFit, http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8, (Accessed in January 2012).

[8] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "CoolSpots: reducing the power consumption of wireless mobile devices with multiple radio interfaces," in *MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services*, 2006.

[9] L. Al-Kanj and Z. Dawy, "Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation," in IEEE 17th International Conference on Telecommunications (ICT), 2010, 4-7 April, 2010, pp. 471-475.

[10] H.-C. Lu and W. Liao, "Cooperative Strategies in Wireless Relay Networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 2, pp. 323–330, 2012.

[11] L. Yuting and R. Deters, "Using cooperation to improve the experience of mobile Web Services consumers," in IEEE Asia-Pacific Services Computing Conference, 2009, 7-11 December, 2009, pp. 213-218.

[12] E. Hernandez-Orallo, M. Serrat, J. Cano, C. Calafate, and P. Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," *IEEE Commun. Lett.*, no. 99, pp. 1–4, 2012.

[13] D. Mathews, K. Ananda, and S. Radha, "Dynamic Pricing Approach for Cooperation Stimulation and QoS in Mobile Ad Hoc Networks," *Computational Science and Engineering, 2008. CSE'08. 11th IEEE International Conference on*, pp. 388–393, 2008.

[14] S. Buchegger and J. -Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in 3rd ACM International Symposium Mobile Ad Hoc Networking and Computing (MobiHoc), 2002, pp. 226–236.

[15] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in 6th IFIP TC6/TC11 Joint Working Conf. Communication Multimedia Security, 2002, pp. 107–121.

[16] Z. Safaei, M. Sabaei, and F. Torgheh, "An efficient reputation-based mechanism to enforce cooperation in MANETs," in *Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on*, 2009, pp. 1–6.

[17] K. Raychaudhuri and P. Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management," in International Journal of e-Health and Medical Communications, Vol. 1, no. 2, 2010, pp.12-23.

[18] U. Blumenthal, F. Maino and K. McClohrie, "The Advance Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security model," in RFC 3826, June 2004.

A Novel Cooperation Strategy for Mobile Health Applications

Bruno M. C. Silva[1], Joel J. P. C. Rodrigues[1], Ivo M. C. Lopes[1], Tiago M. F. Machado[1], and Liang Zhou[2]

[1] Instituto de Telecomunicações, University of Beira Interior, Portugal
[2] Nanjing University of Posts and Telecommunications, Nanjing, China
{bruno.silva; ivo.lopes; tiago.machado}@it.ubi.pt;{joeljr; liang.zhou}@ieee.org

Abstract

Mobile health (m-Health) proposes healthcare services delivering overcoming geographical, temporal, and even organizational barriers. Typical m-Health systems include the use of mobile applications that interact with caretakers. Mobile devices have several constraints (including processor, energy, and storage capacity) that affect the quality of service and user experience. M-Health paradigm of healthcare provides anytime and anywhere benefits with the advent of Web services based systems. The use of Web services on m-Health systems allows health applications available for users with mobility support. This paper proposes a cooperation strategy for m-Health services and applications. It follows a reputation-based strategy built for Web services oriented architectures including a cooperative Web service that manages all the network cooperation and nodes reputation. It includes two modules for mobile nodes, one is for verifying the cooperation status of neighbor nodes and another is for classifying the neighbor nodes in function of their cooperation with others (reputation). A performance evaluation study, in a real scenario, using an m-Health application, called *SapoFit,* is presented. Results comparison with an analytical model is also considered. It was shown that mobile nodes without Internet connectivity could use the application continuously. It also improves the service delivery probability and service average delay, increasing the overall network performance.

Index Terms: Mobile Health, m-Health, Mobile computing, e-Health, Cooperation

I. Introduction

Mobile health (m-Health) is considered the strongest contribution for the next generation e-Health systems and it is already changing typical healthcare services [1],[2]. The study and development of m-Health services and applications have been an important point of attention in the last years. Several research topics related to health have gathered important findings and contributions from m-Health, such as, cardiology [3],[4],[5], diabetes [6],[7], obesity [8],[9],[10], smoking cessation [11], among others. These different medical topics make use of m-Health applications essentially for monitoring, diseases prevention and detection, and, in more advanced services, also provide basic diagnosis. M-Health services are also becoming popular in developing countries [12],[13], where healthcare facilities are frequently remote and inaccessible. Figure 1 illustrates a typical m-health service architecture supported by Web services (WS). These WS are hosted on Web servers and can be used through network connectivity, including the Internet. Caretakers use various equipment, such as mobile devices, sensors, and specialized devices in applications.

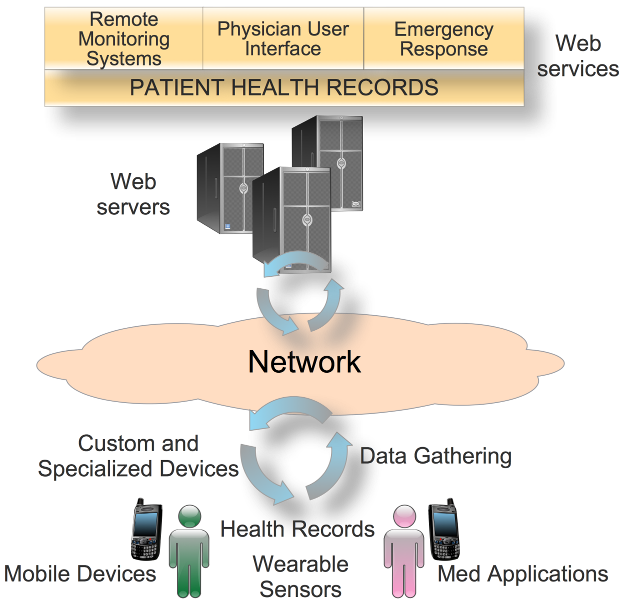


Figure 1. Illustration of an m-Health application framework based on Web Services.

These types of architectures based on mobile devices and wireless communications presents challenged issues taking into account several constraints, such as, battery and storage capacity, broadcast constrains, interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches may be viewed as a good solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability. Cooperation is a hot research topic that has been growing in recent years. With the advent of wireless networks, several recent studies present cooperation mechanisms and algorithms as a solution to improve wireless networks performance [14]. In the absence of a stable network infrastructure, mobile nodes cooperate with each other performing all networking functionalities. For example, it can support intermediate nodes forwarding packets between two distant nodes [15]. To the best of our knowledge, there are no cooperative solutions for m-Health services and applications. Then, this paper proposes a cooperation strategy for m-Health applications focusing on forwarding and retrieving data to/from nodes that have no direct connection to a m-Health application. In this sense, devices without Internet connection can use m-Health applications without problems. This cooperation approach presents a reputation-based strategy where a Web service manages all the cooperation among nodes and their reputation. It considers three main components: a *node control message,* a *network cooperative list,* and a *cooperative Web service* (CWS). The *control message* and the *cooperative list* are included in the mobile nodes requests for services, and record all cooperative and non-cooperative actions. The *CWS* includes a reputation table for all nodes and decides which nodes can have access to the requested services. The performance assessment and validation of the proposal is also considered. It proves the feasibility of this approach and also studies the impact of the cooperation strategy on the performance of an m-Health application taking into account different number of uncooperative nodes. The cooperation proposal is deployed and evaluated in a m-Health application for obesity prevention and control, called *SapoFit* [16],[17],[18]. Results show that mobile nodes without Internet connectivity can use the application continuously with success. It also shows the improvement of the service delivery probability and service average delay, increasing the overall network performance. The remainder of this paper is organized as follows. Section II elaborates on related work about the topic focusing on cooperation techniques that contribute to the proposed cooperation solution, namely, wireless, mobile ad-hoc, and delay-tolerant networks (DTNs). Section III describes the proposed m-Health cooperation strategy, while its performance evaluation and validation through a prototype with an m-Health application is presented in Section IV. This section also includes an analytical model and these results are compared with those from the experiments. Finally, Section V concludes the paper and points out the further research works.

I. Related Work

Cooperative mechanisms have proven to be a promising solution for several network constraints in wireless networks and important solutions have been presented in the literature [19],[20],[21],[22]. Due to the overall characteristics of m-Health architectures, this study mainly focuses on wireless and mobile ad-hoc networks (MANETs). The delay tolerant network (DTN) paradigm is also considered to solve network disconnection problems. These approaches have contributed to the refining of the cooperation proposal for m-Health applications.

ı) *Cooperation in wireless and mobile ad-hoc networks*

Energy saving is a major concern in the context of wireless networks with limited energy resources. Al-Kanj and Dawy [23] present an optimized energy efficient incentives will not get any service from the network. Virtual currency schemes assume that forwarding a message incurs in a cost to a node. Therefore, a non-cooperative node needs an incentive in order to forward messages of other nodes. *Nuglets* [28] and *Sprite* [29] are examples of popular systems that use virtual currency schemes. These systems use virtual payments to incentive nodes to forward messages and the payment is deducted from the sender or destination node.

Reputation schemes use the node reputation to diminish selfish behavior. All network nodes maintain the reputation of other nodes. Reputation is assessed by neighbor monitoring/observation or the exchange of reputation messages between nodes. Three popular reputation based schemes are the following: CONFIDANT [30] and CORE [31]. CONFIDANT detects and isolates non-cooperative nodes, compelling them to cooperate. Through passive observation nodes know all packets within a one-hop neighbor node. CONFIDANT scheme assents on four components per node: *a monitor,* where nodes locally monitor deviating behavior; a *trust manager* that makes decisions about providing or accepting route information; a *reputation system* that is basically the node reputation rating; and a *path manager* that according to the reputation system defines the paths to avoid malicious nodes.

CORE scheme uses collaborative monitoring and reputation mechanisms to stimulate cooperation among nodes. Basically, nodes that have a good reputation can use network services while nodes with a bad reputation, due to non-cooperative behaviors, do not have access to network services. For calculating a node reputation value, CORE defines three types of reputation: *subjective reputation,* calculated based on direct observation; *indirect reputation* which is calculated according to a second hand of information given by other nodes; and *functional reputation* that is calculated through a function that uses a weight in function of its importance.

a) Delay Tolerant Networks Paradigm and Cooperation techniques

In a Delay Tolerant Network (DTN) [32] scenario, network constraints (such as, limited storage capacity, limited network bandwidth, and limited energy) affect the network performance. Furthermore, the performance of a DTN is also affected by long or variable propagation delay, low node density, low transmission reliability, node mobility, and disruption. In such scenarios, node cooperation is a key issue to success. Nodes can cooperate with each other storing and forwarding interested data for all network nodes. DTN routing protocols usually assume a fully cooperative scenario. However, this is an unrealistic assumption. Nodes may not be able to always cooperate, due to resources limitations or even to a selfish behavior [33]. Therefore, several cooperation studies and proposals for DTNs have been presented and also offer contributions for the current proposal.

Shevade *et al.* [34] studies and demonstrates the degradation of a DTN performance due to selfish node behavior. The authors propose the use of practical and simple tit-for-tat (TFT) mechanism as an incentive strategy to stimulate cooperation. Through the TFT inclusion, the proposal assumes and guaranties that every node forwards as much traffic as possible for a neighbor node since the neighbor also forwards to it. Morillo-Pozo *et al.* [35] proposes a cooperation scheme for DTNs based on the cooperative ARQ (C-ARQ). This cooperation proposal reduces data losses in transmissions between fixed access points placed along the roads and passing by vehicles that buffer all the data. Basically, in areas that vehicles have no connectivity to access points, vehicles cooperate between them to increase the data delivery rate. The cooperation mechanism proposed in this paper gathered contributions from the above-described strategies in wireless, mobile ad-hoc, and delay tolerant networks.

III. Cooperation Strategy for Mobile Health Applications

This section describes, in detail, the cooperation approach for m-Healh applications. It is based on the following three modules: *i*) *a node control message*, *ii*) a *cooperative list*, and *iii*) a *cooperative Web service* (*CWS*).

a) Nodes control message and network cooperative list

The *control message* is exchanged when a node establishes contact with a neighbor node. This message tries to provide an awareness control of neighbor nodes knowing if they are willing to cooperate and in what conditions. It contains a *node ID*, *node status* (storage capacity, energy, and Internet connectivity), and its *cooperation status* (cooperative or uncooperative). An illustration a *node control message* and a *cooperative list* may be seen in Figure 2.

The *cooperative list* records all cooperative and uncooperative nodes during a service request. This list classifies all neighbor cooperative actions. It saves the *Node ID* and adds or subtracts a classification threshold according to the node *cooperation status*. Every node updates the *cooperative list* each time that a service is requested from an isolated node (a node without Internet connectivity).

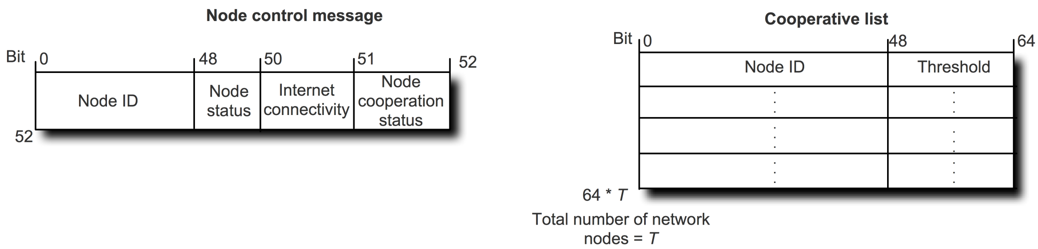


Figure 2. Illustration of a node control message and a cooperative list.

The *cooperative threshold list* (*CT*) starts at *0* (zero) and a unit (*1*) is added or subtracted according to the node *cooperation status* and *node status*. The *CT* influences directly de node reputation. Table I presents the correlation between the *node cooperation status*, the *node status*, its Internet connectivity and the resultant

CT. The node status is based on its storage capacity and energy lifetime. A node has three types of status: *poor, regular,* and *excellent.* It is assumed that a node is *poor* when the device storage capacity is over 95% or its available power energy is below 20%. The *regular* status occurs when a node storage capacity is under 95% and its power energy is between 20% and 80%. A node is in an *excellent* status when the node storage capacity is under 95% and its available power energy is over 80%. The *CT* ranges between *-2* and *+3*. This interval is assumed to guarantee that non-cooperative nodes with a low number of nodes are punished. Cooperative nodes in a *poor* status have the highest *CT* value (+3). Moreover, nodes in a *poor* status with either no storage capacity or low levels of battery, have a plausible justification for being uncooperative, therefore, they are not punished in their *CT* (0). The worst-case scenario for an uncooperative node is the one that is in *excellent* status with Internet connectivity and still refuses the cooperation. This node is punished with the worst *CT* value (equal to *-2).*

Table I. Correlation between the node cooperation status, the node status, its Internet connectivity, and the resultant CT classification

Node Status	Internet Connectivity	Cooperation State	CT
Poor	0	0	**0**
Poor	0	1	**+3**
Poor	1	0	**0**
Poor	1	1	**+3**
Regular	0	0	**-1**
Regular	0	1	**+2**
Regular	1	0	**-2**
Regular	1	1	**+2**
Excellent	0	0	**-2**
Excellent	0	1	**+1**
Excellent	1	0	**-3**
Excellent	1	1	**+1**

a) Cooperative Web Service and Reputation Table

The *cooperative Web service* (*CWS*) includes a node reputation table. To calculate nodes reputation, the *CWS* uses the node *cooperative lists*. It decides if the requesting node should have access to the m-Health application Web service or not, based on the node reputation. The reputation table lists all the network nodes with their respective reputation and current *cooperative threshold*. The threshold value available at the reputation table for node N is represented by C_N. Upon the CWS receives a request and the corresponding *cooperative list*, the service adds the *CT* value to the threshold in the reputation table for nodes listed in the cooperative list, i.e., $C_N = C_N + CT$. The reputation table considers three states of reputation: *selfish*, *cooperative* or *super-cooperative*. As may be seen in (1), these states are calculated considering the node C_N and an optimal interval of time that is based on the total number of networks nodes (*t*). For networks with reduced number of nodes, it is extremely important that uncooperative nodes receive worst *CT*, punishing and motivating them to cooperate. Therefore, half number of the network nodes to limit the interval for reputation states ($\frac{t}{2}$) is used.

$$Rep(N) = \begin{cases} Selfish,\ C_N \in \left]-\infty, -\frac{t}{2}\right[\\ Cooperative,\ C_N \in \left[-\frac{t}{2}, +\frac{t}{2}\right[\\ Super-Cooperative,\ C_N \in \left[+\frac{t}{2}, +\infty\right[\end{cases} \quad (1)$$

Based on nodes reputation, the CWS will not grant access and release any resource from the Web services to *selfish* nodes. *Selfish* nodes are punished by the CWS with an order to cooperate until the reputation reaches a *cooperative* state. The CWS releases resources to *cooperative* nodes, however, *super-cooperative* nodes have a maximum priority over the application resources in case of simultaneous requests.

The CWS also stores a list of all requests that where successfully answered. These requests are saved until its time-to-live (TTL) expires. The TTL is the average delay that takes a request to get answered by the Web service. This list avoids that previous requests from the same node are answered a second time.

A major concern in the proposal is the privacy issue of all forwarded and retrieved data. Privacy is a top priority issue in m-Health services that deal with user sensitive information. On m-Health applications several security issues must be considered, such as, personal information management, secondary use of personal information, improper use of personal information, and errors with stored personal information. Therefore, cryptographic mechanisms can be seen as a solution to guarantied data confidentiality and protection [36].

The presented cooperation strategy assumes secure data transactions among nodes using the Advanced Encryption Standard (AES) cipher algorithm used in Cipher Feedback Mode (CFB) with a key size of 128 bits [37].

IV Performance Evaluation

This section focuses on the performance evaluation and validation of the m-Health cooperation approach. First, the m-Health application (SapoFit) and corresponding network scenario used to evaluate and demonstrate the solution is introduced. Afterwards, the system validation and results are discussed. The performance metrics used in the study are the service requests delivery probability and service average delay. These metrics are the network challenges that proposed approach aims to improve.

a) SapoFit application

SapoFit is a weight control application that allows users to keep track of weight in a healthier and more practical way. SapoFit allows a user to control his/her weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility of following food plans based on his/her needed calories. In this m-Health application all the users must be registered in a Web service. Figure 3 presents three activities screenshots of SapoFit application: *Login*, *Plans*, and *Profile*. At the *Login* window the user enters his/her e-Mail address and corresponding password for authentication. After login, the application communicates with the Web service to obtain the personal user data (name, height, age, sex, weight, etc.). After loading all the data, they are displayed in a *Profile* window, which is the main window of SapoFit. At the *Plans* option, the calories factor that depends on the user target weight are presented. For the performance evaluation of the m-Health cooperation proposal, a user without Internet connection requesting access to the *Login* and *Plans* services is considered. Therefore, the user *Profile* will be totally obtained through cooperation among nodes.

Figure 3. Three activities of SapoFit with *Login*, *Food Plans*, and *User Profile* Screenshots.

a) M-Health network scenario

The real m-Health network scenario used for the performance evaluation study of the cooperative proposal may be seen in Figure 4. It includes eight mobile nodes (using *SapoFit),* assuming that three of them are uncooperative nodes. Node *M* is the single node with connection to the SapoFit Web services. Although an m-Health scenario presents high node mobility, for evaluation purposes, it is assumed the node positioned according to the presented network scenario. The activity diagram of a mobile node (for a mobile device with *SapoFit)* and its cooperation mechanisms are presented in Figure 5. From the given figure, node *A* (without Internet connection) tries to login *SapoFit* server application (authenticating at the *SapoFit* Web service too). The application starts searching for neighbor nodes using Bluetooth connection. Afterwards, the requester node receives the *node control message* from each neighbor node. According to theses messages, the *cooperative list* is updated and the request for login is sent together with the cooperative list to all the cooperative neighbor nodes. This process is repeated until finding a node (Node *M)* that is willing to cooperate and with Internet connectivity as well. When the request reaches a node in these conditions, the *cooperative Web service* will update the reputation table and evaluate the reputation of the requester node. If the node has a *selfish* reputation, the login request is discarded. If it has a cooperative reputation the request is allowed without priority. If it has a super-cooperative reputation, the request is allowed with maximum priority over other sent answers. The same cooperation procedures are followed while retrieving the login service answer, but instead of searching a node with Internet connectivity, it searches for the requester node *id.*

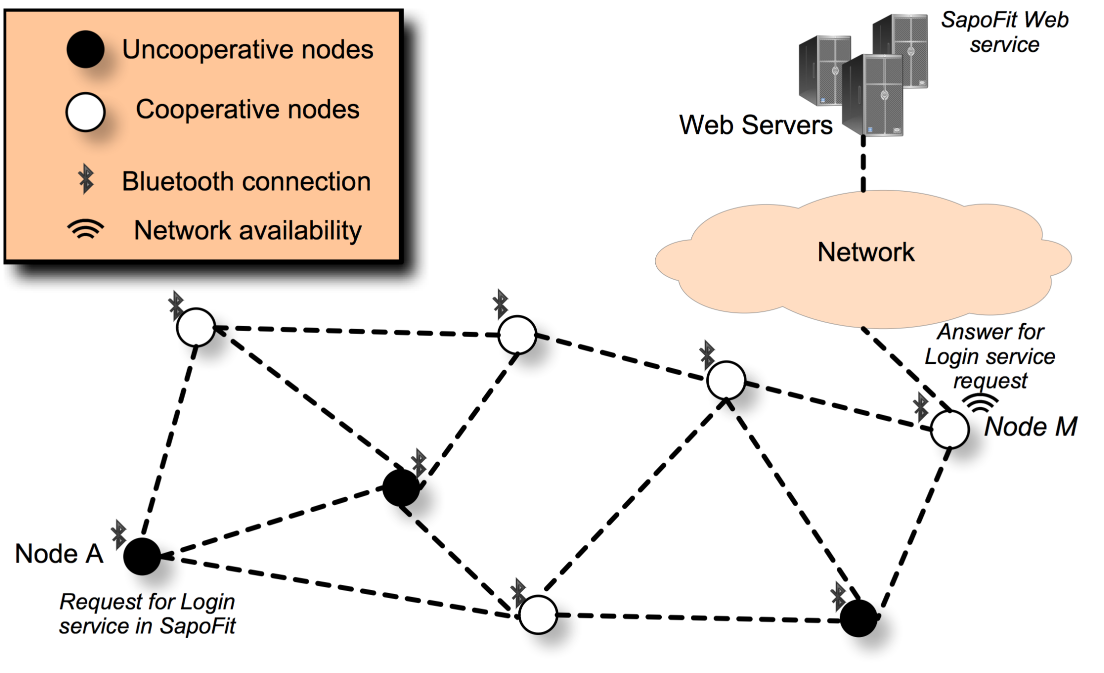


Figure 4. Illustration of the m-Health network scenario used for performance evaluation of the cooperation strategy.

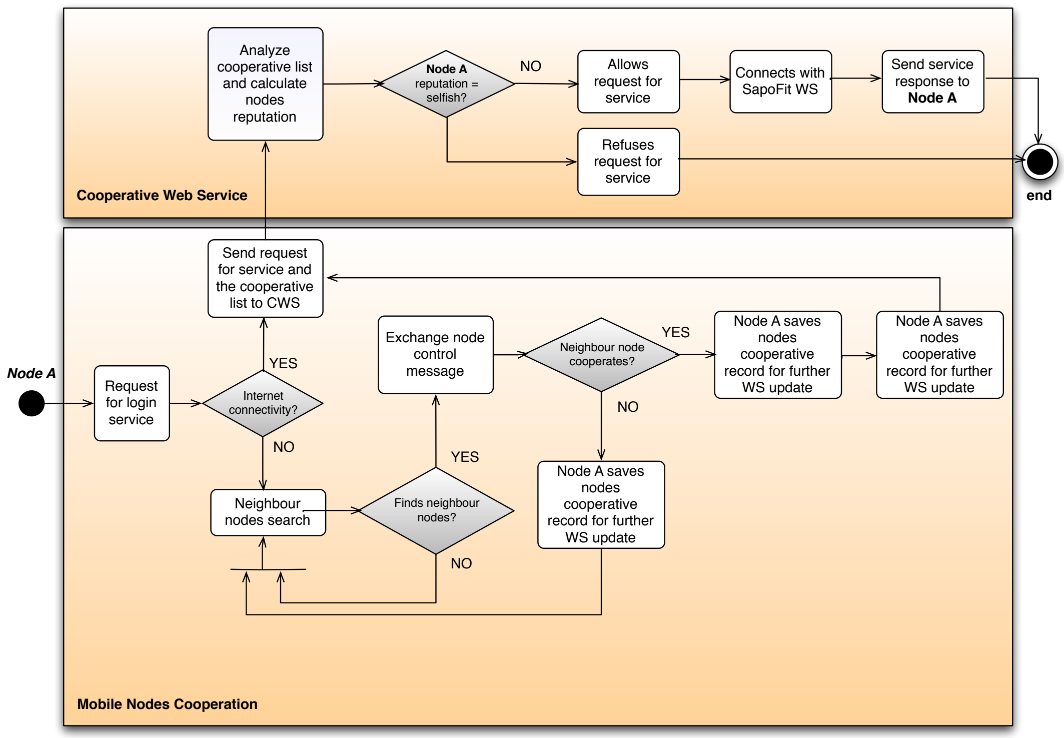


Figure 5. Activity diagram of a mobile node representing a mobile device with *SapoFit* and its cooperation mechanisms.

a) Performance Analysis

This section focuses on the performance analysis of the proposed cooperative strategy and its impact on the overall network performance. The study was performed through the above-described real prototype and each result represents an average of 30 experiments. The first and perhaps the most important analysis refers to the case where without the cooperation strategy, all devices with no Internet connectivity were unable to access the application Web services and therefore cannot use the m-Health application. Through cooperation all devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). The service delay is measured as the time between the request for the application service and its delivery. It was considered a worst-case scenario of three uncooperative nodes. The service delivery probability and the service average delay as function of the number of uncooperative mobile nodes are presented in Figure 6. As may be seen, when the number of uncooperative nodes increases, the service delivery probability decreases about 95, 88, 71, and 57 percent, respectively. As expected, the service average delay also presents the same behavior. Increasing the number of uncooperative nodes the service average delay increases 17.32, 26.1, 36.5, and 54.7 seconds, respectively. The maximum service delay observed with three uncooperative nodes was about 68.7 seconds.

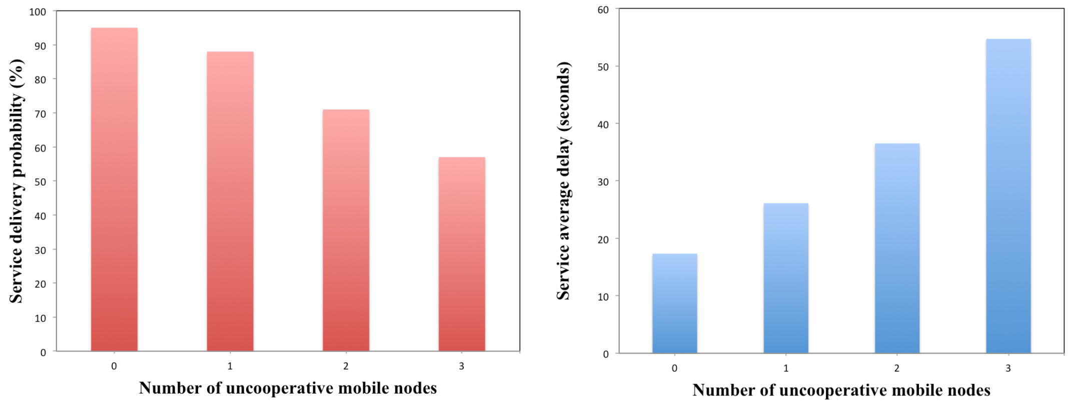


Figure 6. Service delivery probability and service average delay as function of the number of uncooperative mobile nodes.

For analysis of the service average delay results, an analytical model with two equations was used. Equations 2 and 3 calculate the maximum service delay and the service average delay, respectively.

$$Maximum\ service\ delay = (\alpha + \sigma + \varphi) \times Tc + (\alpha + \sigma) \times Tuc, \quad (2)$$

$$\text{Service Average delay} = (\alpha + \sigma + \varphi) \times \text{Tmin} + (\alpha + \sigma) \times \text{Tuc}, \quad (3)$$

where,

- $\alpha = Average\ connection\ establishment\ time = 3.6\ seconds$
- $\sigma = Average\ node\ control\ message\ transfer\ time = 0.43\ seconds$
- $\varphi = Average\ request\ for\ service + Cooperation\ List\ transfer\ time = 0.35\ seconds$
- $\beta = Average\ service\ response\ delivery\ time = 0.28\ seconds$
- $Tmin = Minimum\ required\ nodes\ for\ cooperation = 3\ nodes$
- $Tc = Total\ of\ cooperative\ nodes\ (variable)$
- $Tuc = Total\ of\ uncooperative\ nodes\ (variable)$

The maximum service delay obtained by (2) was about 59.8 seconds, slightly below that one obtained by real experiments. A comparison between the service average delay results from the real experiments and the results obtained by (3) are depicted in Figure 7. As may be seen, the observed results show slightly variances that increase with the number of uncooperative nodes. These variances were mainly caused by mobile devices constrains, such as loss of Bluetooth connection between nodes, distance variation, and different devices hardware specifications. However, this comparison results are satisfactory, proving the feasibility of the obtained results from the real experiments that clearly follows the behavior provided by (3).

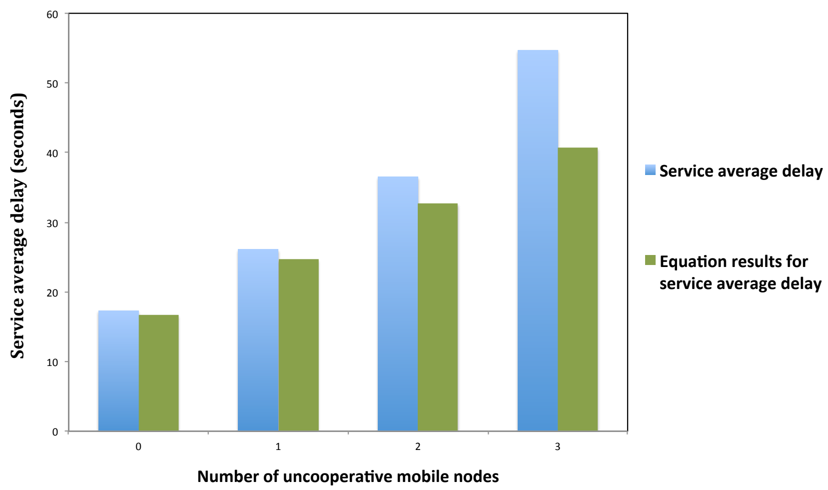


Figure 7. Performance comparison of the service average delay as function of the number of uncooperative mobile nodes considering results obtained by experiments and by the equation (3).

V Conclusion and Future work

This paper proposed a cooperation strategy for m-Health architectures following a Web service oriented approach. This approach presented a reputation-based strategy where a Web service manages all network cooperation. It considered three main modules: a node control message, a network cooperative list, and a cooperative Web service. Based on the m-Health services paradigm, available anytime and anywhere, the main objective of providing m-Health services and applications available in case of network unavailability was accomplished.

The proposed solution was evaluated and validated through a real m-Health prototype using the *SapoFit* m-Health application. The service delivery probability and the service average delay were the considered performance metrics. It was shown that proposed solution provides network connectivity to m-Health servers when Internet connection is not available since at minimum a node provides that connectivity to servers. It was evaluated the influence of the number of uncooperative nodes on the network performance. The results confirm that when the number of uncooperative nodes increases, both the service delivery probability and the service average delay also increases, as expected. An analytical model confirmed these results.

Through the network performance evaluation and its metrics comparisons, it was possible to conclude that the cooperation solution have improved significantly the overall performance and the quality of use of the m-Health application. Despite of some results variations due to high mobility patterns and limited laboratory environment, cooperation mechanisms have shown significantly improvements on the service quality, namely on the request for services probability and its average delay.

Refining the proposed strategy including the treatment of sensitive and priority medical information that is handled in a given m-Health application can be considered for future work. The performance evaluation of the m-Health cooperative proposal in more m-Health applications scenarios should also be considered.

References

[1] S. Akter and P. Ray, "mHealth - an Ultimate Platform to Serve the Unserved," in International Medical Informatics Association (IMIA), 2010, Year Book: 75-81.

[2] S. Tachakra, X. Wang, R. Istepanian, and Y. Song, "Mobile e-Health: the Unwired Evolution of Telemedicine," in Telemedicine Journal and e- Health, Vol. 9, pp. 247-257, 2003.

[3] G. Paré, K. Moqadem K, G. Pineau, and C. St-Hilaire, "Clinical Effects of Home Telemonitoring in the Context of Diabetes, Asthma, Heart Failure and Hypertension: A Systematic Review," in Journal of Medical Internet Research. Vol. 12, no. 2, URL: http://www.jmir.org/2010/2/e21/, 2010.

[4] J. Fayn and P. Rubel, "Toward a Personal Health Society in Cardiology," in IEEE Transactions on Information Technology in Biomedicine, Vol. 14, no. 2, 401-409, 2010.

[5] L. Chin-Teng, C. Kuan-Cheng, L. Chun-Ling, C. Chia-Cheng, L. Shao-Wei, and C. Shih-Sheng et al. "An Intelligent Telecardiology System Using a Wearable and Wireless ECG to Detect Atrial Fibrillation," in IEEE Transactions on Information Technology in Biomedicine. Vol. 14 no. 3, 726-733, 2010.

[6] A. Kollmann, M. Riedl, P. Kastner, G. Schreier, and B. Ludvik, "Feasibility of a Mobile Phone–Based Data Service for Functional Insulin Treatment of Type 1 Diabetes Mellitus Patients," in Journal of Medical Internet Research. Vol. 9, no. 5, 2007.

[7] S. G. Mougiakakou, *et al.* "SMARTDIAB: A Communication and Information Technology Approach for the Intelligent Monitoring, Management and Follow-

up of Type 1 Diabetes Patients," in IEEE Transactions on Information Technology in Biomedicine, Vol. 14, no.3, pp. 622-633, 2010.

[8] F. Zhu, M. Bosh, I. Woo, S. Kim, C. J. Boushey C., and D. S. Ebert, et al. "The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation," in IEEE Journal of Selected Topics in Signal Processing. Vol. 4, pp. 756 – 766, August 2010.

[9] J. P. Pollak, G. Gay, S. Byrne, E. Wagner, D. Retelny, and L. Humphreys "It's Time to Eat! - Using Mobile Games to Promote Healthy Eating," in IEEE Pervasive Computing. Vol. 9, 21-27, July-September, 2010.

[10] K. Patrick, et al. "A Text Message–Based Intervention for Weight Loss: Randomized Controlled Trial," in Journal of Medical Internet Research. Vol. 11, no. 2, 2009.

[11] R. Whittaker, E. Dorey, D. Bramley, C. Bullen, S. Denny, and C. R. Elley, et al. "A Theory-Based Video Messaging Mobile Phone Intervention for Smoking Cessation: Randomized Controlled Trial," in Journal of Medical Internet Research. Vol. 13, no. 1, 2011.

[12] S. Akter, J. D'Ambra, P. Ray, "User Perceived Service Quality of MHealth Services in Developing Countries: Research Paper," in European Conference on Information Systems (ECIS 2010). Pretoria, South Africa, 2010.

[13] D. Vatsalan,, et al. "Mobile Technologies for Enhancing eHealth Solutions in Developing Countries" In 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine (ETELEMED). 10-16 February, St. Maarten, Netherlands Antiles, pp. 84-89, 2010.

[14] Kramer, I. Marić, and R. Yates, "Cooperative communications," *Foundations and Trends in Networking,* vol. 1, no. 3-4, 2006.

[15] L. Buttyán and J-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," in Mobile Networks and Applications, Vol. 8, pp. 579-592, 2003.

[16] Bruno M. Silva, Ivo M. Lopes, Pradeep Ray, and Joel J.P.C. Rodrigues, "SapoFitness: A Mobile Health Application for Continuous Monitoring Dietary Evaluation", This proposal was presented at the IEEE HEALTHCOM 2011, Columbia, MO, USA, June 13-15, 2011.

[17] Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Bruno M. C. Silva, and Isabel de la Torre, "A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit", in Informatics for Health and Social Care, Informa Healthcare, 2012 (accepted for publication).

[18] SapoFit, http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8, (Assessed in December 2011).

[19] I. Maric and R. D.Yates, "Cooperative multi-hop broadcast for wireless networks," IEEE Journal of Selected Areas and Communications, Vol 22, no 6, August 2004, pp. 1080-1088.

[20] B. Sirkeci-Mergen and A. Scaglione, "On the power efficiency of Cooperative broadcast in dense wireless networks," IEEE Journal of Selected Areas and Communications, Vol 25, no 2, February 2007, pp. 497-507.

[21] G. Jakllari, S. V. Krishnamurthy, M. Faloutsos, and P. V. Krishnamurthy, "On broadcasting with cooperative diversity in multi-hop wireless networks," IEEE J. Selected Areas on Communications, vol. 25, no. 2, February 2007, pp. 484-496.

[22] Z. Han, Z. Ji, and K. J. R. Liu, "A cartel maintenance framework to enforce cooperation in wireless networks with selfish users," IEEE Transactions on Wireless Communications, vol 7, no 5, pp. 1889-1899, May 2008.

[23] L. Al-Kanj and Z. Dawy, “Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation,” in IEEE 17th International Conference on Telecommunications (ICT), 2010, 4-7 April, 2010, pp. 471-475.

[24] L. Yuting and R. Deters, “Using cooperation to improve the experience of mobile Web Services consumers,” in IEEE Asia-Pacific Services Computing Conference, 2009, 7-11 December, 2009, pp. 213-218.

[25] S. Corson and J. Macker, "Mobile Ad-hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," in RFC: 2501, 1999.

[26] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad-hoc networks," in Mobile Networks and Applications, Vol. 8, 2003, pp. 579-592.

[27] J. Hu and M. Burmester, “Guide to wireless ad-Hoc networks: Cooperation in Mobile ad-Hoc Networks,” in Computer Communications and Networks, S. Misra, I. Woungang, S. C. Misra (Eds.), ISBN: 978-1-84800-327-9, 2009, ch. 3, pp. 43-57.

[28] L. Buttyan, J.-P. Hubaux, “Nuglets: a Virtual Currency to Stimulate Cooperation in Self Organized Mobile Ad Hoc Networks,” Technical report No. DSC/2001.

[29] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: A simple, Cheat- proof, Credit-based System for Mobile Ad hoc Networks,” in Proceedings of IEEE Infocom 2003, San Francisco, CA, April 2003.

[30] S. Buchegger and J. -Y. L. Boudec, “Performance analysis of the CONFIDANT protocol,” in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc), 2002, pp. 226–236.

[31] P. Michiardi and R. Molva, “CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proc. 6th IFIP

TC6/TC11 Joint Working Conf. Communication Multimedia Security, 2002, pp. 107–121.

[32] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks", *Technical Report*, Standford University, 2003.

[33] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," in RFC 4838, April 2007.

[34] Vasco N. G. J. Soares and Joel J. P. C. Rodrigues, "Cooperation in DTN-Based Network Architectures," in *Cooperative Networking*, S. Misra and M. Obaidat (Ed.s), ISBN: 978-0-470-74915-9, Wiley, 2011, pp. 101-115.

[35] U. Shevade, H. H. Song, L. Qiu and Y. Zhang, "Incentive-Aware Routing in DTNs," in The 16th IEEE International Conference on Network Protocols (ICNP 2008), Orlando, Florida, USA, October 19–22, 2008, pp. 238–247.

[36] J. M. Pozo, O. Trullols, J. M. Barceló and J. G. Vidal, "A Cooperative ARQ for Delay-Tolerant Vehicular Networks," 38 in The 28th International Conference on Distributed Computing Systems (ICDCS 2008), Beijing, China, June 17 – 20, 2008, pp. 192–197.

[37] K. Raychaudhuri and P. Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management," in International Journal of e-Health and Medical Communications, Vol. 1, Nr. 2, 2010, pp.12-23.

[38] U. Blumenthal, F. Maino and K. McClohrie, "The Advance Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security model," in RFC: 3826, June 2004.