UNIVERSIDADE
BEIRA INTERIOR

Q-learning aplicado à protocolos MAC baseados em *Slotted* ALOHA para Redes de Sensores Sem Fios

Versão final após a defesa

Amilton Venâncio Baptista

Dissertação para obtenção do Grau de Mestre em
Engenharia Eletrotécnica e de computadores
(2º ciclo de estudos)

Orientador: Prof. Dr. Fernando José da Silva Velez

Dezembro de 2023

Declaração de Integridade

Eu, Amilton Venâncio Baptista, que abaixo assino, estudante com o número de inscrição M9987 de Mestrado em Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia, declaro ter desenvolvido o presente trabalho e elaborado o presente texto em total consonância com o **Código de Integridades da Universidade da Beira Interior**.

Mais concretamente afirmo não ter incorrido em qualquer das variedades de Fraude Académica, e que aqui declaro conhecer, que em particular atendi à exigida referenciação de frases, extratos, imagens e outras formas de trabalho intelectual, e assumindo assim na íntegra as responsabilidades da autoria.

Universidade da Beira Interior, Covilhã 27 /12 /2023

Dedicatória

Dedico este trabalho especialmente à minha mãe, Isabel Venâncio, cujo amor, apoio e dedicação foram pilares fundamentais em toda a minha caminhada. À sua força e determinação, devo grande parte das conquistas que alcancei. Ao meu pai, Barbosa Baptista (*In memoriam*), cuja memória e legado continuam a inspirar-me a cada dia. Embora já não esteja fisicamente entre nós, a sua presença é sentida em cada página, em cada linha de investigação, em cada desafio superado.

A ambos, com todo o meu amor e gratidão.

Agradecimentos

Em primeiro lugar, expresso minha eterna gratidão a Jeová Deus, o supremo criador, cujo amor e orientação me guiaram durante esta jornada. Em seguida, gostaria de manifestar minha mais profunda gratidão ao meu orientador, Prof. Dr. Fernando José da Silva Velez, por sua contínua orientação, paciência e apoio ao longo da elaboração deste trabalho. Sua dedicação, rigor e sabedoria foram fundamentais para a realização desta dissertação, e sou verdadeiramente grato por ter tido a oportunidade de aprender e crescer sob sua supervisão.

Agradeço aos meus familiares e aos meus irmãos Nelo, Ermelindo, Josimário, Luciana, Leandro, Barbosa, Nelson e Messias por sempre me proporcionarem força para concluir este feito. Ao meu querido tio Felisberto Dias por todo o suporte. Agradeço à minha querida companheira Ana Samara, pela motivação e incentivo. Agradeço também aos meus irmãos que a UBI me deu o privilégio de conhecer, ao Baptista Mandinda, António Baldé, Swellson Buché, Malam Mané e ao Óscar da Silva por toda a força e apoio neste trabalho. Agradeço ao meu mano Kiesse Mangaka e ao Moisés Ferreira (Maf One) por todo o apoio durante esta jornada muito importante na minha vida.

Pelos excelentes acolhimento, apoio e financiamento, agradeço ao Instituto de Telecomunicações. Este trabalho também foi financiado pela FCT/MCTES através de fundos nacionais e, quando aplicável, cofinanciado por fundos comunitários no âmbito do projeto UIDB/EEA/50008/2020.

À Universidade da Beira Interior e à incrível cidade da Covilhã, agradeço por me proporcionarem não apenas um ambiente de aprendizagem saudável e profissional, mas também uma segunda família que levarei comigo para sempre. A todos os meus irmãos de outra mãe da EIE12A e os da EEC que a UBI me deu, cada um de vocês tem um lugar especial no meu coração. Juntos, rimos, aprendemos e crescemos. Estes laços, forjados nos corredores, laboratórios e salas de aula, são eternos.

Por fim, mas não menos importante, quero agradecer a todos aqueles que, direta ou indiretamente, me apoiaram nesta caminhada. A todos os amigos, familiares e professores que acreditaram em mim, que me incentivaram nos momentos difíceis e que celebraram comigo cada conquista, o meu sincero obrigado.

Resumo

Nesta dissertação, abordamos um desafio crucial no âmbito das Redes de Sensores Sem Fios (RSSFs) baseadas no padrão IEEE 802.15.4: a eficiência energética, particularmente relevante diante do crescente interesse na expansão da Internet das Coisas (IoT). Em um cenário em que cidades inteligentes, agricultura de precisão e aplicações de saúde remota impulsionam a evolução da IoT, a eficiência energética dos nós sensores emerge como uma consideração crítica.

Nossa análise concentra-se nos protocolos de acesso ao meio existentes, com especial ênfase no *Carrier Sense Multiple Access* (CSMA), protocolo tradicionalmente adotado neste padrão. Em contrapartida, propomos a adoção e otimização do protocolo *Slotted* ALOHA como alternativa, visando superar as limitações identificadas nos protocolos convencionais e alinhando-se com os requisitos da IoT. Apresentamos variantes aprimoradas do *Slotted* ALOHA, incorporando técnicas como *Binary Exponential Backoff* (BEB) e aprendizado de reforço, nomeadamente o *Q-learning*. A implementação dessas melhorias visa não apenas otimizar o rendimento da rede, mas também aprimorar a eficiência energética, reduzir o atraso nas transmissões e proporcionar benefícios substanciais em diversas métricas operacionais, fundamentais para o sucesso da IoT.

Através de simulações no MATLAB, demonstramos que o *Slotted* ALOHA aprimorado com *Q-learning* oferece benefícios significativos em termos de consumo energético e redução do atraso, destacando-se como uma alternativa promissora ao CSMA para RSSFs na era da IoT. Essa contribuição não só avança na compreensão das dinâmicas de eficiência energética, mas também propõe soluções práticas e inovadoras para otimizar o desempenho global das RSSFs em ambientes diversos e desafiadores.

Palavras-chave

Redes de Sensores Sem Fios (RSSFs); IEEE 802.15.4; Internet das Coisas (IoT); *Slotted* ALOHA; *Q-learning*; Eficiência Energética; *Carrier Sense Multiple Access* (CSMA); *Binary Exponential Backoff* (BEB).

Abstract

In this dissertation, we address a crucial challenge in the context of Wireless Sensor Networks (WSNs) based on the IEEE 802.15.4 standard: energy efficiency, particularly relevant given the growing interest in the expansion of the Internet of Things (IoT). In a scenario where smart cities, precision agriculture, and remote health applications drive the evolution of IoT, the energy efficiency of sensor nodes emerges as a critical consideration.

Our analysis focuses on existing medium access protocols, emphasizing Carrier Sense Multiple Access (CSMA), a protocol traditionally adopted in this standard. Conversely, we propose adopting and optimizing the Slotted ALOHA protocol as an alternative to overcome identified limitations in conventional protocols and align with IoT requirements. We present enhanced variants of Slotted ALOHA, incorporating techniques such as Binary Exponential Backoff (BEB) and reinforcement learning, notably Q-learning. The implementation of these improvements aims not only to optimize network performance but also to enhance energy efficiency, reduce transmission delay, and provide substantial benefits in various operational metrics, crucial for IoT success.

Through simulations in MATLAB, we demonstrate that Slotted ALOHA enhanced with Q-learning offers significant benefits in energy consumption reduction and delay reduction. It is a promising alternative to CSMA for WSNs in the IoT era. This contribution advances the understanding of energy efficiency dynamics and proposes practical and innovative solutions to optimize the overall performance of WSNs in diverse and challenging environments.

Keywords

Wireless Sensor Networks (WSNs); IEEE 802.15.4; Internet of Things (IoT); Slotted ALOHA, Q-learning, Energy Efficiency, Carrier Sense Multiple Access (CSMA), Binary Exponential Backoff (BEB).

Índice

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

5G - Quinta geração
6LoWPAN - *IPv6 over Low-Power Wireless Personal Area Networks*
A/D - *Analog/Digital*
AR – Aprendizado de Reforço (em inglês, *Reinforcement Learning*)
BEB - *Binary Exponential Backoff*
BLE - *Bluetooth Low Energy*
CSMA - *Carrier Sense Multiple Access*
CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance*
CSMA/CD - *Carrier Sense Multiple Access with Collision Detection*
DC/AC - *Direct Current/Alternating Current*
FDMA - *Frequency Division Multiple Access*
IEEE - *Institute of Electrical and Electronics Engineers*
IoT - *Internet of Things*
ISM - *Industrial, Scientific, and Medical*
LoraWAN - *Long Range Wide Area Network*
M2M - *Machine-to-Machine*
MAC - *Medium Access Control*
MDP - *Markov Decision Process*
PAN - *Personal Area Network*
PSK - *Phase Shift Keying*
QAM - *Quadrature Amplitude Modulation*
RAM - *Random Access Memory*
RL - *Reinforcement Learning*
ROM - *Read-Only Memory*
RSSFs - Redes de Sensores Sem Fio
TDMA - *Time Division Multiple Access*
Wi-Fi - *Wireless Fidelity*
WLAN - *Wireless Local Area Network*
WMAN - *Wireless Metropolitan Area Network*
WPAN - *Wireless Personal Area Network*
WWAN - *Wireless Wide Area Network*

Capítulo 1

1. Introdução

1.1. Contextualização

Com o surgimento da Internet das Coisas (IoT, do inglês, *Internet of Things*), o mundo moderno tem testemunhado uma revolução na forma como os dispositivos comuns se comunicam entre si. Essa transformação vai além de ser apenas uma ideia e se torna uma realidade, onde objetos do nosso quotidiano estão cada vez mais conectados à internet, coletando e trocando dados de forma contínua [1]. Dentro desse amplo mundo da IoT, as Redes de Sensores Sem Fios (RSSFs) desempenham um papel crucial, atuando como a base para a obtenção de dados em tempo real em diversos cenários, desde as áreas urbanas até complexos industriais [2]. No meio dessa transformação, o padrão IEEE 802.15.4 se destaca. Com seu *design* voltado para comunicações que exigem baixas taxas de transmissão de dados e priorizam a eficiência energética. Esse padrão adotou o protocolo CSMA como a principal estratégia para controlar o acesso ao meio [3].

1.2. Motivação

Nos últimos anos, temos presenciado um crescimento exponencial da Internet das Coisas (IoT) e, com ela, um aumento no número de dispositivos conectados globalmente. Estima-se que, até 2030, vai existir cerca de 29 bilhões de dispositivos IoT conectados em todo o mundo [4]. Muitos desses dispositivos pertencem a Redes de Sensores Sem Fios (RSSFs) e são fundamentais para aplicações críticas que vão desde monitoramento de saúde, gestão de recursos hídricos, agricultura inteligente até cidades inteligentes [5].

Esses dispositivos, em muitos casos, são alimentados por baterias e colocados em locais remotos onde a substituição frequente de baterias não é viável. Assim, a eficiência energética torna-se um fator crucial para garantir uma operação prolongada desses sensores [6], [7]. Dado este contexto, os protocolos de acesso ao meio, que determinam como os dispositivos comunicam entre si e com a rede central, desempenham um papel vital. Ou seja, escolhas inadequadas ou ineficientes nesse domínio podem resultar em um consumo energético elevado, diminuindo significativamente a vida útil do nó sensor.

O CSMA, como protocolo MAC, já é amplamente adotado ou usado em diversas implementações de RSSFs, particularmente no padrão IEEE 802.15.4. No entanto,

outros protocolos como o *Slotted* ALOHA, por sua simplicidade e robustez, surgem como alternativas promissoras. Entretanto, é fundamental ponderar suas características, vantagens e desvantagens em comparação com o CSMA e outros protocolos consolidados [8]. Portanto, este estudo visa em mergulhar nessa análise, estudar não só apenas o *Slotted* ALOHA em sua forma original, mas também explorando melhorias potenciais através de algumas técnicas avançadas, como o *Binary Exponential Backoff* (BEB) e modelos de aprendizado de reforço (RL, do inglês, *Reinforcement Learning*), como o *Q-learning*.

1.3. Declaração do problema

Protocolos MAC eficientes desempenham um papel importante no gerenciamento de acesso ao canal e na prevenção de conflitos durante a transferência de dados em redes RSSFs. O acesso e uso do meio de comunicação pelos dispositivos nessas redes são definidos pelos protocolos MAC (*Medium Access Control*), sendo assim indispensáveis. Apesar das vantagens apresentadas pelo *Slotted* ALOHA, como a simplicidade e previsibilidade, uma avaliação cuidadosa de suas limitações se torna crucial particularmente quando realizado um paralelo com outros protocolos amplamente utilizados como o CSMA (*Carrier Sense Multiple Access*) - o protocolo amplamente utilizado no padrão IEEE 802.15.4.

1.4. Objetivos

O objetivo principal desta dissertação é estudar as características do *Slotted* ALOHA e descobrir como técnicas avançadas, como o *Binary Exponential Backoff* (BEB) e *Q-learning*, podem ser harmonizadas com o protocolo para reforçar sua eficiência energética e capacidade de adaptação em diferentes cenários de redes de sensores sem fios baseados no padrão IEEE 802.15.4. dentre eles alguns pontos, como:

- Avaliar o desempenho do *Slotted* ALOHA nas Redes de Sensores Sem Fios.
- Comparar o desempenho do *Slotted* ALOHA e CSMA em termos de eficiência energética, taxa de pacotes entregue acumulados e latência.
- Explorar e implementar melhorias no *Slotted* ALOHA utilizando técnicas como *Binary Exponential Backoff* (BEB) e *Q-learning*.
- Avaliar o desempenho das variantes aperfeiçoadas do *Slotted* ALOHA em diferentes cenários de RSSFs, enfatizando sua adaptabilidade e eficiência.

1.5. Justificativa

À medida que o mundo se torna mais digitalizado, a demanda por Redes de Sensores Sem Fios (RSSFs) cresce, com aplicações variando de cidades inteligentes a otimizações na agricultura e indústria através da IoT. A eficiência energética é primordial, visto que muitos sensores operam com baterias em locais de difícil acesso, tornando a manutenção desafiadora. Os protocolos MAC, como o *Slotted* ALOHA, são fundamentais para otimizar o consumo de energia nas comunicações. Este estudo se propõe a investigar ou estudar mecanismos para aprimorar o *Slotted* ALOHA, contrastando-o com outros protocolos estabelecidos, como o CSMA, visando identificar suas vantagens e limitações no contexto de eficiência energética nas RSSFs baseadas no padrão IEEE 802.15.4. Este estudo tem potencial para direcionar futuros desenvolvimentos em RSSFs, beneficiando múltiplas aplicações e, consequentemente, a sociedade em geral.

1.6. Delimitação do estudo

Apesar da grande diversidade nas RSSFs e nos protocolos MAC existentes, este estudo está concentrado na análise do *Slotted* ALOHA juntamente com suas variações comparadas ao CSMA. A decisão de utilizar o padrão IEEE 802.15.4 como base se deve à sua relevância e alto nível de aceitação em aplicações de RSSFs. Além disso, algumas técnicas para aprimoramento como o *Binary Exponential Backoff* (BEB) e o *Q-learning* também serão estudados. No entanto, para preservar o foco na pesquisa, alguns aspetos e variantes de outros padrões não serão explorados em detalhe, para manter uma profundidade adequada na análise proposta.

1.7. Contribuições

Nesta dissertação, mergulhamos profundamente no desafio de aprimorar o protocolo *Slotted* ALOHA em redes RSSFs baseadas no padrão IEEE 802.15.4. Utilizando técnicas modernas, como o *Binary Exponential Backoff* (BEB) e o *Q-learning*, conseguimos não só melhorar a eficiência energética do protocolo, mas também sua adaptabilidade em ambientes variáveis. Ao realizar *benchmarking* detalhado, pôde-se contrastar o desempenho aprimorado do *Slotted* ALOHA com protocolos estabelecidos, como o CSMA, destacando as vantagens do nosso método. A pesquisa também trilha caminhos inovadores ao introduzir o aprendizado de máquina (ML, do inglês, *Machine Learning*) nas RSSFs, sugerindo novas possibilidades para otimizações futuras. As conclusões, fundamentadas em simulações, têm implicações significativas para investigadores e engenheiros da área, oferecendo *insights* e diretrizes para futuras implementações.

1.8. Estrutura da dissertação

Esta dissertação é composta por 5 capítulos e estruturada de forma a fornecer uma compreensão aprofundada do tema, abordando-o de maneira sistemática e lógica. A seguir, apresenta-se a organização dos capítulos:

1. **Introdução**: Este capítulo estabelece a base da pesquisa, apresentando a contextualização, motivação, declaração do problema, objetivos, justificativa, delimitação do estudo e as contribuições esperadas.
2. **Revisão de Literatura**: Constitui-se como a base teórica do trabalho, onde é realizada uma revisão aprofundada sobre as Redes de Sensores Sem Fios (RSSFs), o padrão IEEE 802.15.4, o impacto da Internet das Coisas (IoT) e uma análise dos Protocolos MAC com enfoque na eficiência energética.
3. ***Binary Exponential Backoff* e Aplicação do *Q-learning* em RSSFs**: Aborda dois métodos essenciais para a melhoria da eficiência energética em RSSFs baseadas no padrão IEEE 802.15.4. Aqui, são discutidos os princípios e benefícios do *Binary Exponential Backoff* (BEB), bem como uma introdução ao aprendizado por reforço e a integração do *Q-learning* ao *Slotted* ALOHA.
4. **Análise e Discussão dos Resultados**: Este capítulo concentra-se em apresentar e analisar os resultados obtidos através das simulações realizadas. São detalhados cenários específicos de implementação e avaliação das métricas propostas.
5. **Conclusão e Trabalhos Futuros**: Finalizando a dissertação, este capítulo condensa as principais conclusões da pesquisa, e também sugere direções para investigações futuras na área.

Capítulo 2

2. Revisão de literatura

2.1. Redes Sem Fios e RSSFs: Uma Perspetiva Geral

Desde os primórdios das transmissões via rádio no começo do século XX, que as redes sem fio têm revolucionado nossa maneira de nos comunicar e interagir com o mundo que está à nossa volta. Ao demonstrar a possibilidade de enviar sinais pelo Atlântico, ***Guglielmo Marconi*** se destacou como um dos grandes inovadores na área da comunicação [9], [10].

As redes sem fios são redes de comunicação que permitem a conectividade entre vários dispositivos sem o uso de cabos físicos [10]. Esses tipos de redes baseiam-se em vários padrões de tecnologias e são utilizadas para fornecer acesso à internet, voz, dados para dispositivos móveis e IoT [1]. Existem vários tipos de redes sem fios, algumas delas apresentadas na figura 2.1.

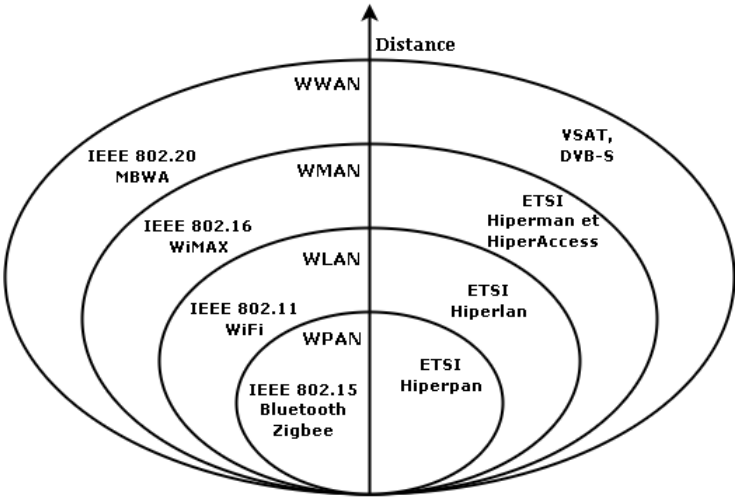

Figura 2.1 – Diferentes tipos de redes sem fios.

Tecnologia e frequência de uso

Ao longo dos anos, as redes sem fios têm assumido um papel importante no domínio das comunicações. Uma análise às tecnologias e frequências em uso evidencia a evolução e versatilidade destes sistemas.

Uma das características mais marcantes das redes sem fios é a sua dependência de bandas de frequência específicas. A banda ISM (*Industrial, Scientific and Medical*) é particularmente notável, dada a sua adoção generalizada em diversas aplicações de comunicação sem fios. Isto abrange frequências como 2,4 GHz e 5 GHz, reconhecidas pelo seu emprego em tecnologias populares como Wi-Fi e Bluetooth [9], [11].

A opção por estas frequências não é aleatória, resulta de um equilíbrio entre capacidade de transmissão de dados, alcance e habilidade para ultrapassar obstáculos [10]. Por exemplo, a frequência de 2,4 GHz é apreciada em muitas aplicações domésticas devido à sua eficiência em ultrapassar paredes e outros obstáculos. Contrariamente, a frequência de 5 GHz, embora ofereça uma capacidade superior de transmissão de dados, tem um alcance mais circunscrito e revela-se mais suscetível a obstruções.

Também é importante notar que estas frequências foram desreguladas para uso sem necessidade de licença, incentivando um vasto leque de inovações e aplicações. Contudo, tal liberalização trouxe consigo desafios. Face à saturação destas bandas, especialmente a de 2,4 GHz [11], emergiu a necessidade de desenvolver técnicas avançadas de gestão de espectro, modulação e codificação, com o objectivo de assegurar comunicações fiáveis.

Modulação e propagação em ambientes sem fios

A modulação e propagação de sinais são duas das áreas mais cruciais nas comunicações sem fios. Entender ambos os conceitos são vitais para garantir a transmissão eficiente e fiável da informação em ambientes adversos.

a. **Modulação:** A modulação refere-se ao processo pelo qual a característica de uma onda portadora (normalmente uma onda senoidal) é alterada de acordo com o sinal de informação que se deseja transmitir. Em ambientes sem fios, a modulação é crucial porque permite a transmissão eficiente de sinais de informação sobre uma onda portadora de alta frequência, que pode então ser transmitida através do espaço. Existem vários esquemas de modulação em uso hoje, com destaque para o QAM (Modulação de Amplitude em Quadratura) e o PSK (Modulação por Deslocamento de Fase) [12][13], [14]. Estes esquemas são projetados para maximizar a eficiência espectral, permitindo a transmissão de mais informações em menos largura de banda.

b. **Propagação:** Uma vez modulado, o sinal é transmitido através do ar, onde enfrenta diversos desafios, incluindo reflexões, refrações, difração e dispersão. Estes fenómenos podem causar interferência, desvanecimento e atrasos, todos os

quais podem degradar a qualidade do sinal recebido. A propagação em ambientes sem fios é, portanto, altamente imprevisível, e muitos fatores, incluindo obstáculos (como edifícios e árvores), a atmosfera e até mesmo fenómenos naturais, podem afetar a forma como um sinal se propaga. Modelos de propagação, como o modelo de perda de percurso, têm sido desenvolvidos para prever o comportamento do sinal em vários ambientes, e são essenciais para o *design* e planeamento de redes sem fios [12].

Vantagens e limitações das redes sem fios

As redes sem fios surgiram como uma solução inovadora para problemas de comunicação, oferecendo uma série de vantagens em comparação com os sistemas tradicionais baseados em cabos. Entre estas vantagens, destacam-se:

- Mobilidade: Uma das características mais marcantes das redes sem fios é a capacidade de manter dispositivos conectados em movimento. Isto abriu portas para novas formas de interação, desde a simples navegação na *web* até aplicações industriais onde sensores móveis coletam dados em tempo real [5].

- Flexibilidade de instalação: Sem a necessidade de instalar cabos, as redes sem fios são frequentemente mais fáceis e rápidas de serem configuradas, tornando-as ideais para eventos temporários, obras ou locais de difícil acesso [15].

- Escalabilidade: As redes sem fios, especialmente aquelas baseadas em padrões modernos, são projetadas para suportar um grande número de dispositivos. Isso torna mais fácil expandir a rede conforme a necessidade, sem a complexidade e custo de adicionar infraestrutura física [1].

No entanto, juntamente com estas vantagens, existem também algumas limitações e desafios associados às redes sem fios:

- Interferência e congestionamento: As redes sem fios operam em frequências que, muitas vezes, são partilhadas por múltiplos dispositivos e serviços. Isso pode levar a interferências, resultando em redução de desempenho ou falhas de conexão [16].

- Segurança: A natureza aberta das transmissões sem fios torna-as potencialmente vulneráveis a escutas indesejadas ou ataques mal-intencionados. Garantir a integridade e confidencialidade dos dados é um desafio contínuo [17].

- Alcance limitado: Embora a tecnologia esteja sempre a avançar, o alcance das redes sem fios ainda é geralmente inferior ao das redes com fio, especialmente em ambientes com muitos obstáculos ou interferências [18].

2.1.1. Características e desafios das RSSFs

A emergência das Redes de Sensores Sem Fios (RSSFs) mudou o paradigma da coleta e processamento de dados em diversas aplicações, desde monitorização ambiental até aplicações em cuidados de saúde. Estas redes baseiam-se em pequenos dispositivos denominados "nós sensores" que têm a capacidade de capturar, processar e transmitir informações sobre o seu ambiente [19] – [21]. Mas o que constitui um nó sensor sem fio? E quais são os seus componentes fundamentais?

Componentes principais de um nó sensor:

a. Módulo de detecção: Este componente é a razão de ser de qualquer nó sensor. É responsável por converter estímulos físicos ou químicos, como luz, temperatura ou movimento, em sinais elétricos que podem ser processados digitalmente [19], [21].

b. Unidade de processamento: Uma vez que o estímulo é convertido em um sinal elétrico, este sinal é processado, muitas vezes localmente, para extrair informações relevantes ou para a compressão de dados, de forma a otimizar as transmissões e economizar energia [21].

c. Armazenamento: Os nós sensores podem necessitar de armazenar dados temporariamente, seja devido a condições adversas na rede (como congestionamento) ou para realizar análises mais robustas no próprio dispositivo [19].

d. Transmissor/receptor: Este é o componente que permite a comunicação sem fios do nó sensor com outros dispositivos na rede, como outros nós sensores ou estações base.

e. Fonte de energia: Muitos nós sensores são desenhados para serem autónomos, contando com baterias ou métodos alternativos, como células solares ou aproveitamento de energia cinética, para operar [12].

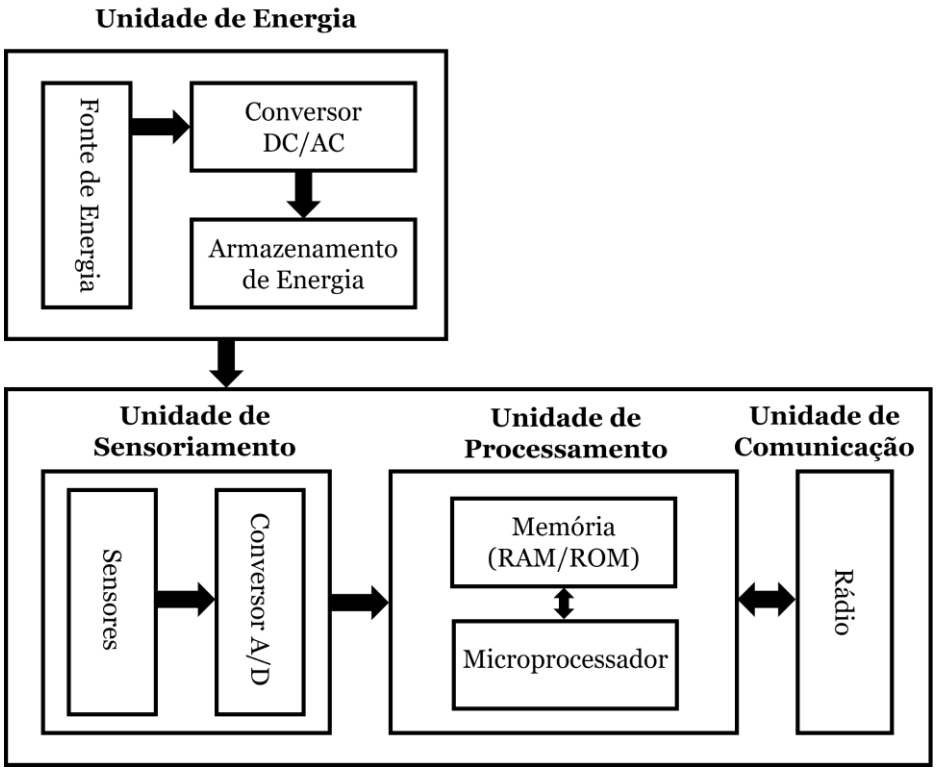

Figura 2.1.1 - Principais unidades de um nó sensor

Desafios:

A miniaturização é um dos principais desafios na conceção de sensores sem fios. Com aplicações que necessitam de uma implantação discreta ou em locais de difícil acesso, o tamanho e o peso tornam-se críticos. Contudo, esta miniaturização não pode comprometer a funcionalidade ou a durabilidade do nó sensor. A eficiência energética também é primordial [22]. Considerando que muitos nós sensores são implantados em locais remotos ou inacessíveis, a troca de baterias pode não ser viável. Assim, maximizar a vida útil da bateria e explorar fontes alternativas de energia é essencial.

Tipos de RSSFs: Estruturadas e Não-estruturadas

As Redes de Sensores Sem Fios (RSSFs) surgiram como uma tecnologia revolucionária para facilitar a monitorização e controle em vários domínios, desde a agricultura inteligente até cidades conectadas [23]. Essas redes são compostas por pequenos dispositivos de sensor que têm a capacidade de recolher dados do ambiente e transmiti-los através de comunicações sem fios. No entanto, a forma como esses nós sensores são organizados e interconectados pode variar, resultando em duas categorias principais: RSSFs estruturadas e RSSFs não-estruturadas.

a. **RSSFs Estruturadas:** Estas redes têm uma organização topológica previamente definida. Geralmente, são planeadas e têm uma configuração fixa com um padrão regular de nós. Uma característica fundamental destas redes é que elas podem ser facilmente geridas devido à sua estrutura predefinida. Em aplicações como monitorização agrícola ou gestão de tráfego urbano, onde os parâmetros de monitorização são fixos e não variáveis com o tempo, as RSSFs estruturadas são frequentemente preferidas. Além disso, devido à sua natureza determinística, são muitas vezes mais fáceis de projetar em termos de conectividade, cobertura e consumo energético [19], [22].

b. **RSSFs Não-estruturadas:** Estas redes, ao contrário das estruturadas, formam-se de maneira *ad-hoc*. Não têm uma organização topológica predefinida e podem mudar a sua configuração com base nas condições do ambiente ou necessidades da aplicação. São mais flexíveis e adaptáveis a ambientes dinâmicos. Imagine uma situação de resgate pós-desastre onde sensores são rapidamente dispersos numa área afetada para avaliar os danos ou encontrar sobreviventes [22], [24]. Neste caso, uma rede *ad-hoc* não-estruturada seria mais adequada devido à sua capacidade de se adaptar rapidamente a novas situações. No entanto, estas redes podem ser mais desafiantes em termos de gestão, otimização e garantia de conectividade constante.

Desafios de conectividade e cobertura em RSSFs

A conectividade e a cobertura são componentes cruciais na eficácia das Redes de Sensores Sem Fios (RSSFs) [19]. A sua importância advém da necessidade de garantir que todos os sensores na rede possam comunicar-se efetivamente, assim como de garantir que a área monitorizada seja coberta de forma adequada.

- Densidade dos nós sensores e a conectividade: A densidade dos nós sensores numa RSSF tem um impacto direto na conectividade. Se houver demasiados nós sensores numa área específica, podem ocorrer colisões, ou seja, dois ou mais nós sensores podem tentar comunicar ao mesmo tempo, levando a falhas na transmissão de dados. Por outro lado, se a densidade for muito baixa, podem surgir lacunas na conectividade, com alguns nós sensores sendo incapazes de comunicar com os seus nós sensores vizinhos ou com um ponto central (nó *sink*), como uma estação-base. Estas situações podem ser agravadas se os nós sensores estiverem sujeitos a falhas ou se a sua energia se esgotar [24].

- Presença de obstáculos e a cobertura: A presença de obstáculos físicos, como edifícios ou árvores, pode influenciar significativamente a cobertura da rede. Estes obstáculos podem atenuar ou bloquear completamente o sinal, levando a zonas sem cobertura na área pretendida. Por isso, a topologia da rede e a localização dos nós sensores tornam-se fatores críticos no projeto de uma RSSF eficaz [24], [25]. As soluções para mitigar estes desafios incluem a utilização de algoritmos avançados de roteamento ou a colocação estratégica de nós em locais elevados ou sem obstáculos.

- Considerações ambientais: As condições ambientais, como humidade, temperatura e fenómenos atmosféricos, também podem influenciar a conectividade e a cobertura [25]. Por exemplo, a humidade pode atenuar o sinal de rádio, enquanto temperaturas extremas podem afetar o desempenho da bateria dos sensores, limitando assim a sua vida útil.

Desta forma, garantir uma conectividade contínua e uma cobertura adequada são desafios fundamentais em RSSFs. Estes desafios requerem uma combinação de *hardware* robusto, algoritmos de roteamento eficientes e um planeamento cuidadoso.

Limitações energéticas e soluções de *harvesting*

As RSSFs têm transformado várias áreas, desde a monitorização ambiental até aplicações em cidades inteligentes. Contudo, um dos principais desafios na implementação e manutenção dessas redes é o consumo de energia. Sensores, geralmente, são alimentados por baterias com vida útil finita. Com o tempo, a troca ou recarregamento destas baterias, especialmente em ambientes remotos ou inacessíveis, pode ser logisticamente desafiador e economicamente inviável. A eficiência energética nos sensores torna-se, portanto, crucial [26]. Cada transmissão, recepção, processamento de dados ou até mesmo o estado ocioso de um nó sensor consome energia. Portanto, uma gestão energética adequada é necessária para maximizar a vida útil da rede. Esquemas de gestão de energia, como o *duty cycling*, onde os sensores alternam entre estados de vigília e sono, são frequentemente empregues [27].

No entanto, uma abordagem ainda mais promissora para enfrentar este desafio é o "*energy harvesting*", que se refere à capacidade de captar e armazenar energia do ambiente [27]. Existem várias fontes potenciais para isso, incluindo, energia solar, energia térmica, energia cinética, energia de radiofrequência (RF) entre outras. Estas soluções de *harvesting*, quando combinadas com estratégias de gestão de energia,

podem não só prolongar significativamente a vida útil de uma RSSF [26], mas em alguns casos, torná-la praticamente autónoma do ponto de vista energético.

Problemas de segurança e privacidade em RSSFs

À medida que as Redes de Sensores Sem Fios (RSSFs) ganham mais relevância em diversos domínios, desde aplicações industriais a ambientes domésticos, torna-se imperativo assegurar que estas redes sejam seguras e confiáveis [28]. As especificidades das RSSFs levantam preocupações únicas em termos de segurança e privacidade, que não são comuns em redes tradicionais.

- Natureza distribuída e falta de infraestrutura centralizada: A topologia *ad-hoc* e distribuída de muitas RSSFs torna-as suscetíveis a ataques e falhas. Na ausência de uma entidade central de coordenação, torna-se desafiante manter a integridade da rede e garantir que os sensores comuniquem de forma segura [29].

- Limitações de recursos: Os nós sensores em RSSFs são frequentemente restritos em termos de energia, capacidade de processamento e armazenamento [29]. Isso significa que a implementação de soluções de segurança robustas, que normalmente requerem algoritmos computacionalmente intensivos, pode ser problemática.

- Ataques maliciosos: As RSSFs estão expostas a uma variedade de ameaças, como o ataque do tipo "homem-do-meio", ataques de negação de serviço (DoS) e ataques físicos aos sensores[30]. Estes ataques podem interromper a operação da rede, comprometer dados ou até mesmo causar danos físicos em aplicações críticas [29].

- Problemas de privacidade: Dado que os nós sensores podem ser implantados em ambientes sensíveis (por exemplo, em casas ou hospitais), há preocupações legítimas sobre a privacidade dos dados recolhidos. Garantir que estes dados sejam transmitidos e armazenados de forma segura e privada é uma prioridade [30].

Em resposta a estes desafios, várias soluções têm sido propostas [30], incluindo protocolos de comunicação segura adaptados a RSSFs, esquemas de autenticação leves e métodos de detecção de intrusão. A pesquisa continua ativa nesta área, com o objetivo de criar RSSFs que não só sejam eficientes e confiáveis, mas também seguras e respeitadoras da privacidade.

2.1.2. O papel do padrão IEEE 802.15.4 em RSSFs

O padrão IEEE 802.15.4, inicialmente introduzido em 2003, posicionou-se rapidamente como um pilar central para comunicações em Redes de Sensores Sem Fios (RSSFs). Concebido especificamente para ambientes que requerem baixa taxa de transferência de dados, baixo consumo energético e operações a baixo custo, este padrão trouxe consigo uma série de características que o tornaram particularmente apelativo para uma variedade de aplicações [31], [32].

Uma das principais razões para a rápida adoção do IEEE 802.15.4 foi a sua capacidade de atender às necessidades específicas de RSSFs. Enquanto outras normas focavam em altas taxas de transferência e operações de alta potência, o 802.15.4 direcionou sua atenção para cenários onde a eficiência energética e a confiabilidade eram prioritárias. Esta abordagem foi fundamental para aplicações como monitorização ambiental, domótica, cuidados de saúde e, mais recentemente, para o crescente ecossistema da Internet das Coisas (IoT) [33].

A evolução do padrão foi motivada pelo reconhecimento das limitações iniciais e pelas demandas crescentes de aplicações emergentes. Em suas revisões subsequentes, observaram-se melhorias significativas na flexibilidade de modulação, na capacidade de endereçamento e na introdução de mecanismos de segurança robustos. Estes avanços garantiram que o padrão se mantivesse relevante e competitivo em um mercado tecnológico em constante mutação.

Contudo, para entender verdadeiramente a importância do IEEE 802.15.4, é essencial considerar os seus objetivos intrínsecos [34]. Mais do que simplesmente fornecer comunicações sem fio, o padrão buscou criar uma base sólida para sistemas que requerem interações confiáveis e de baixo consumo energético. Esta visão estratégica posicionou-o como uma escolha óbvia para *designers* e engenheiros que buscam soluções sustentáveis e eficientes em termos energéticos.

Mecanismos de economia de energia no padrão IEEE 802.15.4

Uma das principais preocupações ao projetar e implementar Redes de Sensores Sem Fios (RSSFs) é a eficiência energética [35]. Dado que muitos desses sensores são alimentados por baterias e estão muitas vezes localizados em ambientes remotos ou inacessíveis, prolongar a vida útil da bateria é essencial para garantir a longevidade e a funcionalidade da rede. O padrão IEEE 802.15.4, reconhecendo essa necessidade, integra vários

mecanismos destinados a minimizar o consumo de energia, permitindo assim uma operação mais eficiente.

- *Duty cycling:* Um dos mecanismos mais comuns para economia de energia é o "*duty cycling*", onde um dispositivo alterna entre estados de atividade e inatividade. Ao acordar apenas quando é estritamente necessário (por exemplo, para transmitir ou receber dados) [32], [36], os dispositivos podem economizar uma quantidade significativa de energia que seria consumida em um estado sempre ativo.

- *Adaptive listening*: O padrão introduz uma técnica chamada "*adaptive listening*", que permite que os dispositivos escutem de forma adaptativa o canal para verificar a atividade [35]. Em vez de ouvir constantemente, o que seria caro em termos de energia, os dispositivos podem periodicamente verificar a presença de sinais, melhorando assim a eficiência energética.

- *Frame pending:* Quando o coordenador (por exemplo, um nó de acesso) tem mais de um pacote para transmitir a um dispositivo final, ele pode usar o bit "*frame pending*" no quadro de controle de quadro do cabeçalho MAC para indicar a situação. Isso permite que o dispositivo final saiba que deve permanecer ativo e escutando por mais tempo, evitando ciclos de sono desnecessários e otimizando a comunicação [35].

- Uso de baixas taxas de transmissão: O padrão IEEE 802.15.4 destina-se a aplicações de baixa taxa de dados. Ao operar em taxas de transmissão mais baixas, o consumo de energia durante a transmissão é significativamente reduzido, permitindo uma operação mais eficiente em cenários de RSSFs [36].

Assim, a integração destes mecanismos no padrão IEEE 802.15.4 reflete a priorização da eficiência energética nas RSSFs. Ao aproveitar essas técnicas, os dispositivos que operam sob este padrão podem otimizar seu consumo de energia, prolongando a vida útil da bateria e, por extensão, a operação confiável da rede.

Topologias suportadas pelo IEEE 802.15.4: Estrela e Ponto a Ponto

A variedade de topologias que o padrão IEEE 802.15.4 suporta (apresentadas na figura 2.1.2) evidencia sua forma versátil e adaptação a diferentes cenários de aplicação [12]. A seguir, apresentamos uma exploração argumentativa dessas topologias.

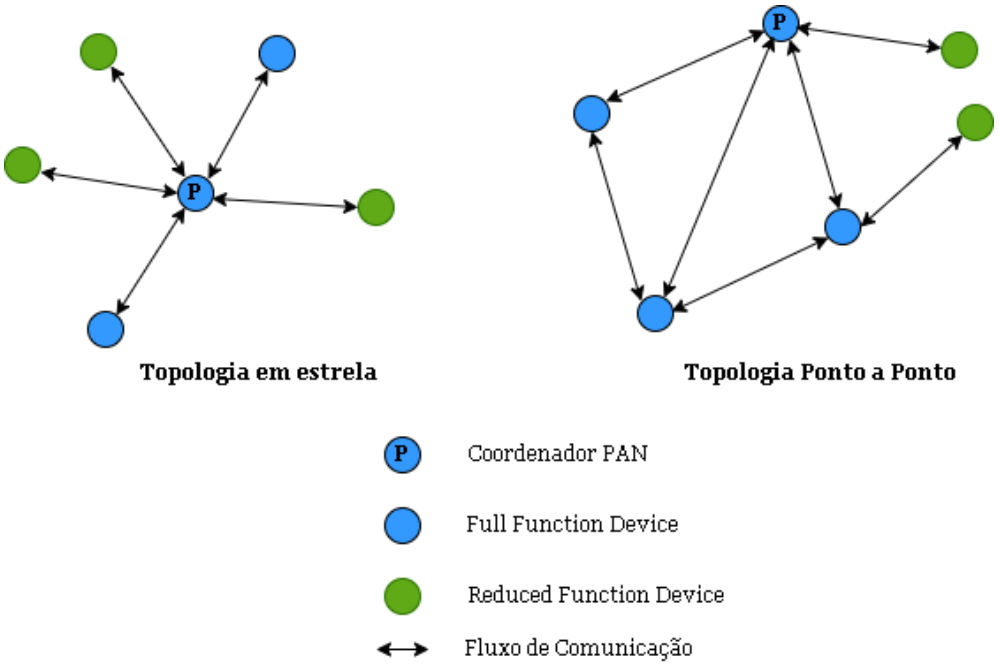

Figura 2.1.2 – Topologias de rede do padrão IEEE 802.15.4.

a) Topologia estrela

Vantagens:

Centralização: Com um único ponto de coordenação, a topologia estrela permite um controle centralizado da rede. Isto facilita a gestão e configuração da rede, tornando-a simples e fácil de monitorizar [37].

Economia de energia: Como os dispositivos apenas se comunicam com o coordenador, podem ser programados para entrar em estados de baixa energia quando não estão transmitindo, o que pode aumentar a vida útil da bateria.

Desafios:

Ponto único de falha: O coordenador central é crucial para o funcionamento da rede. Se falhar, toda a rede fica comprometida.

Escala: Esta topologia pode não ser ideal para grandes redes, devido à sobrecarga potencial no coordenador central com muitos dispositivos a tentar comunicar simultaneamente.

b) Topologia ponto a ponto

Vantagens:

Resiliência: Como cada nó pode se comunicar diretamente com outros nós, a rede pode se reconfigurar rapidamente em caso de falhas, tornando-a resiliente [37].

Extensibilidade: É fácil adicionar novos nós à rede, e eles podem se auto-organizar sem a necessidade de configuração centralizada.

Desafios:

Consumo de energia: A necessidade de manter múltiplas rotas e a comunicação direta entre nós pode levar a um maior consumo de energia.

Gestão de rotas: Manter e atualizar rotas em uma rede de grande dimensão pode tornar-se complexo e desafiador.

Comparação com outros padrões relevantes (como, *Zigbee* e LoRaWAN)

No campo das RSSFs, há uma diversidade de padrões e protocolos projetados para atender a diferentes necessidades e cenários de aplicação. Enquanto o padrão IEEE 802.15.4 é considerado a espinha dorsal para muitas soluções, outros padrões como *Zigbee* e LoRaWAN também têm mostrado notável presença no mercado. Uma compreensão clara de suas diferenças e características é crucial para a escolha informada de um padrão apropriado para uma dada aplicação [38].

Zigbee

Baseado no IEEE 802.15.4: Zigbee é uma tecnologia que foi desenvolvida em cima da camada física e da subcamada MAC do IEEE 802.15.4, fornecendo assim uma camada de rede e de aplicação para sistemas de baixo custo e baixo consumo [39].

Topologia em malha: Uma das características distintas do *Zigbee* é a sua capacidade de formar redes em malha. Isso permite uma maior resiliência, pois os dispositivos podem comunicar-se através de múltiplas rotas [21].

Aplicações: Devido à sua capacidade de formação de rede e baixo consumo, *Zigbee* é frequentemente utilizado em automação residencial, controle industrial e aplicações de monitoramento [10].

LoRaWAN

Comunicação de longa distância: LoRaWAN é conhecido por sua capacidade de transmitir dados por distâncias significativamente longas, chegando a vários quilómetros em áreas rurais [40].

Estrutura de rede: Ao contrário do *Zigbee*, o LoRaWAN normalmente opera numa topologia estrela, onde os dispositivos finais comunicam-se diretamente com um *gateway* central.

Aplicações: Devido à sua capacidade de longo alcance e à sua estrutura de topologia, o LoRaWAN é frequentemente escolhido para aplicações em áreas extensas, como agricultura inteligente, monitoramento de água e rastreamento de ativos [41].

2.2. A Ascensão da Internet das Coisas (IoT)

A Internet das Coisas (IoT) tem emergido como uma evolução natural da conexão global proporcionada pela Internet, almejando não apenas conectar pessoas através de dispositivos convencionais, mas também permitir que objetos do nosso quotidiano tenham a capacidade de se conectar, comunicar e cooperar uns com os outros. Assim, quando falamos da IoT, estamos a referir-nos a uma rede pervasiva de objetos fisicamente embutidos com tecnologia de sensoriamento, *software*, e outras tecnologias, com o intuito de conectar e trocar dados com outros dispositivos e sistemas por meio da Internet [5].

Um dos principais fundamentos que distinguem a IoT de outras tecnologias é a sua capacidade de transformar objetos estáticos, muitas vezes considerados triviais, em entidades inteligentes capazes de gerar, enviar e receber dados, tornando o nosso ambiente mais reativo e adaptativo às necessidades humanas [1]. Estes objetos inteligentes podem variar desde um simples frigorífico que monitoriza a data de validade dos alimentos, até sistemas de iluminação urbanos que adaptam o nível de luminosidade com base na atividade pedestre.

A capacidade de interconexão e interoperabilidade entre diferentes dispositivos e sistemas é outra característica fundamental da IoT. Através de protocolos padronizados e plataformas abertas, a IoT permite que diferentes dispositivos, independentemente do

fabricante ou da tecnologia subjacente, possam trabalhar em conjunto, otimizando recursos e ampliando as possibilidades de aplicações práticas [1], [42]. Em suma, o conceito da IoT baseia-se na premissa de que a vida quotidiana e o ambiente que nos rodeia podem ser enriquecidos e tornados mais eficientes através da integração e comunicação de objetos comuns, transformando-os em entidades inteligentes e conectadas [43].

Da automação à interconexão: A trajetória da IoT

A automação sempre foi um pilar fundamental da engenharia, permitindo que máquinas executassem tarefas sem intervenção humana direta. Desde a revolução industrial, temos testemunhado uma evolução contínua da automação em várias indústrias [43]. No entanto, o que distingue a era atual da Internet das Coisas (IoT) das fases anteriores de automação é a **interconexão**.

Nos primórdios da automação, as máquinas eram programadas para executar tarefas específicas e operavam de forma isolada. Embora fossem eficazes no que faziam, a falta de conectividade entre elas limitava a eficiência e a adaptabilidade do sistema como um todo. Com a evolução das tecnologias de informação e comunicação, nasce o conceito de **Máquina a Máquina (M2M),** onde os dispositivos começaram a comunicar entre si, partilhando informações e tomando decisões com base nesses dados [44]. Contudo, a IoT leva este conceito a um patamar superior, integrando não apenas máquinas, mas também objetos do quotidiano, veículos, eletrodomésticos e até mesmo vestuário, num ecossistema interconectado. Esta vasta rede de dispositivos interligados permite uma troca contínua de informações, possibilitando análises em tempo real e tomada de decisões automatizadas de forma mais informada e inteligente [44], [45].

A transição da automação para a interconexão oferecida pela IoT traz benefícios tangíveis. Os sistemas tornam-se mais resilientes, adaptativos e podem reagir a mudanças no ambiente em tempo real [45]. Por exemplo, numa cidade inteligente, a interconexão entre semáforos, veículos e sistemas de monitorização de tráfego pode otimizar os padrões de tráfego, reduzindo congestionamentos e diminuindo a emissão de gases poluentes [5], [45]. A trajetória da IoT, desde os princípios da automação até à interconexão ubíqua, representa uma revolução na forma como os sistemas são projetados, implementados e geridos. A capacidade de ter objetos quotidianos a "conversar" ou comunicar entre si e a tomar decisões baseadas em dados coletivos amplia as possibilidades de inovação, otimização e eficiência em inúmeras áreas da sociedade.

Os principais agentes e fatores para o crescimento da IoT

A Internet das Coisas (IoT) evoluiu rapidamente nos últimos anos, ultrapassando os domínios da investigação e entrando nos lares, cidades e indústrias. Tal expansão não aconteceu por acaso. Vários agentes e fatores têm desempenhado papéis cruciais no impulso desta revolução tecnológica.

Em primeiro lugar, a miniaturização dos dispositivos eletrónicos tem sido um catalisador fundamental. Com a capacidade de fabricar dispositivos cada vez menores, mais eficientes e mais baratos, tornou-se possível integrar capacidades de comunicação e computação em objetos do quotidiano [43], [46].

Em paralelo, os avanços na comunicação sem fios têm desempenhado um papel vital. Tecnologias como Wi-Fi, *Bluetooth*, e a mais recentemente 5G, não só possibilitaram taxas de transferência de dados mais rápidas, como também habilitaram a comunicação em áreas previamente inacessíveis, como zonas rurais ou ambientes industriais.

O crescimento exponencial da computação em nuvem é outro fator fundamental. Com a capacidade de processar e armazenar enormes quantidades de dados em centros de dados remotos, os dispositivos IoT podem ser mais leves em termos de capacidade de processamento, confiando na nuvem para as tarefas mais pesadas. Além disso, a demanda do consumidor por soluções mais inteligentes e conectadas impulsionou a adoção de dispositivos IoT [42]. Desde casas inteligentes que respondem às nossas necessidades até vestíveis que monitorizam nossa saúde, os consumidores têm mostrado um apetite crescente por tecnologias que enriquecem e facilitam suas vidas [43]. Um outro aspeto crucial é o apoio e investimento de grandes corporações tecnológicas. Empresas como a *Google*, *Amazon* e *Apple* têm investido pesadamente em soluções IoT, criando ecossistemas completos que incentivam a adoção por parte de desenvolvedores e consumidores [46].

Expectativas futuras e predições do mercado

A revolução da Internet das Coisas (IoT) tem consistentemente ultrapassado as fronteiras da inovação, abrindo um leque vasto de oportunidades em diversas áreas e setores da sociedade. As expectativas e predições em relação ao futuro da IoT têm sido objeto de debate e análise por vários investigadores, empresas de análise de mercado e *stakeholders*. A pesquisa realizada pela *Statista Departament*. prediz que, até 2030, o número de dispositivos conectados ultrapassará os 25 bilhões em todo o mundo [4]. Esta predição baseia-se em tendências emergentes, como a miniaturização de dispositivos,

avanços na comunicação sem fios, e a crescente necessidade de análise de dados em tempo real. Além da magnitude de dispositivos conectados, a qualidade e a profundidade das interações entre estes dispositivos também se espera que evoluam, resultando em sistemas mais inteligentes e adaptáveis [47].

2.2.1. Impacto da IoT no mundo moderno

O desenvolvimento rápido e a implementação crescente da Internet das Coisas (IoT) têm desempenhado um papel crucial na transformação digital das cidades contemporâneas. Essa evolução urbana, frequentemente designada por "cidades inteligentes", é, em essência, a fusão da infraestrutura física com a digital, permitindo uma maior interconexão, comunicação e gestão de recursos da cidade [48].

Argumento:

I. Melhoria da qualidade de vida: Com a integração da IoT, sistemas urbanos como iluminação pública, transporte e gestão de resíduos podem ser otimizados em tempo real, melhorando significativamente a qualidade de vida dos residentes. Por exemplo, sensores da IoT podem monitorizar a qualidade do ar e informar os cidadãos em tempo real, permitindo-lhes tomar decisões informadas sobre suas rotas diárias [46].

II. Gestão de recursos eficiente: A capacidade de monitorizar e controlar os recursos de uma cidade em tempo real, desde o consumo de água até à distribuição de energia, pode levar a uma utilização mais eficiente e sustentável desses recursos. Isto não só poupa dinheiro ao município, como também reduz o impacto ambiental [46].

III. Maior segurança: A utilização de dispositivos IoT em infraestruturas críticas, como redes elétricas e sistemas de transporte, pode ajudar a detetar e responder a falhas ou ameaças de forma quase instantânea [49]. Adicionalmente, sistemas de vigilância e monitorização podem ser integrados para melhorar a segurança pública [7].

IV. Participação cidadã: Com a IoT, torna-se possível ter uma comunicação bidirecional entre a administração municipal e os cidadãos. Aplicações e plataformas podem ser desenvolvidas para permitir que os cidadãos reportem problemas, ofereçam sugestões ou até mesmo votem em iniciativas locais, promovendo uma governança mais inclusiva e democrática [49].

Desafios associados: Apesar dos inúmeros benefícios, é essencial considerar os desafios associados à implementação da IoT nas cidades. Questões de privacidade, segurança cibernética e a necessidade de infraestruturas robustas são apenas alguns dos obstáculos que as cidades enfrentam ao adotar uma abordagem mais digital e conectada [46], [48].

Aplicações práticas em diferentes sectores: Agricultura, saúde e indústrias

A Internet das Coisas (IoT) tem catalisado uma profunda transformação em diversos sectores económicos. Ao conectar dispositivos que tradicionalmente operam de forma isolada, tem-se desbloqueado uma série de novas capacidades e funcionalidades, aumentando a eficiência, a segurança e a capacidade de inovação.

Agricultura:

O conceito de "agricultura inteligente" tem-se popularizado graças ao IoT. Sensores são usados para monitorizar condições do solo, níveis de humidade, e saúde das culturas em tempo real [50]. Estes dados permitem aos agricultores tomar decisões informadas sobre irrigação, aplicação de fertilizantes e pesticidas, resultando em maior produtividade e sustentabilidade. Além disso, sistemas de rastreamento podem monitorizar a saúde e localização do gado, melhorando a eficiência da pecuária.

Saúde:

O sector da saúde tem sido profundamente impactado pela IoT. Dispositivos vestíveis, como relógios inteligentes e monitores de frequência cardíaca, podem recolher dados vitais dos pacientes em tempo real e transmiti-los a profissionais de saúde [51]. Isto permite monitorização contínua, deteção precoce de anomalias e intervenção atempada, reduzindo riscos e melhorando a qualidade de vida dos pacientes. Além disso, dispositivos IoT em hospitais ajudam na gestão de ativos, rastreamento de medicamentos e monitorização de condições ambientais.

Indústrias:

A "Indústria 4.0" é a incarnação da integração da IoT no sector industrial [51]. Sensores colocados em máquinas e linhas de produção fornecem *insights* em tempo real sobre o desempenho e eficiência do equipamento. Estes dados ajudam na previsão e prevenção de avarias, otimizando a manutenção e reduzindo tempos de inatividade. Além disso, a

integração da IoT com sistemas de gestão e logística permite uma cadeia de fornecimento mais eficiente e adaptável.

Os desafios da escalabilidade e segurança na IoT

A era digital de hoje testemunha uma explosão sem precedentes na quantidade de dispositivos IoT conectados. Esta rápida expansão introduz desafios tanto em termos de escalabilidade quanto de segurança.

Escalabilidade:

- Quantidade massiva de dispositivos: O crescente número de dispositivos interconectados exige uma infraestrutura robusta que possa acomodar tal magnitude. A crescente demanda pode sobrecarregar as redes existentes, causando atrasos ou falhas na transmissão de dados [52].

- Gestão de dados: Estima-se que dispositivos IoT produzam quantidades vastas de dados. A gestão eficaz e a análise destes dados são cruciais para garantir que as informações sejam utilizadas de forma eficiente e em tempo real [47], [48].

- Interoperabilidade: Com a variedade de fabricantes e padrões emergindo no domínio da IoT, garantir a interoperabilidade entre dispositivos e sistemas torna-se uma preocupação significativa [52].

Segurança:

- Ataques e vulnerabilidades: A natureza aberta e interconectada da IoT o torna vulnerável a uma variedade de ataques, incluindo, mas não limitado a ataques de negação de serviço (DoS), acesso não autorizado e sequestro de dispositivos.

- Privacidade: A recolha de dados de dispositivos IoT, que frequentemente inclui informações pessoais ou sensíveis, suscita preocupações de privacidade. A garantia de que esses dados são coletados, armazenados e transmitidos de maneira segura é essencial [52].

- Padrões e regulamentações: Atualmente, há uma falta de padrões universais no que diz respeito à segurança da IoT. Isto pode resultar em implementações inseguras ou incompatíveis que ameaçam tanto os utilizadores quanto as redes.

Considerações éticas e de privacidade associadas ao IoT

Com a rápida ascensão da IoT, a quantidade de dados gerados, partilhados e armazenados aumentou exponencialmente. Enquanto estes dados têm o potencial de melhorar significativamente as nossas vidas, trazem também preocupações sérias sobre a privacidade e ética da sua utilização [52].

- Privacidade dos dados e consentimento: A natureza omnipresente da IoT implica que uma quantidade significativa de dados pessoais é constantemente gerada e partilhada. Em muitos casos, os utilizadores podem não estar completamente cientes de quais dados estão a ser partilhados, ou com quem estão a ser partilhados. A questão crucial é: até que ponto os utilizadores deram verdadeiramente o seu consentimento informado para a coleta e uso desses dados? Em ambientes onde dispositivos Io estão sempre "ligados", o conceito tradicional de "*opt-in*" ou "*opt-out*" pode não ser suficientemente robusto [47], [52].

- Segurança de dados e vulnerabilidades: O aumento de dispositivos conectados amplia a superfície de ataque para potenciais ameaças cibernéticas. Estes dispositivos, muitas vezes, podem não possuir mecanismos de segurança robustos, tornando-os alvos atraentes para hackers. Uma vez comprometidos, estes dispositivos podem ser usados para ataques subsequentes ou para a obtenção ilícita de dados pessoais. Os fabricantes e desenvolvedores têm, por isso, uma responsabilidade ética de garantir que os dispositivos IoT sejam seguros por *design* [47], [52].

- Tomada de decisão automatizada e responsabilidade: Com a integração de algoritmos de inteligência artificial e aprendizagem automática na IoT, muitas decisões são tomadas sem intervenção humana. No entanto, quem é responsável quando algo corre mal? Determinar a responsabilidade por decisões automatizadas em sistemas IoT complexos pode ser um desafio ético significativo [52].

2.2.2. Interação e repercussões em RSSFs

O crescimento da IoT tem como cerne a promessa de uma interconectividade omnipresente e a consequente transformação digital de inúmeros sectores da sociedade. Diversas são as aplicações imaginadas. Portanto, para materializar tal visão, é imperativo

contar com redes robustas, eficientes e expansíveis. É neste contexto que as Redes de Sensores Sem Fios (RSSFs) emergem como um pilar fundamental.

As RSSFs oferecem uma capacidade intrínseca de monitorização distribuída. Estes sensores, frequentemente alimentados por baterias ou por métodos alternativos de colheita de energia, podem ser dispersos em ambientes hostis ou inacessíveis, transmitindo dados valiosos sobre o seu meio envolvente [24], [53]. Tal capacidade é essencial para várias aplicações da IoT, tais como a monitorização ambiental ou a detecção precoce de falhas em infraestruturas críticas. Além disso, a natureza sem fios das RSSFs permite uma implementação flexível e escalável. Conforme o ecossistema do IoT continua a crescer, a necessidade de expandir e adaptar a infraestrutura de rede torna-se premente. As RSSFs, com a sua capacidade de auto-organização e adaptação, alinham-se perfeitamente com este requisito [24].

No entanto, é relevante notar que, apesar das suas vantagens, as RSSFs também apresentam desafios quando integradas no paradigma do IoT. Questões como a eficiência energética, latência e segurança precisam ser levadas a sério para garantir que estas redes possam sustentar o crescimento exponencial previsto para o IoT.

Adaptação dos protocolos de comunicação ao crescimento da IoT

A adaptação dos protocolos de comunicação torna-se imperativa à medida que o IoT continua a expandir-se, permeando múltiplos sectores da sociedade e da economia. O crescimento exponencial do número de dispositivos conectados tem desafiado os protocolos de comunicação tradicionais, forçando-os a evoluir para dar resposta às novas exigências do mercado.

Para começar, a heterogeneidade dos dispositivos IoT, variando desde simples sensores até dispositivos inteligentes robustos, exige uma flexibilidade inerente nos protocolos de comunicação. As soluções tradicionais, que tendem a ser monolíticas e adaptadas a cenários específicos, podem não ser suficientemente versáteis para lidar com a diversidade do ambiente IoT [5]. Além disso, os protocolos de comunicação também enfrentam desafios em termos de escalabilidade. Com milhões, ou mesmo bilhões, de dispositivos projetados para serem conectados na próxima década, é essencial que os protocolos sejam capazes de lidar com uma tão ampla escala de conexões simultâneas sem comprometer o desempenho. As abordagens tradicionais, que poderiam funcionar bem em redes menores, agora enfrentam desafios em termos de latência, gestão de tráfego e eficiência energética.

O consumo de energia é outro ponto crucial. Dado que muitos dispositivos IoT são alimentados por baterias ou soluções de *harvesting* de energia [26], os protocolos de comunicação precisam ser extremamente eficientes do ponto de vista energético. Isso é particularmente verdadeiro para RSSFs, onde a duração da bateria pode determinar a viabilidade de uma aplicação. A segurança é ainda uma outra dimensão que não pode ser negligenciada. Com um número crescente de dispositivos conectados, as superfícies de ataque ampliam-se, tornando a rede mais vulnerável [29]. Protocolos de comunicação seguros e robustos são necessários para garantir a integridade, confidencialidade e disponibilidade dos dados no ambiente IoT. Por último, mas não menos importante, a interoperabilidade emerge como um dos principais desafios na adaptação dos protocolos. Com uma vasta gama de dispositivos, plataformas e aplicações em jogo, garantir uma comunicação fluida e sem interrupções entre os diferentes componentes da rede IoT torna-se vital.

Desafios energéticos das RSSFs na era da IoT

O universo da IoT propõe uma visão de interconexão global de dispositivos, onde cada objeto pode comunicar e interagir com outros, formando uma rede massiva e complexa. Neste cenário, as RSSFs desempenham um papel crucial, pois são muitas vezes a fonte primária de dados, desde monitorização ambiental a aplicações industriais e de saúde. Contudo, como qualquer tecnologia, as RSSFs enfrentam desafios significativos à medida que se integram mais profundamente na infraestrutura da IoT [46].

A questão da eficiência energética, em particular, é fundamental. Os nós sensores, frequentemente, operam com baterias limitadas e, em muitos casos, são implantados em locais remotos ou inacessíveis, tornando a substituição ou recarga de baterias impraticável [54]. Neste contexto, garantir uma vida útil de bateria longa não é apenas uma questão de economia, mas também de funcionalidade. Uma rede de sensores com baterias rapidamente esgotadas pode comprometer todo um ecossistema da IoT, especialmente em aplicações críticas como monitorização de saúde ou infraestruturas urbanas.

A ascensão da IoT intensifica este desafio. Com mais dispositivos interligados, espera-se que cada sensor transmita e receba mais dados do que antes. Além disso, a necessidade de manter conexões estáveis e a demanda por atualizações frequentes podem aumentar a carga de trabalho dos nós sensores, elevando o consumo energético [46], [54]. Há também a expectativa de que os sensores processem informações localmente (um conceito conhecido como "computação de borda" ou "*edge computing*"), para reduzir a

latência e a sobrecarga da transmissão de dados. Embora isso possa trazer benefícios em termos de desempenho e eficiência da rede, pode igualmente intensificar o consumo de energia do sensor. A solução para estes desafios passa por uma combinação de *hardware* avançado, otimização de protocolos de comunicação, e algoritmos inteligentes de gerenciamento de energia. É essencial considerar a eficiência energética não apenas como um componente isolado, mas como parte integrante do *design* e implementação de sistemas IoT.

Oportunidades e inovações proporcionadas pelo crescimento da IoT nas Redes de Sensores Sem Fios (RSSFs)

Com o crescimento da IoT, temos testemunhado uma onda crescente de dispositivos interconectados, variando de simples sensores ambientais a dispositivos inteligentes avançados. A inclusão destes dispositivos nas RSSFs não é apenas uma inevitabilidade, mas também uma necessidade, dada a demanda por informação em tempo real, análise preditiva e automação [39], [46]. Neste contexto, as RSSFs, enquanto estrutura base, têm potencial para desempenhar um papel vital na realização das promessas da IoT. A integração bem-sucedida de RSSFs e IoT pode dar origem a uma série de oportunidades e inovações, como:

1. Interconexão e interoperabilidade melhoradas: Ao capitalizar as características das RSSFs, como sua capacidade de auto-organização e adaptação, os sistemas IoT podem alcançar um nível de interconexão e interoperabilidade sem precedentes. Esta interligação não se restringe apenas a dispositivos dentro de uma rede específica, mas também entre diferentes redes, permitindo a criação de um verdadeiro ecossistema global de dispositivos conectados.

2. Eficiência energética e sustentabilidade: Dada a natureza inerente das RSSFs de serem conscientes em relação ao consumo de energia, a sua integração com a IoT pode conduzir a soluções mais energeticamente eficientes. Estas soluções, por sua vez, têm potencial para sustentar a crescente densidade de dispositivos no ecossistema IoT [46].

3. Inovações em aplicações e serviços: A combinação de RSSFs e IoT pode dar origem a novos serviços e aplicações que eram anteriormente impensáveis. Por exemplo, na área de saúde, poderíamos ver sistemas de monitorização de pacientes em tempo real, usando sensores vestíveis que transmitem dados diretamente para plataformas de análise médica avançada, resultando em diagnósticos mais precisos e em tempo hábil.

4. Evolução na tomada de decisões e análise de dados: RSSFs são conhecidas pela sua capacidade de processar e transmitir dados de forma eficiente. Integradas ao IoT, estas redes poderiam servir como a espinha dorsal de uma infraestrutura de análise de dados avançada, possibilitando melhores *insights* e tomada de decisões mais informadas em setores como o empresarial, governamental e até mesmo pessoal.

O crescimento da IoT apresenta uma oportunidade única para as RSSFs. Embora desafios como segurança, privacidade e escalabilidade certamente persistam, o potencial para inovação e melhoria é vasto. Ao abraçar esta evolução, podemos estar à beira de uma nova era de conectividade e inteligência, onde as possibilidades são tão vastas quanto a própria internet [49].

2.3. Protocolos MAC e Eficiência Energética

A camada MAC (*Medium Access Control*) representa uma das pedras angulares nas Redes de Sensores Sem Fios (RSSFs). Esta camada é responsável por determinar como os dispositivos numa rede acessam o meio para transmitir informação. Dada a natureza e o contexto das RSSFs, a eficiência e eficácia desta camada são fundamentais para garantir o funcionamento otimizado e a vida útil da rede. Abaixo, argumento sobre a sua importância no contexto das RSSFs [55].

- Consumo de energia: Os nós sensores em RSSFs são frequentemente alimentados por baterias com energia limitada. Ineficiências na camada MAC, como colisões frequentes ou esperas longas para transmissões, podem resultar em consumo desnecessário de energia, reduzindo assim a longevidade da rede [55]. Uma camada MAC bem projetada assegura que os nós sensores consumam energia apenas quando é estritamente necessário.

- Confiabilidade da transmissão: Nas RSSFs, a confiabilidade é crucial, uma vez que a perda de dados pode comprometer a integridade da informação recolhida [2]. Uma camada MAC eficaz minimiza as colisões e as retransmissões, garantindo assim a entrega de pacotes com maior precisão.

- Escalabilidade da rede: À medida que as RSSFs crescem em tamanho e complexidade, a camada MAC desempenha um papel vital em garantir que novos nós sensores possam ser incorporados na rede sem degradar significativamente

o seu desempenho [56]. Isto é especialmente importante em aplicações como monitorização ambiental ou cidades inteligentes, onde o número de sensores pode ser na ordem das centenas ou milhares.

- Latência: Em algumas aplicações de RSSFs, a rapidez com que a informação é transmitida e processada é vital. Uma camada MAC eficiente minimiza o atraso ao transmitir dados, garantindo tempos de resposta rápidos.

- Interoperabilidade e coexistência: Dadas as diversas tecnologias e padrões presentes no espectro sem fio, uma camada MAC bem projetada assegura que os dispositivos de RSSFs possam operar harmoniosamente em ambientes congestionados, minimizando interferências e melhorando a coexistência com outros dispositivos [56].

A camada MAC é um componente essencial das RSSFs, influenciando diretamente a sua eficiência energética, confiabilidade, escalabilidade, latência e capacidade de coexistir com outras redes. A escolha e implementação adequada de protocolos MAC podem, assim, ditar o sucesso ou falha de uma aplicação baseada em RSSFs.

2.3.1. Desafios de eficiência energética

A eficiência energética em Redes de Sensores Sem Fios (RSSFs) é fundamental dada a natureza das aplicações e das restrições energéticas frequentemente associadas a estas redes. O consumo de energia eficiente prolonga a vida útil da rede, reduz a frequência de substituição da bateria e torna viável a implantação em áreas remotas ou de difícil acesso [57]. Vários fatores e desafios tornam a eficiência energética uma área crucial de pesquisa e desenvolvimento:

a. Restrições de fonte de energia: Muitos sensores sem fios são alimentados por baterias, que têm uma capacidade de energia limitada. Em muitos cenários, como monitorização ambiental em locais remotos, a substituição de baterias pode ser proibitivamente cara ou logisticamente complexa.

b. Diversidade de tarefas dos sensores: Dependendo da aplicação, os nós sensores podem estar envolvidos em tarefas que variam em termos de exigências energéticas - desde simples monitorizações periódicas até tarefas intensivas, como processamento de imagem.

c. Comunicação vs. processamento: A comunicação entre os sensores muitas vezes consome mais energia do que o processamento. Portanto, protocolos eficientes que reduzam o tráfego desnecessário ou evitem colisões são essenciais [3].

d. Energia de *harvesting*: A capacidade de colher energia a partir de fontes ambientais (solar, vibração, etc.) oferece uma oportunidade para sensores "autossustentáveis". No entanto, a energia colhida pode ser intermitente ou insuficiente, exigindo gestão inteligente [55] .

e. Estratégias de economia de energia: Mecanismos como *duty cycling*, em que os sensores alternam entre estados de vigília e sono, podem melhorar a eficiência energética. No entanto, essas estratégias devem ser bem geridas para não comprometer a funcionalidade ou a latência da rede.

f. Otimização de topologia: A formação e manutenção de uma topologia de rede que minimiza a energia de comunicação é crucial. Soluções, como a criação de rotas de múltiplos saltos otimizadas, podem desempenhar um papel vital.

2.3.2. Visão geral dos protocolos MAC

Os protocolos de Controlo de Acesso ao Meio (MAC, do inglês "*Medium Access Control*") têm como principal função definir as regras segundo as quais os dispositivos numa rede decidem quando transmitir dados no canal de comunicação [58]. Num cenário em que vários dispositivos tentam transmitir simultaneamente, os protocolos MAC desempenham um papel crucial na prevenção e resolução de conflitos, garantindo uma utilização eficiente do canal e, consequentemente, um bom desempenho da rede. Existem várias abordagens para a implementação de protocolos MAC, cada uma com suas vantagens e desvantagens específicas:

Protocolos MAC baseados em divisão de canal:

- Divisão de Tempo (TDMA, *Time Division Multiple Access*): Aqui, o canal é dividido em diferentes intervalos de tempo, e cada dispositivo é alocado a um intervalo específico. Isso elimina colisões, mas requer uma sincronização rigorosa entre os dispositivos [59].

- Divisão de Frequência (FDMA, *Frequency Division Multiple Access*): Neste método, o espectro é dividido em diferentes bandas de frequência, atribuídas a diferentes dispositivos. Requer um bom controlo de frequência e pode não ser ideal para dispositivos com recursos limitados.

- Divisão de Código (CDMA, *Code Division Multiple Access*): Em CDMA, cada dispositivo tem um código único que é usado para modular a sua transmissão. O receptor desmodula a transmissão usando o mesmo código, permitindo que várias transmissões ocorram ao mesmo tempo no mesmo canal. Embora ofereça uma boa utilização do espectro, a complexidade na implementação pode ser um desafio [59].

Protocolos MAC baseados em contenção:

- CSMA (*Carrier Sense Multiple Access*): Nesta abordagem, os dispositivos, primeiro "ouvem" o canal para detetar se ele está livre. Se estiver, eles transmitem; caso contrário, eles esperam e tentam novamente depois de um certo tempo. Variações como CSMA/CD (onde os dispositivos detetam colisões) e CSMA/CA (onde eles tentam evitar colisões) são comuns [59].

- ALOHA e *Slotted* ALOHA: ALOHA é um dos primeiros protocolos baseados em contenção, onde os dispositivos transmitem sempre que têm dados e, em seguida, aguardam por uma confirmação. Se não receberem a confirmação, eles retransmitem após um período aleatório. *Slotted* ALOHA melhora isso ao dividir o tempo em "*slots*" e permitir transmissões apenas no início destes "*slots*" [59] .

Existem ainda outras variações e métodos (6LoWPAN, *Bluetooth Low Energy* (BLE), entre outros), como protocolos baseados em escuta ou baseados em agendamento, cada um adaptado a diferentes cenários e requisitos. Dada a diversidade de protocolos MAC, a seleção do protocolo certo depende em grande medida do cenário específico e dos requisitos da aplicação [59]. Para Redes de Sensores Sem Fios (RSSFs), a eficiência energética é um critério fundamental, uma vez que os sensores frequentemente operam com baterias limitadas. Portanto, há uma tendência para favorecer protocolos MAC que minimizem as colisões, evitem escutas desnecessárias e reduzam as retransmissões.

CSMA e suas Variações

O protocolo de Múltiplo Acesso com Monitorização de Portadora (CSMA) é um dos pilares fundamentais das técnicas de controle de acesso ao meio em redes sem fios, especialmente no contexto das RSSFs [59]. A sua essência reside no princípio de "escutar antes de falar" - um dispositivo só transmite dados se perceber que o canal de comunicação está livre, evitando assim colisões [60]. Existem algumas variações do CSMA, dentre elas:

a. CSMA Persistente e Não Persistente:

O CSMA persistente implica que, uma vez que o canal é percebido como livre, a transmissão começa imediatamente [60]. Por outro lado, no CSMA não persistente, o dispositivo aguarda um período aleatório antes de verificar novamente se o canal está livre.

b. CSMA/CA (Múltiplo Acesso com Monitorização de Portadora e Prevenção de Colisões):

Comum no padrão IEEE 802.11 (Wi-Fi), o CSMA/CA acrescenta uma camada adicional de lógica para prevenir colisões [59], [60]. Se um dispositivo perceber que o canal está ocupado, ele irá esperar por um período aleatório antes de tentar retransmitir, minimizando a probabilidade de duas estações transmitirem simultaneamente.

c. CSMA/CD (Múltiplo Acesso com Monitorização de Portadora e Detecção de Colisões):

Usado tradicionalmente em redes *Ethernet*, este protocolo não só escuta o canal antes da transmissão, mas também durante [60]. Se uma colisão é detetada, a transmissão é interrompida, e um algoritmo de *backoff* é usado para determinar quando a próxima tentativa de transmissão deve ocorrer.

A escolha do CSMA como um protocolo MAC base para muitas redes é justificada pela sua simplicidade e eficácia em minimizar colisões, especialmente quando o tráfego é esporádico. No entanto, as redes de alta densidade e tráfego intenso podem testemunhar um aumento na ocorrência de colisões, tornando variantes como CSMA/CA mais relevantes [59]. A principal crítica ao CSMA e suas variantes é que elas não são totalmente eficazes na prevenção de colisões, especialmente em redes com latências variáveis e altas taxas de transmissão. Isto leva a uma redução na eficiência do canal e, em redes de sensores sem fios, resulta em maior consumo de energia devido a retransmissões [60].

Dado o foco da presente dissertação na eficiência energética, é crucial entender as limitações do CSMA e suas variantes. Embora o CSMA represente um avanço significativo em relação a protocolos sem gestão de acesso, as suas limitações energéticas podem justificar a exploração de alternativas, como o *Slotted* ALOHA, em ambientes de RSSFs.

Slotted ALOHA

O protocolo *Slotted* ALOHA, como uma evolução direta do ALOHA original (ambos baseados na ideia da distribuição de *Poisson*), surgiu da necessidade de aumentar a eficiência da utilização do canal, ao introduzir o conceito de "*slots*" de tempo. Antes de nos aprofundarmos nos pormenores técnicos e benefícios do *Slotted* ALOHA, é crucial entender o panorama geral das redes de comunicação e o desafio subjacente que o ALOHA procurava resolver [61].

Surgimento:

O protocolo ALOHA original (*Pure* ALOHA) foi concebido na Universidade do Havai para a rede ALOHAnet, visando permitir que várias estações de base transmitissem dados numa única frequência de rádio compartilhada [62]. No entanto, uma das principais limitações do ALOHA puro é a sua baixa eficiência, principalmente devido a colisões que ocorrem quando duas estações transmitem ao mesmo tempo. Aqui surge o *Slotted* ALOHA, uma variante que segmenta o tempo em intervalos discretos ou "*slots*", nos quais as estações são permitidas a transmitir, aumentando assim a eficiência.

Funcionamento:

No *Slotted* ALOHA, as estações só podem começar a transmitir no início de um *slot* de tempo. Se duas ou mais estações transmitirem no mesmo *slot*, ocorre uma colisão e as estações são informadas da falha (Ver a Fig.2.3.1). As estações então esperam um período aleatório e tentam retransmitir [62].

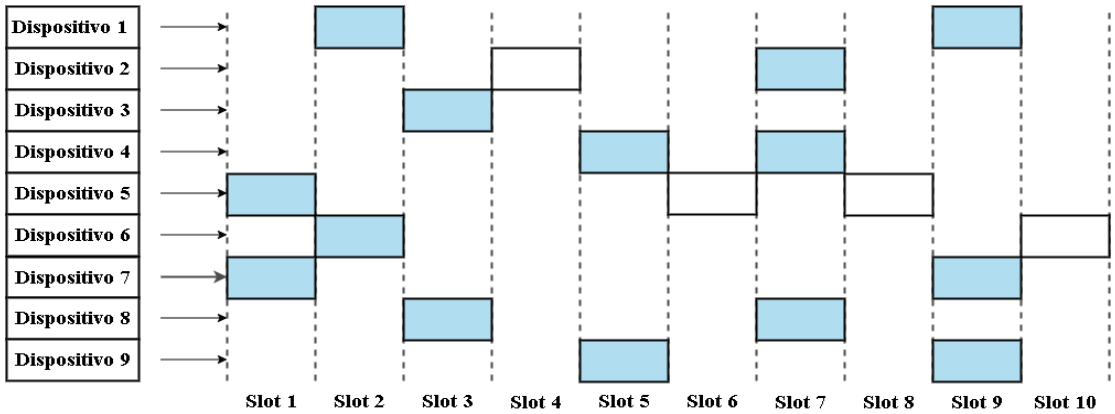

Figura 2.3.1 - Funcionamento do *Slotted* ALOHA [1].

[1] Os pacotes vazios ou não preenchidos indicam um envio bem-sucedido (apenas um pacote foi enviado naquele *slot*), enquanto os pacotes com preenchimento azul-claro indicam uma colisão (dois ou mais pacotes foram enviados no mesmo *slot*).

Vantagens do *Slotted* ALOHA sobre o ALOHA puro:

- Maior eficiência: A introdução de *slots* de tempo dobrou a eficiência do protocolo em comparação com o ALOHA puro (com 18%), alcançando uma eficiência teórica máxima de cerca de **37%** (conforme apresentado na figura 2.3.2) [3].

- Previsibilidade: Com *slots* de tempo definidos, é mais fácil para as estações sincronizarem suas transmissões, reduzindo assim a probabilidade de colisões.

- Simplicidade de implementação: Apesar da necessidade de sincronização, o *Slotted* ALOHA mantém a simplicidade fundamental do protocolo ALOHA, facilitando a sua implementação e manutenção.

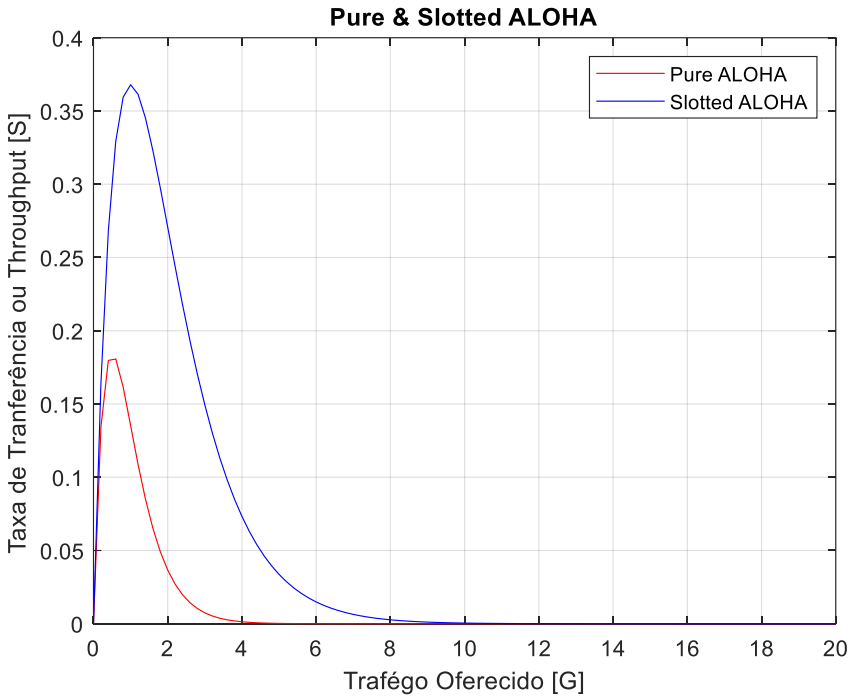

Figura 2.3.2 - Comparação do ALOHA Original VS. *Slotted* ALOHA.

Limitações:

Apesar de suas vantagens claras sobre o ALOHA puro, o *Slotted* ALOHA ainda tem as suas limitações. A necessidade de sincronização rigorosa entre estações é uma delas. Além disso, mesmo com a melhoria na eficiência, 37% ainda é relativamente baixo para muitas aplicações práticas, o que levou a busca por protocolos alternativos e melhorias subsequentes no ALOHA, como o *Q-learning* e *Binary Exponential Backoff* (BEB).

2.3.3. Comparação e justificativa da escolha do *Slotted* ALOHA

Ao abordar o universo dos protocolos MAC, muitos protocolos têm ganhado relevância na literatura técnica, especialmente quando se trata de Redes de Sensores Sem Fios (RSSFs) [60], [62]. Entre estes protocolos, o CSMA (*Carrier Sense Multiple Access*) e o *Slotted* ALOHA são frequentemente discutidos devido às suas características singulares. Para fundamentar a escolha do *Slotted* ALOHA como foco desta pesquisa, é crucial realizar uma análise comparativa e sublinhar as suas vantagens, particularmente em relação ao CSMA e outros protocolos.

- Eficiência espetral e simplicidade: O *Slotted* ALOHA, quando comparado com o ALOHA puro, oferece uma eficiência espetral dobrada, devido à sua abordagem sincronizada de alocação de *slots* de tempo [63]. Esta eficiência, embora inferior à do CSMA em condições ideais, é alcançada com uma arquitetura e implementação substancialmente mais simples. Esta simplicidade é uma característica chave para sensores com capacidades limitadas.

- Previsibilidade: Ao contrário do CSMA, que tenta detetar e evitar colisões, o *Slotted* ALOHA aceita a possibilidade de colisões, mas opera de forma que estas sejam relativamente previsíveis [59]. Esta previsibilidade pode ser essencial em cenários onde a consistência e a capacidade de planeamento são mais valiosas do que simplesmente maximizar a eficiência.

- Adaptabilidade a melhorias: O *Slotted* ALOHA, embora antigo, mostrou-se adaptável a melhorias e variações. Exemplos, como a adição do *Binary Exponential Backoff* (BEB) ou a integração com técnicas de aprendizado de máquina como o *Q-learning*, indicam que o protocolo pode ser otimizado ainda mais em termos de eficiência energética e desempenho [3].

- Desempenho sob carga variável: Nos cenários de tráfego variável, a eficiência do *Slotted* ALOHA pode aproximar-se ou até superar a do CSMA, especialmente quando a carga de tráfego é baixa a moderada [63]. Isso torna o *Slotted* ALOHA particularmente atrativo para RSSFs onde o padrão de tráfego pode ser variável.

- Energia e eficiência: Em ambientes onde a detecção de portadora do CSMA é desafiadora ou ineficiente, o *Slotted* ALOHA pode oferecer uma melhor eficiência energética. Esta é uma consideração crítica em RSSFs, onde a longevidade da bateria é uma preocupação primordial [5].

Embora o CSMA e outros protocolos tenham seus méritos, a simplicidade, previsibilidade e adaptabilidade do *Slotted* ALOHA tornam-no uma escolha promissora para ambientes de RSSFs, especialmente quando otimizado para eficiência energética. A decisão de focar no *Slotted* ALOHA, portanto, não é apenas justificada, mas também alinhada com o objetivo primordial desta investigação: melhorar a eficiência energética em RSSFs.

2.4. Conclusão

Neste capítulo, estudamos de forma abrangente sobre as redes sem fios e, mais especificamente, das Redes de Sensores Sem Fios (RSSFs). Começando com uma introdução geral, pudemos compreender as características distintivas destas redes e os desafios inerentes a elas. A norma IEEE 802.15.4 emergiu como um pilar fundamental neste domínio, estabelecendo padrões que facilitam a interoperabilidade e o desempenho eficiente das RSSFs.

A seguir embarcamos para a ascensão da Internet das Coisas (IoT), uma revolução que está a redefinir o nosso mundo moderno. Não só discutimos o impacto profundo que a IoT tem em diversos setores, como também explorámos a sua estreita interação e as repercussões nas RSSFs, que muitas vezes servem como os olhos e ouvidos do mundo IoT. Posteriormente, abordámos o cerne da questão em relação aos protocolos MAC, com um foco especial na eficiência energética. Dada a natureza restritiva da energia em muitas RSSFs, a eficiência energética é uma preocupação primordial. Vários protocolos MAC foram apresentados, permitindo-nos entender a diversidade de estratégias e mecanismos utilizados para aceder o meio de comunicação. A nossa análise comparativa destacou a superioridade potencial do *Slotted* ALOHA, uma escolha que se justifica não apenas pelo seu desempenho, mas também pela sua adaptabilidade e simplicidade.

Concluindo, através desta revisão de literatura, estabelecemos um fundamento sólido para os capítulos subsequentes. As RSSFs, no contexto da IoT e com a necessidade imperativa de eficiência energética, exigem soluções inovadoras, e a nossa exploração dos protocolos MAC aponta para direções promissoras. Os capítulos seguintes aprofundarão mais sobre os mecanismos utilizados para aprimorar o protocolo *Slotted* ALOHA neste trabalho, as simulações, os testes e as análises, tendo por base o conhecimento acumulado neste capítulo.

Capítulo 3

3. *Binary Exponential Backoff* e Aplicação do *Q-learning* em RSSFs

3.1. Princípios e funcionamento do BEB

O *Binary Exponential Backoff* (BEB) é um algoritmo fundamental utilizado em muitos protocolos de Controlo de Acesso ao Meio (MAC) para regular a transmissão de pacotes e mitigar colisões em redes sem fios e com fios. A sua eficácia e simplicidade tornaram-no uma escolha popular, particularmente em protocolos como o IEEE 802.11 (Wi-Fi) e o IEEE 802.3 (*Ethernet*) [64].

A ideia subjacente ao BEB é que após uma colisão, a estação (ou nó) deve esperar um período aleatório antes de tentar retransmitir. Este período aleatório é escolhido de um conjunto de janelas de tempo que cresce exponencialmente com cada colisão consecutiva para esse pacote. Isso ajuda a distribuir de forma aleatória as retransmissões no tempo e reduz a probabilidade de colisões consecutivas [65].

Funcionamento:

1) Inicialização: Quando um nó tem um pacote para transmitir, ele primeiro verifica se o canal está livre. Se estiver livre por um determinado período (usualmente o tempo de difusão, $DIFS$ em Wi-Fi), pacote é transmitido.

2) Detecção de colisão: Se ocorrer uma colisão, o nó detetará a falha da transmissão (usualmente por falta de reconhecimento).

3) *Backoff*: Após a detecção de colisão, o nó entra no procedimento de *backoff*. Ele seleciona um número aleatório, k, de intervalos de *backoff* (*slot*) a partir do seguinte intervalo:

$$k \in [0, CW - 1] \tag{3.1}$$

   Onde, CW é a janela de contenção, que inicialmente é definida como $CWmin$, o valor mínimo da janela.

4) Dobro da janela: Após cada colisão, a janela de contenção, CW, é dobrada, até um máximo de $CWmax$. Assim, para cada retransmissão consecutiva, temos:

$$CW = min(2 \times CW, CWmax) \quad (3.2)$$

5) Espera e retransmissão: O nó espera k *slots* de tempo antes de tentar retransmitir. Se o canal estiver livre após esse tempo, o nó retransmite o pacote. Se outra colisão ocorrer, o processo de *backoff* é repetido.

6) Reinicialização: Uma vez que o pacote é transmitido com sucesso ou o número máximo de tentativas de retransmissão é atingido, o valor de CW é reiniciado para $CWmin$.

A principal vantagem do BEB é a sua capacidade de adaptar-se às condições da rede. Em redes pouco congestionadas, o algoritmo tende a permitir retransmissões mais rápidas, enquanto em redes mais congestionadas, ele espaça as tentativas de transmissão para reduzir a probabilidade de colisão [3]

3.1.1. *Slotted* ALOHA-BEB: Conceção e benefícios por esperar

O *Slotted* ALOHA, uma variante do protocolo ALOHA original, é estruturado de forma que as transmissões ocorram apenas no início de intervalos de tempo discretos, ou "*slots*"[66]. Esta sincronização reduz as colisões, mas ainda assim, em ambientes de alta densidade, as colisões podem ser frequentes. O BEB (*Binary Exponential Backoff*) foi introduzido para otimizar ainda mais o *Slotted* ALOHA, gerando o que chamamos de "*Slotted* ALOHA-BEB" [67].

Conceção do *Slotted* ALOHA-BEB

A ideia principal do BEB é evitar colisões subsequentes depois de uma primeira colisão. Se um pacote transmitido colidir, o nó não tenta retransmitir imediatamente, mas sim espera por um período aleatório determinado.

Esse tempo é multiplicado por dois a cada colisão subsequente até um valor máximo. Isso permite que, em situações de alta contenda, os nós não estejam continuamente a colidir uns com os outros, dando a cada nó uma janela mais clara para a transmissão [66].

Matematicamente, a janela de *backoff* W depois da i^{a} colisão é dada por:

$$W(i) = min(2^i \times W_0, Wmax) \tag{3.3}$$

onde W_0 é a janela inicial de backoff e $Wmax$ é a janela máxima permitida.

Isto significa que, após a primeira colisão, o nó escolherá aleatoriamente entre retransmitir no próximo *slot* ou esperar por mais um *slot*. Se ocorrer outra colisão, ele escolherá aleatoriamente entre 0 e 4 *slots* para esperar, e assim por diante.

Benefícios a Esperar:

- Redução de colisões: O BEB espaça as retransmissões, diminuindo a probabilidade de colisões subsequentes. Esta abordagem reduz as colisões mais eficientemente no contexto de *Slotted* ALOHA, uma vez que as transmissões estão confinadas a *slots* discretos.

- Aumento da eficiência do canal: Com uma diminuição nas colisões, a eficiência global do canal melhora, permitindo uma maior taxa de sucesso na entrega de pacotes.

- Adaptabilidade: O *Slotted* ALOHA-BEB pode adaptar-se dinamicamente às condições da rede. A adaptabilidade é ainda mais acentuada com a estruturação por *slots*, permitindo uma resposta mais rápida às mudanças nas condições da rede.

- Eficiência energética: As retransmissões reduzidas significam menos consumo de energia, o que é essencial em ambientes de RSSFs.

- *Fairness:* A natureza aleatória da espera pelo BEB garante que todos os nós sensores tenham uma oportunidade justa de transmitir, evitando que um único nó monopolize o canal.

3.2. Aprendizado por reforço e aplicação do *Q-learning* em RSSFs

O Aprendizado por Reforço (RL, do inglês, *Reinforcement Learning*) constitui uma área robusta e em expansão dentro do domínio de aprendizado de máquina [68]. Diferentemente da aprendizagem supervisionada, onde o modelo é treinado com dados previamente etiquetados, ou da aprendizagem não supervisionada, onde os dados não

têm etiquetas e o modelo procura por padrões, o RL é uma abordagem em que um agente aprende a tomar decisões ao interagir com um ambiente e receber recompensas ou penalizações com base nas ações tomadas.

O paradigma central do RL é baseado na ideia de que os agentes tomam ações que maximizam uma recompensa cumulativa esperada ao longo do tempo. O objetivo primário é encontrar uma política, que é uma estratégia de ação, que obtenha a maior recompensa a longo prazo [69]. Isto é particularmente útil em ambientes onde não se sabe inicialmente qual é a melhor ação a tomar e é necessário explorar diferentes ações para aprender a melhor estratégia.

Markov Decision Processes (MDP) são frequentemente utilizados como uma *framework* matemática para modelar problemas de AR. Um MDP fornece uma forma de descrever a relação entre as ações do agente, os estados do ambiente e as recompensas recebidas [70]. O algoritmo *Q-learning* é uma abordagem popular dentro do RL. A sua essência reside na estimação dos valores Q, que representam a recompensa esperada ao tomar uma ação em um determinado estado, seguindo uma política ótima. Com o tempo, através de iterações e interações com o ambiente, o agente atualiza estes valores Q até convergir para uma solução ótima [69].

A adoção do aprendizado por reforço em Redes de Sensores Sem Fios (RSSFs), como no caso do aperfeiçoamento do protocolo *Slotted* ALOHA, tem um enorme potencial[71]. Dada a natureza dinâmica e imprevisível das RSSFs, métodos adaptativos, como o RL, podem ser cruciais para otimizar a eficiência energética e a eficácia da rede.

3.2.1. Processo de Decisão de *Markov* (MDP)

Um Processo de Decisão de *Markov* é um modelo matemático usado para descrever sistemas que evoluem no tempo, onde as decisões tomadas a cada etapa influenciam os estados futuros do sistema e as recompensas associadas[70]. MDPs têm aplicações em várias áreas, desde engenharia a finanças e, notavelmente, em aprendizado por reforço.

Definição

Um MDP é definido por um conjunto de elementos:

- s: Um conjunto finito de estados.
- a: Um conjunto finito de ações.

- P: Uma função de transição de estado $P(s' \mid s, a)$, que representa a probabilidade de transitar do estado s para o estado s' ao tomar a ação a.

- R: Uma função de recompensa $R(s, a, s')$, que representa a recompensa esperada ao transitar do estado s para s' ao tomar a ação a.

- γ : Um fator de desconto no intervalo $[0, 1]$, que desconta recompensas futuras. Um valor de γ próximo de 0 faz o agente "miópico", enquanto um valor próximo de 1 faz com que o agente valorize recompensas a longo prazo.

Equações de *Bellman*

O valor esperado de um estado s sob uma política específica π, que mapeia estados em ações, é dado por:

$$V^{\pi}(s) = \mathbb{E}[R(s, \pi(s), s') + \gamma V^{\pi}(s') \mid s] \tag{3.4}$$

A equação acima é frequentemente chamada de equação de *Bellman* para políticas de valor. Além disso, a equação de *Bellman* para funções de valor de ação, que indica o valor de tomar uma ação a no estado s e depois seguir a política π, é dada por:

$$Q^{\pi}(s, a) = \mathbb{E}[R(s, a, s') + \gamma Q^{\pi}\big(s', \pi(s')\big) \mid s, a] \tag{3.5}$$

Política ótima

Uma política ótima é aquela que maximiza a função de valor em todos os estados. A equação de *Bellman* para valor ótimo é:

$$V^{*}(s) = \max_{a} [\, \mathbb{E}\,[R(s, a, s') + \gamma V^{*}(s') \mid s]] \tag{3.6}$$

E a equação de *Bellman* para a função de valor de ação ótima é:

$$Q^{*}(s, a) = \mathbb{E}[R(s, a, s') + \gamma \max_{a'} Q^{*}\,(s', a') \mid s, a] \tag{3.7}$$

Estas equações servem como base para muitos algoritmos em aprendizado por reforço, permitindo que agentes aprendam políticas que maximizem a recompensa esperada ao longo do tempo.

3.2.2. Introdução ao *Q-learning*: princípios e funcionamento

O *Q-learning* é uma técnica popular no campo do aprendizado por reforço, cujo objetivo é encontrar a melhor ação a ser tomada em cada estado, de modo a maximizar a recompensa esperada ao longo do tempo. Esta técnica é frequentemente utilizada em situações onde um agente, como um sensor numa rede, deve aprender a se comportar em um ambiente desconhecido, sem um modelo explícito desse ambiente [1].

A ideia central do *Q-learning* é usar uma função Q, que estima o valor de um par estado-ação. O valor Q representa a recompensa esperada a longo prazo ao se tomar uma ação a em um estado s, considerando-se uma política ótima. Em palavras simples, Q indica o "quão bom" é para o agente tomar uma ação a no estado s.

Funcionamento e atualização de *Q-values*:

A cada iteração, o agente observa o estado atual s, toma uma ação a, recebe uma recompensa r e observa o novo estado s'.

A função Q é atualizada usando a seguinte fórmula:

$$Q_{new}(s,a) \leftarrow Q(s,a) \; + \; \alpha \, [r + \gamma \max_{a'} Q\,(s', a') - Q(s,a)] \qquad (3.8)$$

Onde:

- $Q_{new}(s,a)$: é o novo valor da função Q para o estado s e ação a.
- $Q(s,a)$: é o valor atual da função Q para o estado s e ação a.
- α: é a taxa de aprendizagem, que determina o quanto a nova estimativa afetará o valor Q atual.
- r: é a recompensa obtida após a execução da ação a no estado s.
- γ: é o fator de desconto, que modela a importância das recompensas futuras. Um valor de γ próximo de 1 faz com que o agente valorize recompensas a longo prazo, enquanto um valor próximo de 0 o faz focar em recompensas imediatas.
- $\max_{a'} Q\,(s', a')$: é o valor máximo de Q para o novo estado s', ou seja, a melhor ação possível a ser tomada após a ação atual.

Conforme o agente continua a explorar o ambiente e atualizar a função Q através desta equação, a função Q converge progressivamente para Q^*, que é a função de valor ótimo. Neste ponto, quando o agente consulta Q^*, está efetivamente consultando a melhor ação possível em qualquer estado, dado que seguirá uma política ótima daí em diante.

Aplicação do *Q-learning* em RSSFs

Em redes de sensores sem fios, o *Q-learning* pode ser usado para otimizar decisões, como quando transmitir dados, escolher rotas ou gerenciar energia. Por exemplo, em um cenário de alocação dinâmica de canal, um sensor pode usar *Q-learning* para decidir em qual canal transmitir, levando em conta a qualidade do canal, a interferência e outros fatores, visando maximizar a eficiência da transmissão [72].

3.2.3. Q-ALOHA: Integração do *Q-learning* no *Slotted* ALOHA

A integração do *Q-learning* com o *Slotted* ALOHA, denominado aqui como Q-ALOHA, representa uma fusão promissora entre técnicas de aprendizado por reforço e protocolos MAC tradicionais. Este cruzamento almeja melhorar a eficiência e a adaptabilidade do protocolo ALOHA em ambientes com variação dinâmica de tráfego [73].

O *Q-learning* é um algoritmo de aprendizado por reforço que não requer um modelo do ambiente e pode ser usado para encontrar uma ação que maximiza a recompensa cumulativa esperada[72]. Em termos matemáticos, o objetivo do *Q-learning* é aprender uma política π^* que maximiza o retorno esperado a partir de qualquer estado inicial s.

$$Q^*(s,a) = \max_{\pi} \mathbb{E}\left[R_t \mid s_t = s, a_t = a\right] \tag{3.9}$$

Onde $Q^*(s,a)$ é a função de valor de ação ótima, representando o retorno esperado quando se inicia no estado s, toma ação a e depois segue a política ótima, e R_t é a recompensa imediata após a ação a.

3.2.4. Adaptação do *Q-learning* ao *Slotted* ALOHA

A ideia principal por trás do Q-ALOHA é adaptar as decisões de transmissão dos nós sensores, com base nas recompensas e penalidades percebidas durante as tentativas anteriores de transmissão. Se um nó sensor perceber que há muitas colisões ocorrendo em um determinado *slot*, ele pode decidir atrasar sua transmissão, esperando um melhor cenário de canal em futuros *slots*.

Para implementarmos essa ideia, é preciso entender algumas definições:

- **Estado** s: Representa o resultado percebido da última tentativa de transmissão (por exemplo, sucesso, falha devido a colisão ou canal ocupado).
- **Ação** a: Representa a decisão do nó sensor em transmitir ou adiar sua transmissão para um próximo slot
- **Recompensa** R: Um valor positivo para uma transmissão bem-sucedida, valor negativo para colisão, e valor zero ou ligeiramente negativo para a não transmissão.

Com base nesse *framework*, cada nó atualiza sua política de transmissão usando a regra de atualização *Q-learning*:

$$Q_{new}(s,a) \leftarrow Q(s,a) \; + \; \alpha \left[R + \gamma \max_{a'} Q\left(s', a'\right) - Q(s,a)\right] \qquad (3.10)$$

Onde α é a taxa de aprendizado e γ é o fator de desconto.

Expectativas de desempenho

Ao integrar *Q-learning* ao *Slotted* ALOHA, espera-se que os nós sensores da rede adaptem suas decisões de transmissão de forma a minimizar colisões e maximizar a utilização do canal. Assim, em ambientes de tráfego dinâmico, o Q-ALOHA poderá apresentar um desempenho superior em comparação com o *Slotted* ALOHA tradicional, principalmente em termos de taxa de sucesso de transmissão e eficiência energética.

3.3. Conclusão

Neste capítulo, debruçámo-nos sobre a integração de estratégias avançadas como o *Binary Exponential Backoff* (BEB) e o *Q-learning* em Redes de Sensores Sem Fios (RSSFs), com o intuito de garantir melhor eficiência energética nas RSSFs principalmente baseadas no padrão IEEE 802.15.4. Iniciando com o BEB, explorámos os seus princípios fundamentais e o seu mecanismo intrínseco de ajuste de tempos de espera, visando minimizar colisões em situações de retransmissão. Ao introduzir este conceito ao *Slotted* ALOHA, observámos como a introdução de uma espera adaptativa, baseada em tentativas anteriores, pode reduzir a probabilidade de colisões consecutivas, melhorando assim a eficiência do canal.

Na segunda metade do capítulo, aprofundámos o campo do aprendizado por reforço e, especificamente, como o *Q-learning* pode ser integrado às RSSFs. Ao entender o Processo de Decisão de *Markov* (MDP) e os princípios fundamentais por trás *do Q-learning*, ficou evidente o potencial desta técnica em adaptar dinamicamente as decisões dos nós sensores baseado em recompensas e punições acumuladas, otimizando o uso do canal. A consequente integração do *Q-learning* ao *Slotted* ALOHA, denominada Q-ALOHA, mostrou-se uma promissora abordagem adaptativa, em que cada nó sensor aprende a melhor estratégia de transmissão com base em experiências anteriores.

Em suma, este capítulo enfatizou a importância e o potencial das abordagens adaptativas no contexto das RSSFs. Enquanto o BEB oferece uma solução baseada na experiência de colisões passadas, o *Q-learning* proporciona uma abordagem mais sofisticada, permitindo uma adaptação proativa baseada em um conjunto mais amplo de experiências acumuladas. Estas estratégias, quando implementadas de forma adequada, têm o potencial de revolucionar a forma como os nós sensores comunicam entre si, tornando as RSSFs mais resilientes, eficientes e adaptáveis às dinâmicas do ambiente de rede.

Capítulo 4

4. Análise e discussão dos resultados

Neste capítulo, colocamos em prática toda a abordagem teórica e fórmulas matemáticas já estudadas por cada um dos protocolos usados para a nossa análise. Realizamos uma abrangente simulação em diferentes cenários para compreender e avaliar o comportamento de cada um deles e, em seguida, discutimos os resultados.

Antes de tudo, começaremos por compreender o comportamento do *Slotted* ALOHA aplicado às RSSFs por meio de simulações usando o MATLAB. No Cenário 1, implementamos o protocolo *Slotted* ALOHA para analisar seu desempenho nas RSSFs.

4.1. Cenário 1 – Implementação do *Slotted* ALOHA para as RSSFs

Neste primeiro cenário, baseamos nossos estudos de simulação no MATLAB para avaliar o comportamento do protocolo *Slotted* ALOHA nas RSSFs, levando em conta um determinado número de repetições. Utilizamos o código aberto [74] (apresentado no Apêndice A) para nos auxiliar nesse processo. Inicialmente, fizemos pequenas alterações no código, implementando uma variável m que nos ajudou a determinar o número de repetições que o programa poderia realizar na simulação.

Definimos os parâmetros iniciais de acordo com o real funcionamento das RSSFs e criamos uma estrutura no código que nos ajudou a armazenar os dados de saída das variáveis e o número de usuários (no caso, dispositivos da rede). Calculamos a média por número de repetições para a simulação já definida anteriormente (m). Com isso, foi possível realizar os *plots* dos resultados para uma melhor análise. Por fim, calculamos o intervalo de confiança. Na figura abaixo, serão apresentados os resultados obtidos para diferentes eventos:

Analisamos as métricas de saída pretendidas em relação ao número de dispositivos da rede, com $m = 20$, sendo m o número de repetições da simulação.

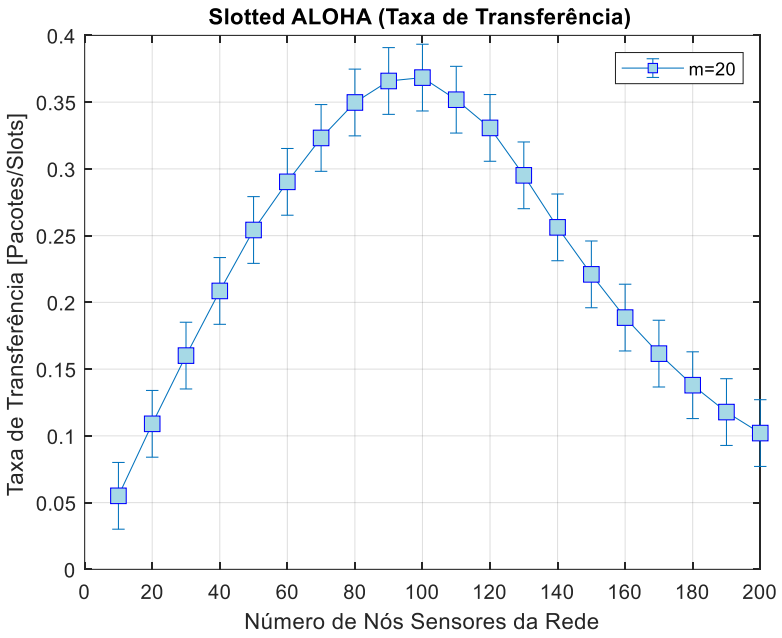

Figura 4.1.1 - Taxa de Transferência VS. Número de Nós Sensores da Rede [2].

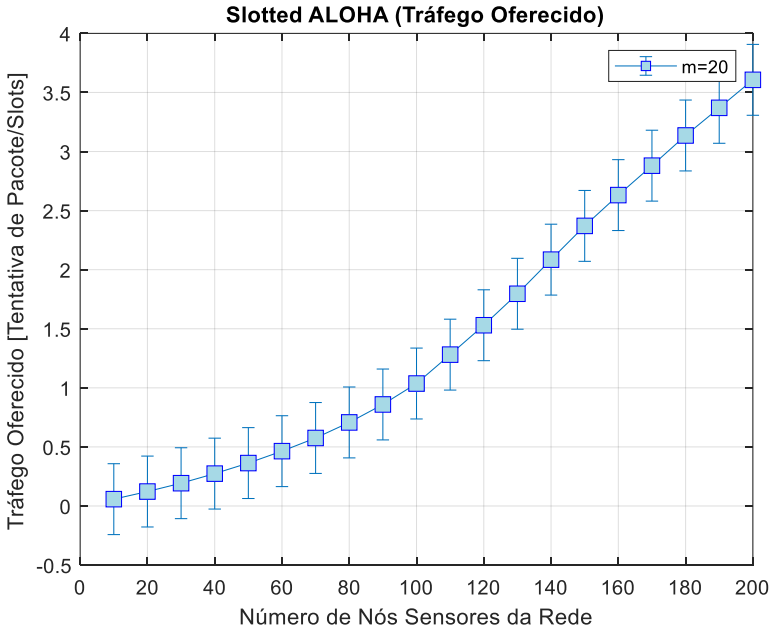

Figura 4.1.2 - Tráfego Oferecido VS. Número de Nós Sensores da Rede [3].

[2] A figura 4.1.1 ilustra como a taxa de transferência varia conforme o número de nós sensores na rede aumenta, com 20 repetições ou amostras de simulação (m). Observamos que, à medida que o número de nós sensores cresce, a taxa de transferência tende a diminuir devido ao aumento da competição pelo acesso ao canal de comunicação.

[3] A figura 4.1.2 representa como o tráfego oferecido evolui com o aumento do número de nós sensores na rede, considerando 20 repetições ou amostras na simulação ($m = 20$). É percetível que, à medida que mais nós sensores são adicionados, o tráfego oferecido também aumenta, o que pode resultar em um aumento de colisões e, portanto, afetar a qualidade da rede.

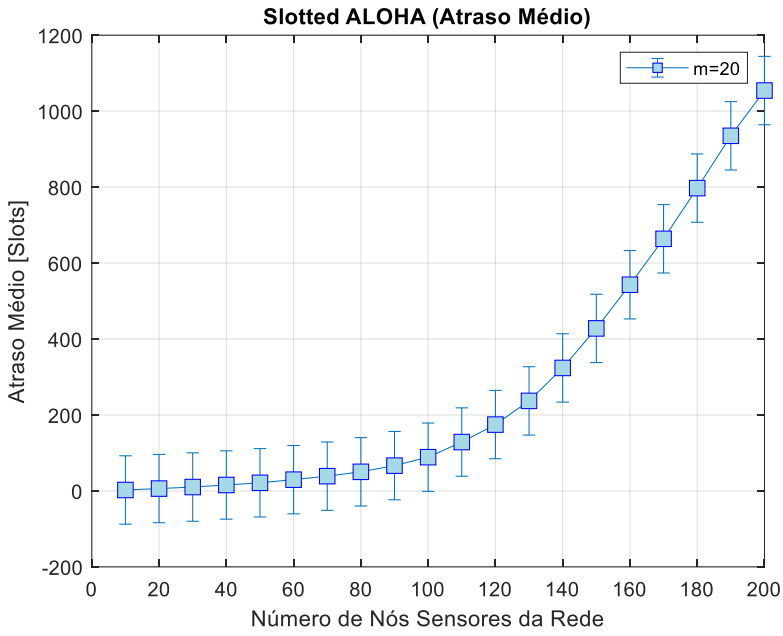

Figura 4.1.3 - Atraso Médio VS. Número de Nós Sensores da Rede [4].

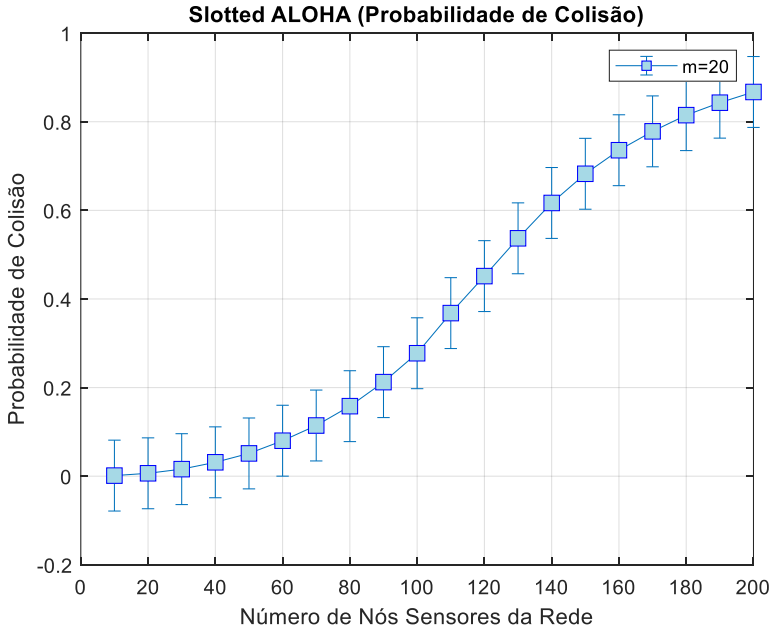

Figura 4.1.4 - Probabilidade de Colisão VS. Número de Nós Sensores da Rede [5].

[4] A figura 4.1.3 ilustra como o atraso médio se comporta em relação ao número de nós sensores na rede, com 20 repetições ou amostras de simulação ($m = 20$). À medida que o número de nós sensores aumenta, o atraso médio tende a aumentar, indicando que a rede pode experimentar maior latência à medida que mais nós sensores competem pelo canal de comunicação.

[5] Na figura 4.1.4, observamos como a probabilidade de colisão de pacotes varia com o aumento do número de nós sensores na rede, considerando 20 repetições de simulação ($m = 20$). A probabilidade de colisão aumenta à medida que mais nós sensores competem pelo canal, destacando a importância de estratégias eficazes de controle de acesso ao meio.

Depois, analisamos o comportamento do protocolo em relação a diversos eventos possíveis, levando em consideração a média obtida a partir da simulação com 20 repetições.

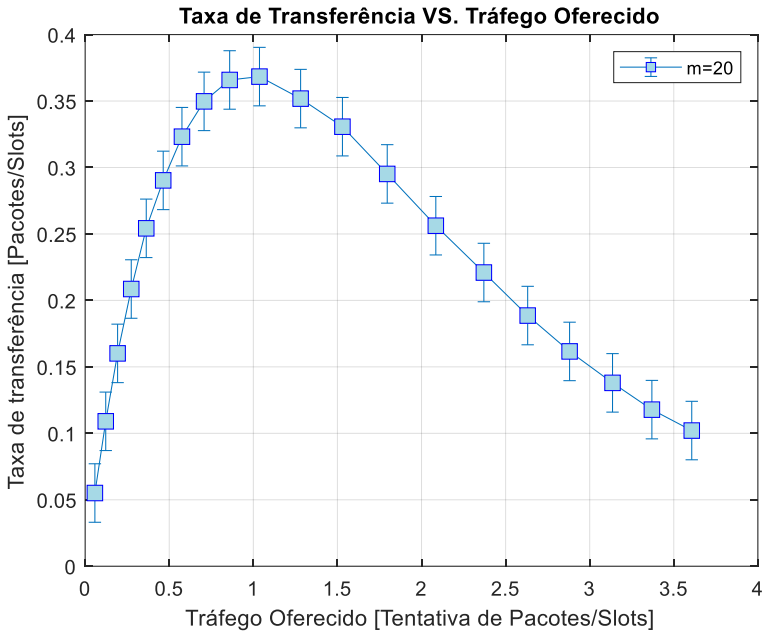

Figura 4.1.5 - Taxa de Transferência de Pacotes VS. Tráfego Oferecido.

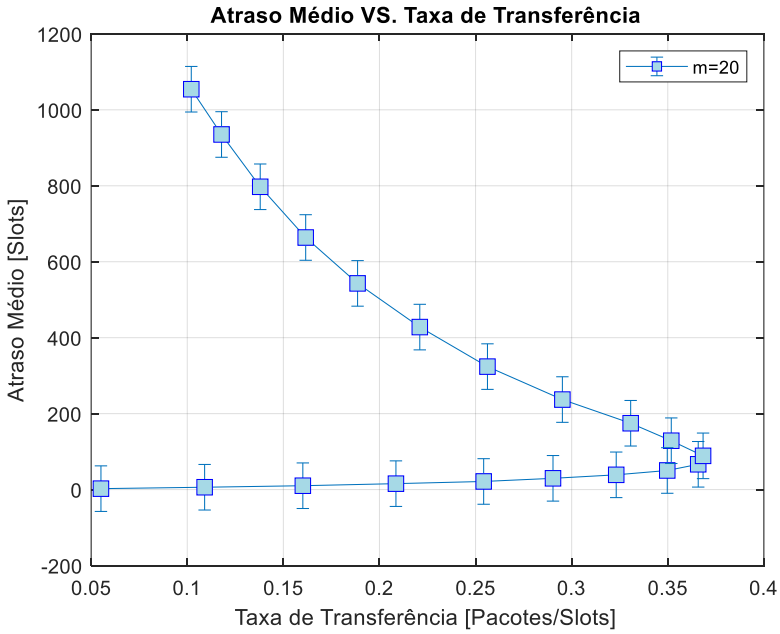

Figura 4.1.6 - Atraso Médio VS. Taxa de Transferência de Pacotes.

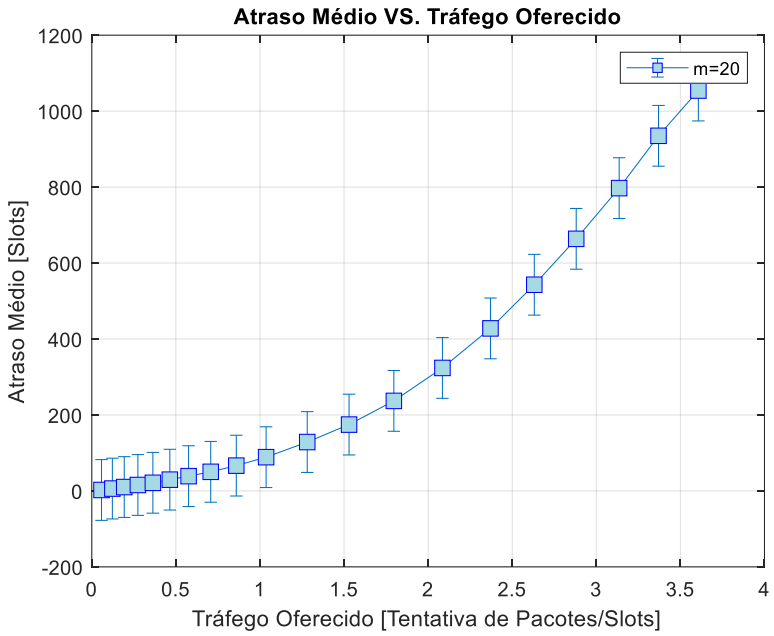

Figura 4.1.7 - Atraso Médio VS. Tráfego Oferecido.

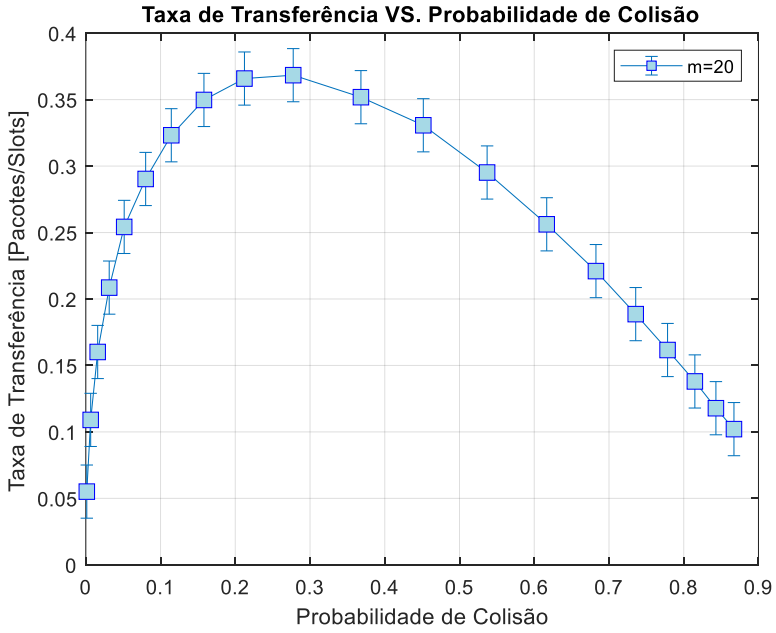

Figura 4.1.8 - Taxa de Transferência de Pacotes VS. Probabilidade de Colisão.

Durante essas simulações, conseguimos compreender como o protocolo *Slotted* ALOHA se comporta em diferentes cenários. Notamos que sua taxa de transferência tende a aumentar até atingir o máximo e, em seguida, diminui até chegar a zero.

Percebemos também que, à medida que o número de dispositivos na rede aumenta, o tráfego oferecido aumenta, resultando em maior atraso e probabilidade de colisão. Além disso, apresentamos uma série de gráficos comparativos para analisar o desempenho do protocolo na rede. Inicialmente, observamos a relação entre a taxa de transferência e o tráfego oferecido, alcançando uma eficiência máxima de 37 pacotes por intervalo quando $G = 1$.

Em seguida, analisamos a relação entre o atraso médio e a taxa de transferência de pacotes, percebendo que o atraso médio tende a aumentar à medida que a taxa de transferência cresce. Posteriormente, examinamos a relação entre o atraso médio e o tráfego oferecido, constatando que o atraso aumenta à medida que o tráfego aumenta.

Finalmente, analisamos a taxa de transferência em relação à probabilidade de colisão, concluindo que o protocolo *Slotted* ALOHA é eficiente em um curto intervalo de probabilidade e, posteriormente, diminui à medida que a probabilidade de colisão aumenta.

Com esse entendimento e após um estudo abrangente para analisar o comportamento do *Slotted* ALOHA em diferentes cenários, estamos prontos para explorar o Cenário 2. Nessa próxima etapa, concentraremos nossa análise nos protocolos CSMA, *Slotted* ALOHA, *Slotted* ALOHA-BEB e Q-ALOHA para diferentes cenários nas RSSFs, baseando-nos no padrão IEEE 802.15.4. Para isso, definiremos os parâmetros iniciais conforme apresentados na Tabela 4.1.1, seguindo as diretrizes do referido padrão IEEE 802.15.4.

Parâmetros iniciais:

Tabela 4.1.1 - Parâmetros iniciais para a rede.

Parâmetros	Valores
Taxa de transmissão de dados	250 kbps
Taxa de recepção de dados	250 kbps
Energia de transmissão	50 mJ
Energia de recepção	50 mJ
Tamanho do pacote de dados	1044 bits
Número de *slots*	1000 *slots*

4.2. Cenário 2 – Pacotes Entregue Acumulados

Com os parâmetros iniciais definidos, começamos por implementar o código no MATLAB para analise do segundo cenário. Neste cenário 2, iremos estudar e avaliar a dinâmica de cada um dos protocolos no que concerne o envio de pacotes acumulados. Afinal, a eficiência na entrega de pacotes é fundamental, especialmente em redes de sensores, onde a energia é uma preocupação primordial.

A retransmissão de pacotes devido a colisões, atrasos ou outros problemas de comunicação pode levar ao consumo desnecessário de energia. Além disso, a entrega de pacotes de forma eficiente e confiável garante que os dados dos sensores sejam comunicados à estação base ou a outros nós sensores, permitindo um monitoramento e análise adequado dos ambientes ou sistemas que estão sendo observados.

Por exemplo:

Se temos um vetor que representa a entrega de pacotes ao longo do tempo como:

$$Pacotes = [1,0,1,1,0,0,1]$$

Onde *1* indica que um pacote foi entregue com sucesso e *0* indica que não houve entrega no respetivo *slot*/tempo. O Acumulado desses pacotes seria:

$$Acumulados = [1,1,2,3,3,3,4]$$

Onde cada elemento da série representa o total acumulado de pacotes entregues até aquele momento ou *slot*.

Portanto, ao analisarmos o acumulado de pacotes entregues, conseguimos ter uma ideia da taxa de sucesso ao longo do tempo e avaliar a eficácia de um protocolo ou sistema em garantir a entrega de pacotes. Essa perspetiva cumulativa é particularmente útil para entender tendências e comparar o desempenho de diferentes sistemas ou protocolos ao longo de um período. por esta razão implementamos o cenário 2 de modo a compreender este comportamento, e tivemos os seguintes resultados (apresentado na Figura 4.2.1).

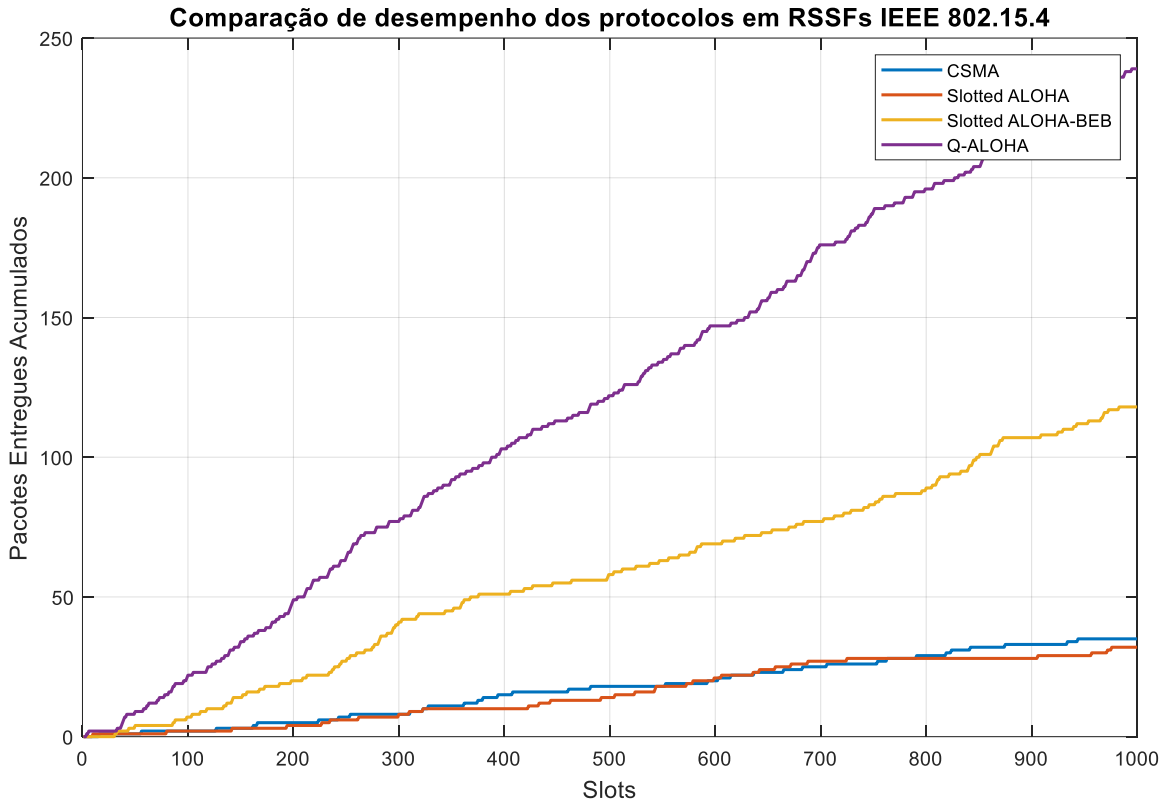

Figura 4.2.1 - Pacotes Entregues Acumulados.

Discussão do cenário 2:

Neste cenário, observamos a implementação de quatro protocolos de acesso ao meio distintos para redes de sensores sem fios baseadas no padrão IEEE 802.15.4: Q-ALOHA, *Slotted* ALOHA-BEB, CSMA e *Slotted* ALOHA.

O Q-ALOHA, que incorpora técnicas de aprendizagem por reforço, apresentou o desempenho mais elevado, com aproximadamente 239 pacotes entregues acumulados ao longo dos *slots*. Este resultado era esperado, uma vez que a técnica procura aprender dinamicamente a melhor probabilidade de transmissão para maximizar a entrega de pacotes. A adaptabilidade intrínseca do *Q-learning* permite que os nós sensores ajustem suas decisões de transmissão com base nas experiências anteriores, maximizando assim a eficiência do canal.

Por outro lado, o *Slotted* ALOHA-BEB, que utiliza o mecanismo de *Binary Exponential Backoff*, mostrou-se superior ao CSMA e ao *Slotted* ALOHA simples, com aproximadamente 118 pacotes entregues acumulados. O BEB permite que os nós sensores ajustem dinamicamente seus intervalos de *backoff* após colisões, permitindo

assim um uso mais eficiente do canal do que o *Slotted* ALOHA simples, que não tem este mecanismo de ajuste. Por sua vez, o CSMA, mesmo sendo um protocolo amplamente utilizado, neste cenário específico mostrou um desempenho inferior quando comparado ao Q-ALOHA e ao *Slotted* ALOHA-BEB com 35 pacotes entregues acumulados. Isso pode ser atribuído a vários fatores, incluindo a densidade de nós sensores na rede e a configuração do canal. E finalmente, o *Slotted* ALOHA, na sua forma mais básica, apresentou o desempenho mais baixo entre todos, com aproximadamente 32 pacotes entregues acumulados. Este resultado ilustra as limitações do protocolo quando não há mecanismos adicionais de ajuste ou aprendizagem.

A partir dos resultados observados, fica evidente que a integração de mecanismos de aprendizagem ou adaptação, como o *Q-learning* ou o *Binary Exponential Backoff*, pode significativamente melhorar o desempenho de protocolos de acesso ao meio em Redes de Sensores Sem Fios (RSSFs).

O Q-ALOHA, com a sua capacidade de aprendizagem dinâmica, mostrou-se especialmente promissor, superando os outros protocolos avaliados. O CSMA e o *Slotted* ALOHA, enquanto protocolos clássicos, mostraram limitações neste cenário específico, reforçando a necessidade de evolução e adaptação destas técnicas à medida que a densidade e as exigências das redes sem fios evoluem.

4.3. Cenário 3 – Latência Média

Neste cenário fizemos um estudo comparativo da latência media nos protocolos CSMA, *Slotted* ALOHA, *Slotted* ALOHA-BEB e Q-ALOHA. Como referido anteriormente, a latência nas RSSFs baseadas no padrão IEEE 802.15.4 é muito importante, as redes com latência elevada podem não ser adequadas para aplicações em tempo real, como controle de sistemas, jogos ou aplicações VoIP.

Por outra, dispositivos que frequentemente colidem e têm de retransmitir gastam mais energia. Assim, protocolos que minimizam a latência podem, indiretamente, aumentar a vida útil da bateria dos dispositivos na rede. Daí a grande importância de analisarmos este aspeto para avaliarmos a eficiência energética nos protocolos de RSSFs.

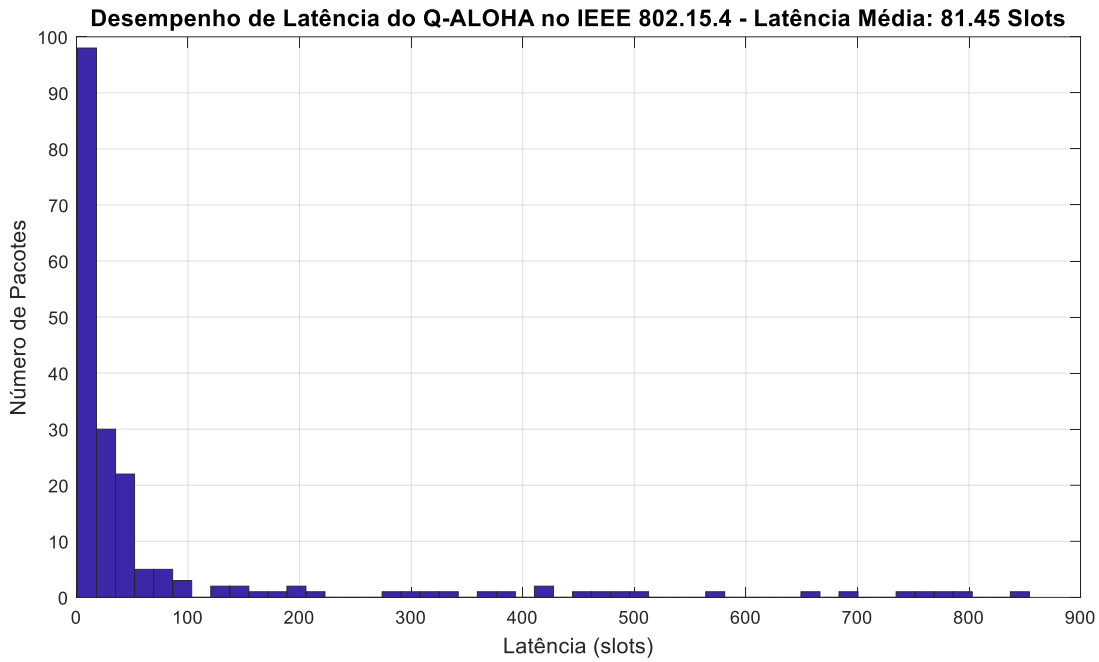

Figura 4.3.1 – Latência média do protocolo Q-ALOHA.

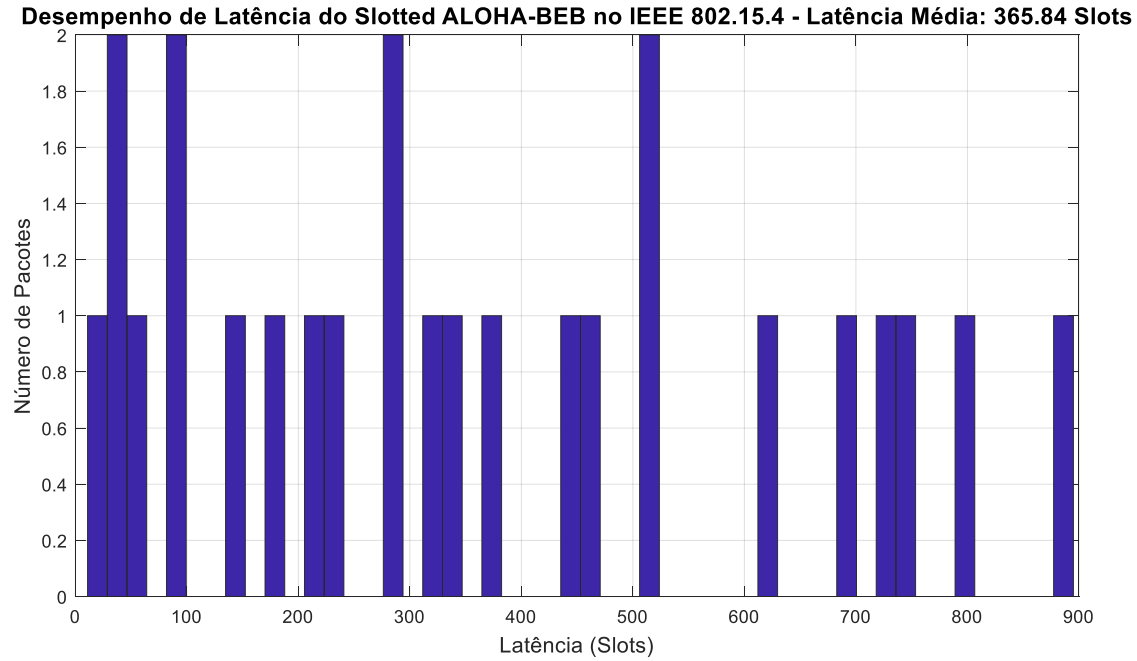

Figura 4.3.2 – Latência média do protocolo *Slotted* ALOHA-BEB.

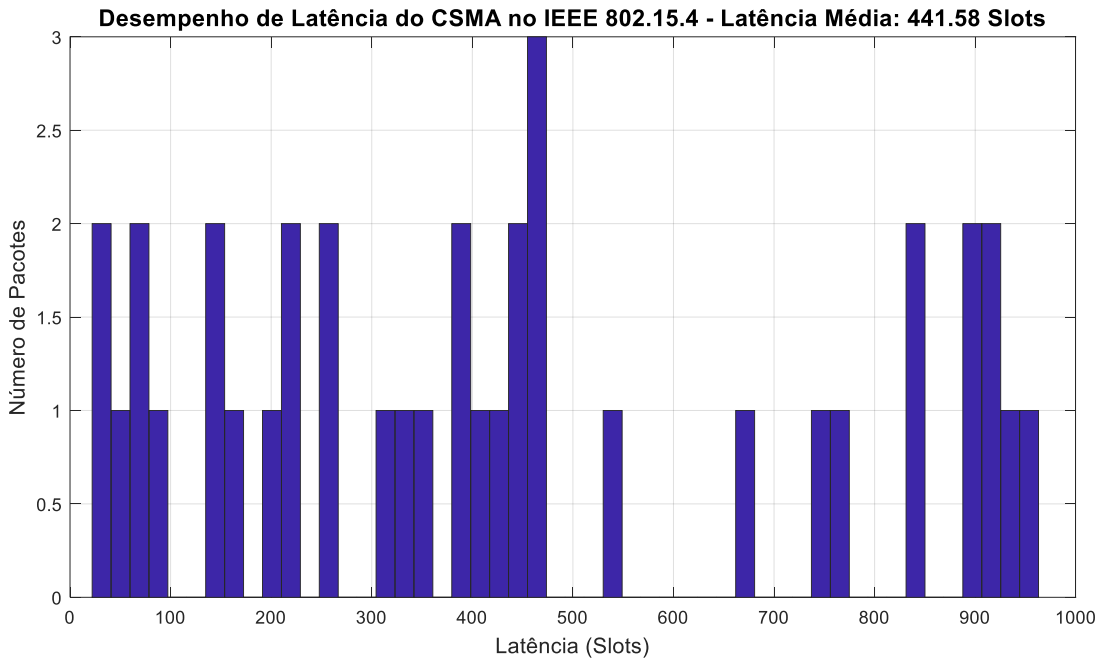

Figura 4.3.3 – Latência média do protocolo CSMA.

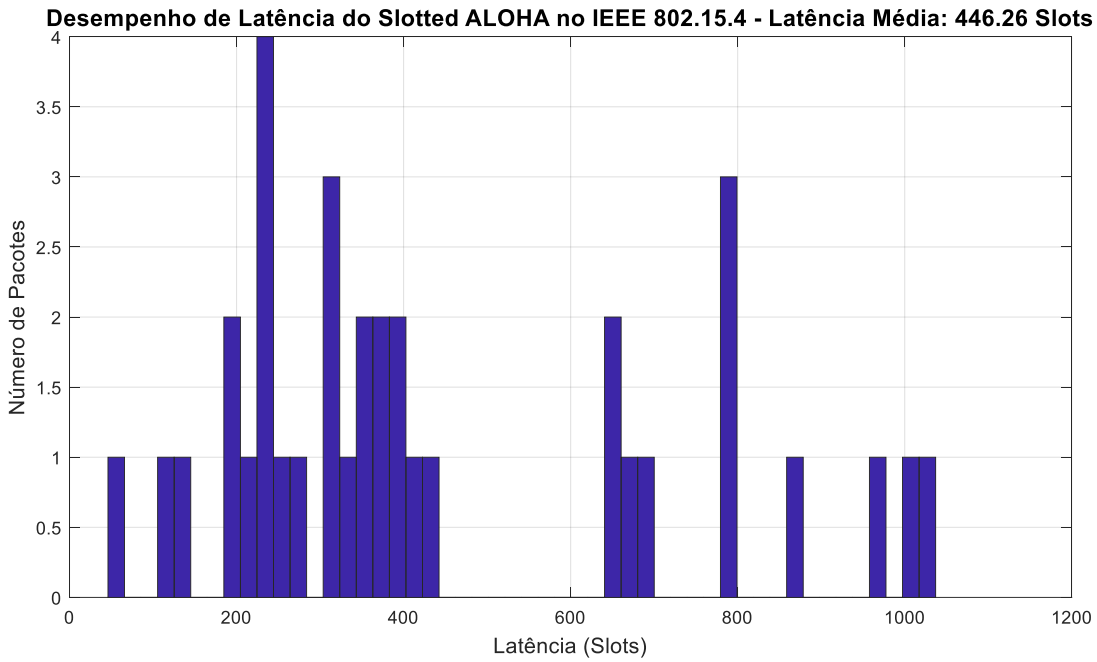

Figura 4.3.4 – Latência média do protocolo *Slotted* ALOHA.

Discussão do cenário 3:

- **Q-ALOHA:** Este protocolo apresentou a menor latência média entre os quatro protocolos, com 81,45 *slots*. Esta melhoria é uma consequência da abordagem de aprendizado por reforço, que permite que cada nó sensor ajuste adaptativamente sua estratégia de transmissão com base nas recompensas obtidas de transmissões anteriores. O Q-ALOHA, por meio do *Q-learning*, busca continuamente otimizar as decisões de transmissão de cada nó sensor, minimizando colisões e, consequentemente, a latência.

- ***Slotted* ALOHA-BEB:** Apesar de sua latência média ser significativamente maior que o Q-ALOHA, com 365,84 *slots*, o *Slotted* ALOHA com BEB mostra-se mais eficiente que os outros dois protocolos. O *Binary Exponential Backoff* ajuda a espaçar as retransmissões após colisões, o que pode reduzir a probabilidade de colisões subsequentes.

- **CSMA**: Com uma latência média de 441,58 *slots*, o CSMA fica atrás do Q-ALOHA e do *Slotted* ALOHA-BEB. o CSMA (*Carrier Sense Multiple Access)* tenta detetar o meio antes de transmitir, mas em ambientes com muitos nós sensores e tráfego intenso, ainda pode haver um alto número de colisões, resultando em maior latência.

- ***Slotted* ALOHA:** Este protocolo tem uma latência média muito próxima à do CSMA, com 446,26 *slots*. Embora seja simples e não necessite de detecção de portadora como o CSMA, sem mecanismos adicionais como BEB ou aprendizado por reforço, ele pode sofrer de muitas colisões, especialmente quando a rede está congestionada.

Dentre os quatro protocolos testados, o Q-ALOHA demonstrou novamente ser o mais eficiente em termos de latência, seguido pelo *Slotted* ALOHA-BEB, CSMA e, finalmente, pelo *Slotted* ALOHA. A eficácia do Q-ALOHA pode ser atribuída ao uso de técnicas de aprendizado por reforço, que permitem uma adaptação em tempo real às condições da rede, otimizando a decisão de transmissão para minimizar a latência. O *Slotted* ALOHA-BEB, apesar de menos eficiente que o Q-ALOHA, mostra que a incorporação de mecanismos adicionais, como o *Binary Exponential Backoff* (BEB), pode melhorar significativamente o desempenho do *Slotted* ALOHA tradicional.

Capítulo 5

5. Conclusão e Trabalhos Futuros

5.1. Conclusões Gerais

Ao longo desta dissertação, exploramos os diversos protocolos de acesso ao meio com foco de otimizar o desempenho e eficiência energética em Redes de Sensores Sem Fios (RSSFs) baseadas no padrão IEEE 802.15.4. A escolha do protocolo adequado é fundamental para maximizar a vida útil da rede e garantir uma comunicação eficiente entre os nós sensores.

Este estudo revelou que o Q-ALOHA, que integra técnicas de aprendizado por reforço, especificamente o *Q-learning*, apresenta uma notável superioridade em termos de latência e em acumular pacotes entregues em comparação com os protocolos tradicionais, como o CSMA, *Slotted* ALOHA e a combinação do *Slotted* ALOHA-BEB. Esta eficiência deve-se, em grande parte, à capacidade dos nós sensores de adaptar-se dinamicamente às condições da rede, minimizando colisões e otimizando o tempo de transmissão.

Também é de notar que a integração do *Binary Exponential Backoff* (BEB) no Slotted ALOHA melhorou seu desempenho, mas ainda assim ficou aquém do Q-ALOHA. O CSMA, embora seja um padrão comprovado, mostrou-se menos eficiente em cenários de alta densidade, reforçando a necessidade de explorar alternativas mais adaptáveis.

5.2. Trabalhos Futuros

- Adaptação dinâmica do protocolo: Considerando a diversidade de cenários onde as redes de sensores sem fios podem operar, seria interessante desenvolver um mecanismo que permita a adaptação dinâmica do protocolo em uso. Por exemplo, a rede poderia alternar entre Q-ALOHA e CSMA dependendo das condições de tráfego e densidade de nós sensores.

- Redes neurais em protocolos MAC: A implementação de redes neurais para tomada de decisão no protocolo MAC pode ser uma abordagem inovadora. Essas

redes poderiam aprender e adaptar-se em tempo real às mudanças nas condições da rede, otimizando o desempenho com base em experiências anteriores.

- Segurança em protocolos MAC adaptativos: Com a crescente necessidade de segurança nas comunicações, seria relevante explorar como os protocolos MAC adaptativos, como o Q-ALOHA, podem ser projetados para resistir a ataques, tais como *jamming* ou *spoofing*, sem comprometer a sua eficiência.

- Integração de IoT e *edge computing*: Com a crescente ascensão do *edge computing*, um estudo sobre como os nós sensores sem fios podem processar dados localmente e tomar decisões de transmissão baseadas nesse processamento seria valioso. Isto poderia reduzir a latência geral e o tráfego na rede, ao evitar a transmissão de dados desnecessários.

- Otimização Multi-objetivo: Em vez de focar-se apenas na latência ou eficiência energética, um algoritmo de otimização multiobjectivo poderia ser desenvolvido para encontrar um equilíbrio entre diferentes métricas, garantindo um desempenho holístico otimizado.

- Integração de redes 5G e RSSFs: Com a implantação crescente de redes 5G, investigar como as redes de sensores sem fios podem ser integradas a este novo padrão e quais os desafios e benefícios desta integração, particularmente em termos de latência e *throughput*, seria um campo frutífero de pesquisa.

- Protocolos MAC para RSSF Heterogéneas: Em muitas aplicações, a rede de sensores pode consistir em diferentes tipos de nós sensores com diferentes capacidades. Criar protocolos MAC que podem acomodar essa heterogeneidade, garantindo a eficiência, é um desafio intrigante.

Estes trabalhos futuros são sugestões baseadas em tendências tecnológicas atuais e nas necessidades identificadas durante a nossa investigação. O campo das redes de sensores sem fios é vasto e em constante evolução, e a integração de técnicas avançadas de aprendizado de máquina, processamento de sinais e otimização pode abrir caminho para soluções inovadoras.

Referências Bibliográficas

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, “Middleware for internet of things: A survey,” *IEEE Internet Things J*, vol. 3, no. 1, pp. 70–95, Feb. 2016.

[3] X. Vilajosana *et al.*, “6TiSCH: Industrial Performance for IPv6 Internet of Things Networks,” *Proceedings of the IEEE*, vol. 2019, no. 6, pp. 1153–1165.

[4] Statista Research Department, Total number of connected devices worldwide from 2019 to 2030, Statista, 2021.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet Things J*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[6] O. O. Ogundile and A. S. Alfa, “A survey on an energy-efficient and energy-balanced routing protocol for wireless sensor networks,” *Sensors (Switzerland)*, vol. 17, no. 5, May 2017.

[7] R. Soua and P. Minet, “A survey on energy efficient techniques in wireless sensor networks,” in *Proceedings of 2011 4th Joint IFIP Wireless and Mobile Networking Conference, WMNC 2011*, 2011.

[8] M. Zareei, A. K. M. Muzahidul Islam, S. Baharun, C. Vargas-Rosales, L. Azpilicueta, and N. Mansoor, “Medium access control protocols for cognitive radio ad hoc networks: A survey,” *Sensors (Switzerland)*, vol. 17, no. 9. MDPI AG, Sep. 16, 2017.

[9] T. S. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2002.

[10] William. Stallings and William. Stallings, *Wireless communications, and networks*. Pearson Prentice Hall, 2005.

[11] H. Singh, B. K. Kanaujia, A. Kumar, K. Srivastava, and S. Kumar, “Wideband textile multiple-input-multiple-output antenna for industrial, scientific and medical (ISM)/wearable applications,” *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 30, no. 12, Dec. 2020.

[12] R. Soua and P. Minet, "A Survey on Energy Efficient Techniques in Wireless Sensor Networks," INRIA, Rocquencourt, 78153 Le Chesnay cedex, France. 2011.

[13] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[14] International Symposium on Wireless Communication Systems (ISWCS): Proceedings. 2012.

[15] M. Chiang and T. Zhang, “Fog and IoT: An Overview of Research Opportunities,” *IEEE Internet of Things Journal*, vol. 3, no. 6. Institute of Electrical and Electronics Engineers Inc., pp. 854–864, Dec. 01, 2016.

[16] A. A. Khan, M. H. Rehmani, and M. Reisslein, “Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols,” *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 860–898, 2016.

[17] T. Yaqoob, H. Abbas, and M. Atiquzzaman, “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3723–3768, Oct. 2019.

[18] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, and J. Zhang, “Overview of Millimeter Wave Communications for Fifth Generation (5G) Wireless Networks-With a Focus on Propagation Models,” *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12. Institute of Electrical and Electronics Engineers Inc., pp. 6213–6230, Dec. 01, 2017.

[19] S. Cherukuvada, "A Survey on Research Challenges in Wireless Sensor Network," Department of Computer Science and Engineering, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhrapradesh, India. 2020.

[20] J. E. Balota, C. Pattinson, A.-L. Kor, "Wireless Personal Area Networks: A Survey of Low-Rate and Low-Power Network Technologies," School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK. 2017.

[21] F. Boavida, R. M. Silva, and J. Sá Silva, Redes de Sensores Sem Fios. Lisboa FCA, 2016.

[22] C. Bambang and D. Kuncoro, “Miniature and Low-Power Wireless Sensor Node Platform: State of the Art and Current Trends,” 2014.

[23] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[24] A. Ali, Y. Ming, S. Chakraborty, and S. Iram, “A comprehensive survey on real-time applications of WSN,” *Future Internet*, vol. 9, no. 4. MDPI AG, 2017.

[25] Institute of Electrical and Electronics Engineers. Madras Section and Institute of Electrical and Electronics Engineers, *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*.

[26] K. S. Adu-Manu, N. Adam, C. Tapparello, H. Ayatollahi, and W. Heinzelman, "Energy-harvesting wireless sensor networks (EH-WSNs): A review," *ACM Transactions on Sensor Networks*, vol. 14, no. 2. Association for Computing Machinery, Mar. 01, 2018.

[27] H. Elahi, K. Munir, M. Eugeni, S. Atek, and P. Gaudenzi, "Energy harvesting towards self-powered iot devices," *Energies*, vol. 13, no. 21. MDPI AG, Oct. 22, 2020.

[28] C. H. Cao, Y. N. Tang, D. Y. Huang, W. M. Gan, and C. Zhang, "IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security," *Security and Communication Networks*, vol. 2021, 2021.

[29] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Proceedings - CIMSim 2011: 3rd International Conference on Computational Intelligence, Modelling and Simulation*, 2011, pp. 308–311.

[30] X. Zhang, Y. Liu, and Y. Zhang, "A Secure Clock Synchronization Scheme for Wireless Sensor Networks Against Malicious Attacks," *J Syst Sci Complex*, vol. 34, no. 6, pp. 2125–2138, Dec. 2021.

[31] A. Jamalipour, Annual IEEE Computer Conference, IEEE International Conference on Communications 2014.06.10-14 Sydney, and IEEE ICC 2014.06.10-14 Sydney, *IEEE International Conference on Communications (ICC), 2014 10-14 June 2014, Sydney, Australia*.

[32] N. Barroca, F. J. Velez, L. M. Borges, and P. Chatzimisios, "Performance enhancement of IEEE 802.15.4 by employing RTS/CTS and frame concatenation," *IET Wireless Sensor Systems*, vol. 10, no. 6, pp. 308–319, Dec. 2020.

[33] A. R. Urke, Ø. Kure, and K. Øvsthus, "A survey of 802.15.4 tsch schedulers for a standardized industrial internet of things," *Sensors*, vol. 22, no. 1. MDPI, Jan. 01, 2022.

[34] A. Jamalipour, Annual IEEE Computer Conference, IEEE International Conference on Communications 2014.06.10-14 Sydney, and IEEE ICC 2014.06.10-14 Sydney, *IEEE International Conference on Communications (ICC), 2014 10-14 June 2014, Sydney, Australia*.

[35] A. Khalifeh, R. Tanash, M. AlQudah, and S. Al-Agtash, "Enhancing energy efficiency of IEEE 802.15.4- based industrial wireless sensor networks," *J Ind Inf Integr*, vol. 33, Jun. 2023.

[36] P. Dani, P. Adi, and A. Kitagawa, "Quality of Service and Power Consumption Optimization on the IEEE 802.15.4 Pulse Sensor Node based on Internet of Things," 2019.

[37] L. Alkama and L. Bouallouche-Medjkoune, “IEEE 802.15.4 historical revolution versions: A survey,” *Computing*, vol. 103, no. 1, pp. 99–131, Jan. 2021.

[38] Tekhnicheski universitet--Sofiiā, Institute of Electrical and Electronics Engineers. Bulgaria Section, and Institute of Electrical and Electronics Engineers, *2020 XXIX International Scientific Conference Electronics (ET): proceedings: September 16-18, 2020, Sozopol, Bulgaria*.

[39] E. Ogungbemi, N. E. Akpan, O. E. Oluropo, and O.-O. C. Onwunali, “Evaluation of energy demand and lifespan of battery-powered ZigBee IEEE 802.15.4 compliant sensor node for Internet of Things-based applications,” 2022.

[40] A. Ali, R. R. Irshad, A. A. Alattaab, and A. Fatahayab, “Data Reliability and Sensors Lifetime in Bridge Health Monitoring using LoRaWAN-Zigbee,” *Computers, Materials and Continua*, vol. 73, no. 2, pp. 2663–2678, 2022.

[41] I. Bouazzi, M. Zaidi, M. Usman, M. Z. M. Shamim, V. K. Gunjan, and N. Singh, “Future Trends for Healthcare Monitoring System in Smart Cities Using LoRaWAN-Based WBAN,” *Mobile Information Systems*, vol. 2022, 2022.

[42] V. K. Quy *et al.*, “IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges,” *Applied Sciences (Switzerland)*, vol. 12, no. 7. MDPI, Apr. 01, 2022.

[43] A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, “Internet of Things (IoT): From awareness to continued use,” *Int J Inf Manage*, vol. 62, Feb. 2022.

[44] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[45] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[46] S. Raman, A. Chougule, and V. Chamola, “A low power consumption mobile based IoT framework for real-time classification and segmentation for apple disease,” *Microprocess Microsyst*, vol. 94, Oct. 2022.

[47] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, “Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions,” *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296–312, Feb. 2023.

[48] R. A. Radouan Ait Mouha, “Internet of Things (IoT),” *Journal of Data Analysis and Information Processing*, vol. 09, no. 02, pp. 77–101, 2021.

[49] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, “Survey on IoT: Security threats and applications,” *Journal of Robotics and Control (JRC)*, vol. 2, no. 1. Department of Agribusiness, Universitas Muhammadiyah Yogyakarta, pp. 42–46, Jan. 01, 2021.

[50] Institute of Electrical and Electronics Engineers, IEEE Industrial Electronics Society, and C. and T. E. Consiglio Nazionale Delle Ricerche (Italy). Institute of Electronics, *WFCS 2018: 2018 14th IEEE International Workshop on Factory Communication Systems: 13 - 15 June 2018, Imperia, Italy*.

[51] SCAD College of Engineering and Technology and Institute of Electrical and Electronics Engineers, *Proceedings of the International Conference on Trends in Electronics, and Informatics (ICOEI 2019): 23-25, April 2019*.

[52] "Mitton, Nathalie, et al. Interoperability, safety, and security in IoT. Second international conference, Internet of Things (IoT) 2016 and third international conference, SaSeIoT. 2016.".

[53] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[54] N. H. Motlagh, M. Mohammad Rezaei, J. Hunt, and B. Zakeri, "Internet of things (IoT) and the energy sector," *Energies*, vol. 13, no. 2. MDPI AG, 2020.

[55] J. Hu, G. Xu, L. Hu, S. Li, and Y. Xing, "An Adaptive Energy Efficient MAC Protocol for RF Energy Harvesting WBANs," *IEEE Transactions on Communications*, vol. 71, no. 1, pp. 473–484, Jan. 2023.

[56] A. S. Sadeq, R. Hassan, H. Sallehudin, A. H. M. Aman, and A. H. Ibrahim, "Conceptual Framework for Future WSN-MAC Protocol to Achieve Energy Consumption Enhancement," *Sensors*, vol. 22, no. 6. MDPI, Mar. 01, 2022.

[57] Z. U. Khan *et al.*, "A Comprehensive Survey of Energy-Efficient MAC and Routing Protocols for Underwater Wireless Sensor Networks," *Electronics (Switzerland)*, vol. 11, no. 19. MDPI, Oct. 01, 2022.

[58] A. N. Sakib, M. Drieberg, S. Sarang, A. A. Aziz, N. T. T. Hang, and G. M. Stojanović, "Energy-Aware QoS MAC Protocol Based on Prioritized-Data and Multi-Hop Routing for Wireless Sensor Networks," *Sensors*, vol. 22, no. 7, Apr. 2022.

[59] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, "A Survey on MAC Protocol Approaches for Underwater Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 21, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 3916–3932, Feb. 01, 2021.

[60] A. Nasipuri, J. Zhuang, and S. R. Das, "A Multichannel CSMA MAC Protocol for Multihop Wireless Networks."

[61] S. A. Tegos, P. D. Diamantoulakis, A. S. Lioumpas, P. G. Sarigiannidis, and G. K. Karagiannidis, "Slotted ALOHA with NOMA for the Next Generation IoT," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6289–6301, Oct. 2020.

[62] L. Li, Y. Dong, C. Pan, and P. Fan, “Timeliness of wireless sensor networks with random multiple access,” *Journal of Communications and Networks*, vol. 25, no. 3, pp. 405–418, May 2023.

[63] D. Klair, K. W. Chin, and R. Raad, “On the energy consumption of Pure and Slotted Aloha based RFID anti-collision protocols,” *Comput Commun*, vol. 32, no. 5, pp. 961–973, Mar. 2009.

[64] A. M. Hamzah and Y. J. K. Nukhailawi, “The Backoff in Intermediate Networks for a Real-Time System Embedded Ethernet,” in *Proceedings - CSCTIT 2022: 5th College of Science International Conference on Recent Trends in Information Technology*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 277–281.

[65] Y. Li, Z. Lv, Z. Fan, and H. Zhang, “Adaptive Two-step Binary Exponential Backoff Strategy for Random Access,” in *ITNEC 2023 - IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1104–1109.

[66] L. Barletta, F. Borgonovo, and I. Filippini, “The throughput and access delay of slotted-aloha with exponential backoff,” in *IEEE/ACM Transactions on Networking*, Institute of Electrical and Electronics Engineers Inc., Feb. 2018, pp. 451–464.

[67] M. Abid Ali Khan, H. Ma, S. Muhammad Aamir, A. Baris Cekderi, M. Ahamed, and A. Abdo Ali Alsumeri, “Performance of Slotted ALOHA for LoRa-ESL Based on Adaptive Backoff and Intra Slicing,” in *2022 6th International Conference on Communication and Information Systems, ICCIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 169–173.

[68] B. Jang, M. Kim, G. Harerimana, and J. W. Kim, “Q-Learning Algorithms: A Comprehensive Classification and Applications,” *IEEE Access*, vol. 7, pp. 133653–133667, 2019.

[69] S. Spanò *et al.*, “An efficient hardware implementation of reinforcement learning: The q-learning algorithm,” *IEEE Access*, vol. 7, pp. 186340–186351, 2019.

[70] J. He, H. Zhao, D. Zhou, and Q. Gu, “Nearly Minimax Optimal Reinforcement Learning for Linear Markov Decision Processes”.

[71] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, “Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 302–3108, Oct. 2019.

[72] Y. Chu Thesis, “Application of Reinforcement Learning on Medium Access Control for Wireless Sensor Networks,” 2013.

[73] S. Tyagi, P. Chand Jain, and P. C. Jain, “Optimization of Slotted-ALOHA using Q-Learning Water Level Monitoring and Management of Dams using IoT View project to no more about 5G and its impact on society View project SEE PROFILE Optimization of Slotted-ALOHA using Q-Learning”.

[74] https://github.com/afcuttin/slotted-aloha.

Apêndices

A. Implementação de códigos no MATLAB para do *Slotted* ALOHA nas RSSFs (Cenário 1)

A.1. Implementação da função *saloha.m*

```
function [throughput,meanDelay,trafficOffered,pcktCollisionProb] =
saloha(sourceNumber,packetReadyProb,maxBackoff,simulationTime,showProgressBar,niceOutp
ut)
% function [throughput,mean delay,traffic offered,packet collision probability]
%    = saloha(source number,packet ready probability, maximum backoff,simulation time,
%      show progress bar,nice output)
%
% +++ Function input parameters
%
% source number (positive integer): the number of sources that generate packets.
%
% packet ready probability (real, [0,1]): the probability that a given source has
%        a packet ready to be transmitted at any given time slot.
%
% maximum backoff (positive integer): the maximum backoff value that a backlogged
%        source must wait before a new transmission attempt.
%
% simulation time (positive integer): the duration of the simulation in time slots.
%
% show progress bar (optional): if true, a progress bar showing the simulation
%        advance will be displayed. Default behaviour is showProgressBar = false
%        for faster simulations.
%
% nice output (optional): if true, prints out the function outputs. Default
%        behaviour is niceOutput = false.
%
% +++ Function outputs
%
% throughput: normalized throughput of the slotted aloha random access protocol
%
% mean delay: the average delay (in slots) for a packet to be successfully
%        transmitted (acknowledge) from the moment it is ready at the source
%
% traffic offered: normalized traffic offered to the system,including
%        retransmissions
%
% packet collision probability: probability that a packet collides with others
%        at any given time slot

sourceStatus = zeros(1,sourceNumber);
% legit source statuses are always non-negative integers and equal to:
% 0: source has no packet ready to be transmitted (is idle)
% 1: source has a packet ready to be transmitted, either because new data must be sent
or a previously collided packet has waited the backoff time
% >1: source is backlogged due to previous packets collision, the value of the status
equals the number of slots it must wait for the next transmission attempt
sourceBackoff = zeros(1,sourceNumber);
pcktTransmissionAttempts = 0;
ackdPacketDelay = zeros(1,simulationTime);
ackdPacketCount = 0;
pcktCollisionCount = 0;
pcktGenerationTimestamp = zeros(1,sourceNumber);
currentSlot = 0;
```

Continuação (1) *saloha.m*

```
if exist('showProgressBar','var') && showProgressBar == 1
    showProgressBar = 1;
    progressBar = waitbar(0,'Generating
traffic...','CreateCancelBtn','setappdata(gcbf,''canceling'',1)');
    setappdata(progressBar,'canceling',0);
else
    showProgressBar = 0;
end

while currentSlot < simulationTime
    currentSlot = currentSlot + 1;

    if showProgressBar == 1
        if getappdata(progressBar,'canceling')
            delete(progressBar);
            fprintf('\nWarning: terminated by user!\n');
            break
        end
        waitbar(currentSlot /
simulationTime,progressBar,sprintf('Packets sent: %u; packets
acknowledged: %u.',pcktTransmissionAttempts,ackdPacketCount));
    end

    for eachSource1 = 1:length(sourceStatus)
        if sourceStatus(1,eachSource1) == 0 && rand(1) <=
packetReadyProb % new packet
            sourceStatus(1,eachSource1) = 1;
            sourceBackoff(1,eachSource1) = randi(maxBackoff,1);
            pcktGenerationTimestamp(1,eachSource1)=currentSlot;
        elseif sourceStatus(1,eachSource1)==1 % backlogged packet
            sourceBackoff(1,eachSource1)=randi(maxBackoff,1);
        end
    end

    pcktTransmissionAttempts = pcktTransmissionAttempts +
sum(sourceStatus == 1);

    if sum(sourceStatus == 1) == 1
        ackdPacketCount = ackdPacketCount + 1;
        [~,sourceId] = find(sourceStatus == 1);
        ackdPacketDelay(ackdPacketCount) = currentSlot -
pcktGenerationTimestamp(sourceId);
    elseif sum(sourceStatus == 1) > 1
        pcktCollisionCount = pcktCollisionCount + 1;
        sourceStatus  = sourceStatus + sourceBackoff;
    end

    sourceStatus = sourceStatus - 1; % decrease backoff interval
    sourceStatus(sourceStatus < 0) = 0; % idle sources stay idle (see
permitted statuses above)
    sourceBackoff = zeros(1,sourceNumber);
end

if currentSlot == simulationTime && showProgressBar == 1
    delete(progressBar);
end
```

Continuação (2) *saloha.m*

```
trafficOffered = pcktTransmissionAttempts / currentSlot;
if ackdPacketCount == 0
    meanDelay = simulationTime; % theoretically, if packets collide
continously, the delay tends to infinity
else
    meanDelay = mean(ackdPacketDelay(1:ackdPacketCount));
end
throughput = ackdPacketCount / currentSlot;
pcktCollisionProb = pcktCollisionCount / currentSlot;

if exist('niceOutput','var') && niceOutput == 1
    fprintf('\nTraffic offered (G): %.3f,\nThroughput (S):
%.3f,\nMean delay (D): %.2f slots,\nCollision probability (P_c):
%.3f.\n',trafficOffered,throughput,meanDelay,pcktCollisionProb);
end
```

A.2. Implementação do *script* principal (*run_program.m*)

```
clear all
close all
clc

% the following values return a throughput very close to the
theoretical maximum
% sources number = 100
% maximum backoff = 100
% packet ready probability = 0.0057
% simulation time = 5000
%dim= 2;


users=input('Introduz o numero de utizadores ou dispositivos: \n');
n_vezes = input('Introduz o nº de vezes que queres que o programa
corre neste nº de dispositivos: \n');
dados_sAloha = zeros(n_vezes,4+1);

i=0;
   for n=1: n_vezes
   i=i+1;
   [throughput,meanDelay,trafficOffered,pcktCollisionProb]=
saloha(users,0.0057,100,5000,true,true);
   dados_sAloha(i,1:5)=
[users,throughput,meanDelay,trafficOffered,pcktCollisionProb];

   end

save('Dados_Slotted_Aloha_200_users_and_10x.mat','dados_sAloha');
```

B. Implementação de códigos no MATLAB para obtenção dos resultados pretendidos (Cenário 2)

B.1. Implementação do código para o CSMA (Pacotes Entregues Acumulados):

```
clear all
close all
clc
% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 130.5 bytes convertidos em 1044 bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
resultados = zeros(1, num_slots);
prob_escuta = 0.05; % Probabilidade de um nodo escutar o canal em um
slot dado

% CSMA
canal_ocupado = false;
for slot = 1:num_slots
if ~canal_ocupado
nodos_escuta = rand(1, num_nodos) < prob_escuta;
num_escuta = sum(nodos_escuta);
if num_escuta == 1
resultados(1, slot) = 1;
canal_ocupado = true;
elseif num_escuta > 1
canal_ocupado = false;
end
else
canal_ocupado = false; % Supondo que uma transmissão ocupa apenas um
slot
end
end

% Gráficos
cum_resultados = cumsum(resultados);

figure;
plot(cum_resultados, 'LineWidth', 1.5);
xlabel('Slots');
ylabel('Pacotes entregues acumulados');
title('Desempenho do CSMA no IEEE 802.15.4');
grid on;
```

B.2. Implementação do código para o *Slotted* ALOHA (Pacotes Entregues Acumulados):

```
clear all
close all
clc

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 130.5 bytes convertidos em 1044 bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
resultados = zeros(1, num_slots);
prob_transmissao = 0.05; % Probabilidade de um nodo transmitir em um
slot dado

% Slotted ALOHA
for slot = 1:num_slots
    transmissions = rand(1, num_nodos) < prob_transmissao;
    if sum(transmissions) == 1
        resultados(1, slot) = 1;
    end
end

% Gráficos
cum_resultados = cumsum(resultados);

figure;
plot(cum_resultados, 'LineWidth', 1.5);
xlabel('Slots');
ylabel('Pacotes entregues acumulados');
title('Desempenho do Slotted ALOHA no IEEE 802.15.4');
grid on;
```

B.3. Implementação do código para o *Slotted* ALOHA-BEB (Pacotes Entregues Acumulados):

```
clear all
close all
clc

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 130.5 bytes convertidos em 1044 bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
resultados = zeros(1, num_slots);
prob_transmissao = 0.05; % Probabilidade inicial de um nodo
transmitir em um slot dado
m = 5; % Valor máximo para k no BEB
retransmissoes = zeros(1, num_nodos); % Armazena o número de
retransmissões para cada nodo
backoff = zeros(1, num_nodos); % Valor de backoff para cada nodo

% Slotted ALOHA-BEB
for slot = 1:num_slots
    ready_to_transmit = (rand(1, num_nodos) < prob_transmissao) &
(backoff == 0);
    transmissions = sum(ready_to_transmit);

    if transmissions == 1
        resultados(1, slot) = 1;
        retransmissoes(ready_to_transmit) = 0; % Reseta o contador de
retransmissões para o nodo bem-sucedido
    elseif transmissions > 1
        colliding_nodes = find(ready_to_transmit);
        for nodo = colliding_nodes
            retransmissoes(nodo) = retransmissoes(nodo) + 1;
            k = min(retransmissoes(nodo), m);
            backoff(nodo) = randi( [0, 2^k - 1]);
        end
    end

    % Decrementa os contadores de backoff para todos os nodos
    backoff = backoff - 1;
    backoff(backoff < 0) = 0;
end

% Gráficos
cum_resultados = cumsum(resultados);

figure;
plot(cum_resultados, 'LineWidth', 1.5);
xlabel('Slots');
ylabel('Pacotes entregues acumulados');
title('Desempenho do Slotted ALOHA-BEB no IEEE 802.15.4');
grid on;
```

B.4. Implementação do código para o Q-ALOHA (Pacotes Entregue Acumulados):

```
clear all
close all
clc

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 130.5 bytes convertidos em 1044 bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
resultados = zeros(1, num_slots);
alpha = 0.1; % Taxa de aprendizagem
gamma = 0.9; % Fator de desconto
epsilon = 0.1; % Política ε-greedy
n_estados = 10;
n_acoes = 10;
q_table = zeros(n_estados, n_acoes); % Tabela Q
estado_atual = 1;
acoes = linspace(0.01, 0.1, n_acoes); % Diferentes probabilidades de
transmissão

% Q-ALOHA
for slot = 1:num_slots
    % Política ε-greedy para escolher a ação
    if rand() < epsilon
        acao = randi( [1, n_acoes]);
    else
        [~, acao] = max(q_table(estado_atual, :));
    end
    prob_transmissao = acoes(acao);

    transmissions = rand(1, num_nodos) < prob_transmissao;
    n_transmissions = sum(transmissions);

    % Recompensa e atualização do estado
    if n_transmissions == 1
        recompensa = 1;
        resultados(1, slot) = 1;
        estado_atual = 1;
    else
        recompensa = -n_transmissions;
        estado_atual = min(n_estados, estado_atual + 1);
    end

    % Atualização da tabela Q usando o Q-learning
    max_q_next = max(q_table(estado_atual, :));
    q_table(estado_atual, acao) = (1 - alpha) * q_table(estado_atual, acao)
+ alpha * (recompensa + gamma * max_q_next);
end
% Gráficos
cum_resultados = cumsum(resultados);

figure;
plot(cum_resultados, 'LineWidth', 1.5);
xlabel('Slots');
ylabel('Pacotes entregues acumulados');
title('Desempenho do Q-ALOHA no IEEE 802.15.4');
grid on;
```

C. Implementação de códigos no MATLAB para obtenção dos resultados pretendidos (Cenário 3)

C.1. Implementação do código para o CSMA (Latência):

```
clear;
clc;

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 127 bytes convertidos em bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
prob_escuta = 0.05;

latencias = []; % Para armazenar latências de pacotes entregues
fila_nodos = zeros(1, num_nodos);

canal_ocupado = false;

% CSMA
for slot = 1:num_slots
    if ~canal_ocupado
        nodos_escuta = rand(1, num_nodos) < prob_escuta;
        num_escuta = sum(nodos_escuta);

        if num_escuta == 1
            nodo_transmitido = find(nodos_escuta);
            latencias = [latencias, fila_nodos(nodo_transmitido)];
            fila_nodos(nodo_transmitido) = 0; % Reset do contador para esse nodo
            canal_ocupado = true;
        elseif num_escuta > 1
            nodos_colisao = find(nodos_escuta);
            fila_nodos(nodos_colisao) = fila_nodos(nodos_colisao) + 1;
        end
    else
        canal_ocupado = false;
    end

    fila_nodos = fila_nodos + 1; % Incremento do contador para todos os nodos
end

% Cálculo da latência média
latencia_media = mean(latencias);

% Gráficos
figure;
hist(latencias, 50);
xlabel('Latência (slots)');
ylabel('Número de pacotes');
title( ['Desempenho de Latência do CSMA no IEEE 802.15.4 - Latência Média: ',
num2str(latencia_media, '%.2f'), ' slots']);
grid on;
```

C.2. Implementação do código para o *Slotted* ALOHA (Latência):

```
clear;
clc;

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 127 bytes convertidos em bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
prob_transmissao = 0.05; % Probabilidade de transmissão em um slot

resultados = zeros(1, num_slots);
latencias = []; % Para armazenar latências de pacotes entregues

fila_nodos = zeros(1, num_nodos); % Cada entrada representa o tempo desde que o pacote foi gerado

% Slotted ALOHA
for slot = 1:num_slots
    transmissoes = rand(1, num_nodos) < prob_transmissao;
    n_transmissoes = sum(transmissoes);

    if n_transmissoes == 1
        nodo_transmitido = find(transmissoes);
        latencias = [latencias, fila_nodos(nodo_transmitido)];
        fila_nodos(nodo_transmitido) = 0; % Reset do contador para esse nodo
    elseif n_transmissoes > 1
        nodos_colisao = find(transmissoes);
        fila_nodos(nodos_colisao) = fila_nodos(nodos_colisao) + 1;
    end

    fila_nodos = fila_nodos + 1; % Incremento do contador para todos os nodos
end

% Cálculo da latência média
latencia_media = mean(latencias);

% Gráficos
figure;
hist(latencias, 50);
xlabel('Latência (slots)');
ylabel('Número de pacotes');
title( ['Desempenho de Latência do Slotted ALOHA no IEEE 802.15.4 - Latência Média: ',
num2str(latencia_media, '%.2f'), ' slots']);
grid on;
```

C.3. Implementação do código para o *Slotted* ALOHA-BEB (Latência):

```
clear;
clc;

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 127 bytes convertidos em bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
prob_transmissao = 0.05;

latencias = []; % Para armazenar latências de pacotes entregues
fila_nodos = zeros(1, num_nodos);
tentativas_nodos = zeros(1, num_nodos); % Para armazenar o número de
tentativas de cada nodo

% Slotted ALOHA com BEB
for slot = 1:num_slots
    nodos_transmissao = (rand(1, num_nodos) < prob_transmissao) &
(tentativas_nodos == 0);
    num_transmissoes = sum(nodos_transmissao);

    if num_transmissoes == 1
        nodo_transmitido = find(nodos_transmissao);
        latencias = [latencias, fila_nodos(nodo_transmitido)];
        fila_nodos(nodo_transmitido) = 0;
        tentativas_nodos(nodo_transmitido) = 0;
    elseif num_transmissoes > 1
        nodos_colisao = find(nodos_transmissao);
        for nodo = nodos_colisao
            if tentativas_nodos(nodo) < 10 % Para evitar crescimento
indefinido
                tentativas_nodos(nodo) = 2^tentativas_nodos(nodo) * rand();
% BEB
            else
                tentativas_nodos(nodo) = 10; % Limite máximo de tentativas
            end
        end
    end

    tentativas_nodos = max(0, tentativas_nodos - 1);
    fila_nodos = fila_nodos + 1;
end

% Cálculo da latência média
latencia_media = mean(latencias);

% Gráficos
figure;
hist(latencias, 50);
xlabel('Latência (slots)');
ylabel('Número de pacotes');
title( ['Desempenho de Latência do Slotted ALOHA-BEB no IEEE 802.15.4 -
Latência Média: ', num2str(latencia_media, '%.2f'), ' slots']);
grid on;
```

C.4. Implementação do código para o Q-ALOHA (Latência):

```
clear;
clc;

% Parâmetros específicos do IEEE 802.15.4
taxa_transmissao = 250e3; % 250 kbps
tamanho_pacote = 130.5 * 8; % 127 bytes convertidos em bits

% Parâmetros e Inicialização
num_nodos = 100;
num_slots = 1000;
gamma = 0.9; % Fator de desconto
alpha = 0.1; % Taxa de aprendizado
epsilon = 0.1; % Estratégia ε-greedy

Q = zeros(num_nodos, 2); % Tabela Q inicializada com zeros
latencias = [];
fila_nodos = zeros(1, num_nodos);

% Q-ALOHA
for slot = 1:num_slots
    if rand() < epsilon
        acao = randi( [1, 2], num_nodos, 1) - 1; % Exploração
    else
        [~, acao] = max(Q, [], 2); % Ação ótima
        acao = acao - 1;
    end

    transmissoes = (rand(1, num_nodos) < 0.05) & acao'; % Apenas nodos que decidem
transmitir
    num_transmissoes = sum(transmissoes);

    recompensa = zeros(1, num_nodos);

    if num_transmissoes == 1
        nodo_transmitido = find(transmissoes);
        latencias = [latencias, fila_nodos(nodo_transmitido)];
        fila_nodos(nodo_transmitido) = 0;
        recompensa(nodo_transmitido) = 1;
    elseif num_transmissoes > 1
        recompensa(transmissoes) = -1;
    end

    for nodo = 1:num_nodos
        if acao(nodo)
            Q(nodo, 2) = Q(nodo, 2) + alpha * (recompensa(nodo) + gamma * max(Q(nodo,
:)) - Q(nodo, 2));
        else
            Q(nodo, 1) = Q(nodo, 1) + alpha * (recompensa(nodo) + gamma * max(Q(nodo,
:)) - Q(nodo, 1));
        end
    end

    fila_nodos = fila_nodos + 1;
end

% Cálculo da latência média
latencia_media = mean(latencias);

% Gráficos
figure;
hist(latencias, 50);
xlabel('Latência (slots)');
ylabel('Número de pacotes');
title( ['Desempenho de Latência do Q-ALOHA no IEEE 802.15.4 - Latência Média: ',
num2str(latencia_media, '%.2f'), ' slots']);
grid on;
```

D. Ambiente de Simulação

D.1. MATLAB

MATLAB é uma plataforma de software de alto desempenho desenvolvida pela *MathWorks*, que é utilizada principalmente para computação numérica, visualização e programação. A palavra "MATLAB" significa "laboratório de matrizes", e como o nome sugere, é especialmente conhecido por sua capacidade de manipular matrizes e realizar cálculos complexos com facilidade. Algumas características e funcionalidades do MATLAB incluem:

- Linguagem de programação de alto nível: MATLAB fornece uma linguagem de programação que é simples de aprender e usar, especialmente para aqueles com uma formação em engenharia ou ciências. Ela é otimizada para operações de matrizes e análise de dados.

- Toolboxes especializadas: MATLAB vem com uma série de *toolboxes* especializadas para domínios específicos, como processamento de sinais, comunicações, finanças, aprendizado de máquina e muitos outros. Estas *toolboxes* fornecem funções adicionais e algoritmos que são relevantes para esses campos específicos.

- SIMULINK: É uma extensão do MATLAB que permite a modelagem, simulação e análise de sistemas dinâmicos usando diagramas de blocos. É amplamente utilizado para simulação em domínios como controle de sistemas, aeroespacial e eletrônica.

- Visualização: MATLAB oferece uma vasta gama de ferramentas para visualização de dados, desde simples *plots* e gráficos até visualizações 3D complexas.

- Integração com outras linguagens: É possível chamar funções de bibliotecas escritas em C, C++, Java e FORTRAN diretamente do MATLAB.

- Interface amigável: Além da linha de comando, o MATLAB oferece uma interface gráfica do usuário (GUI) rica, que inclui um editor de código, um browser para navegar pelo *workspace*, ferramentas para visualizar variáveis e muitos outros recursos.

- Extensibilidade: Os usuários podem escrever seus próprios scripts, funções e criar suas próprias *toolboxes*, tornando-o adaptável a uma variedade de aplicações.

Nessa dissertação, o MATLAB foi utilizado como nossa plataforma de simulação. Ele forneceu as ferramentas e recursos necessários para modelar, analisar e simular nossos sistemas e algoritmos com precisão e eficiência. A capacidade do MATLAB de lidar com grandes conjuntos de dados, realizar cálculos complexos e visualizar os resultados fez dele uma escolha ideal para nossas necessidades de simulação