isec Engenharia

MESTRADO EM ENGENHARIA ELETROTÉCNICA

DEFINITIVO

Ad Hoc Wireless Network for Long Range Applications

Autor

João Rafael Craveiro Ferreira

Orientadores

Professor Adjunto, Doutor José Pedro de Matos Nogueira Amaro

Professora Coordenadora, Doutora Cristina Isabel Ferreira Figueiras Faustino Agreira

Coimbra, Abril 2024

INSTITUTO POLITÉCNICO DE COIMBRA

INSTITUTO SUPERIOR DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELETROTÉCNICA

Ad Hoc Wireless Network for Long Range Applications

Trabalho de Projeto para a obtenção do grau de Mestre em Engenharia Eletrotécnica

Especialização em Automação e Comunicações em Sistemas Industriais

Autor

João Rafael Craveiro Ferreira

Orientadores

Professor Adjunto, Doutor José Pedro de Matos Nogueira Amaro

Professora Coordenadora, Doutora Cristina Isabel Ferreira Figueiras Faustino Agreira

INSTITUTO POLITÉCNICO DE COIMBRA

INSTITUTO SUPERIOR DE ENGENHARIA

Coimbra, Abril 2024

ACKNOWLEDGMENTS

The project presented here, in addition to my full dedication, would not have been possible without the help, support, and collaboration of certain people and/or entities to whom I express my sincere thanks.

First, I want to express my gratitude to the Instituto Superior de Engenharia de Coimbra and its Departamento de Engenharia Eletrotécnica. The resources and facilities provided by these entities were essential for the completion of this project.

I also thank Professor José Pedro M. N. Amaro, my supervisor for this project. His guidance was essential for the completion of this work. His vast knowledge, advice, and recommendations played a crucial role. His availability, even when difficult, dedication, and trust in me throughout this journey, marked also by our joint work on the Luxifer project, are invaluable.

I also want to extend my thanks to Professor Cristina Isabel F. F. F. Agreira, whose support, help, and constant motivation played a significant role in the completion of this project and in my academic career. It is fair to highlight her availability, knowledge, and inspiration, which proved to be significant in the context of the Luxifer project.

I thank the Fablab Penela, in the name of Engineer Belmiro Luís, for the implementation of the LoRaWAN network in the municipality of Penela. This initiative played a fundamental role in the realization of the objectives of this project.

Thank you to my parents, brother, and sister-in-law, for your love and for the importance and help you have always given me in my education and in my achievements.

Lastly, I want to give a special thanks to my colleague and friend João Cardoso, with whom I shared the challenges and achievements of the past few years. From academic work to the current project, Luxifer, we have walked a long and challenging path, but one that has strengthened a friendship that is equally invaluable.

ABSTRACT

The Long Range (LoRa) technology has been gaining popularity, becoming one of the most promising and frequently used technologies among Low Power Wide Area Networks (LPWANs). Highly compatible with Internet of Things (IoT) applications, LoRa enables long-range communications, albeit with low transmission rates and duty cycle constraints. Despite all this enthusiasm, challenges persist in LoRa networks, especially in terms of coverage, with the occurrence of problematic areas where communications are inconsistent, often referred to as shadow zones. The reasons are diverse, ranging from the urban propagation environment, physical obstruction to the network base station, or locations with significant electromagnetic attenuation, among others. In this context, this project focused on designing an Ad Hoc protocol integrated with the LoRaWAN network to perfect communication in unstable scenarios. This protocol was designed for non-mobile devices that rely exclusively on LoRa technology for communication. The Ad Hoc LoRa approach aims to address small areas with unstable connectivity by transforming unstable nodes into Slave devices that connect to relay nodes called Masters, resulting in the formation of two-hop communication trees. The test results reveal the effectiveness of the Ad Hoc LoRa protocol in optimizing network coverage and improving the success rates of transmitted messages. Furthermore, the results suggest that the protocol may offer superior energy efficiency compared to direct transmissions to LoRaWAN base stations.

Keywords: LoRaWAN, Shadow Zones, Ad Hoc, Multihop, Two-Hop Tree

RESUMO

A tecnologia Long Range (LoRa) tem vindo a ganhar bastante popularidade, tornando-se numa das tecnologias mais promissoras e frequentemente utilizadas entre as *Low Power Wide Area Network*s (LPWAN). Altamente compatível com aplicações da *Internet of Things* (IoT), LoRa permite comunicações de longo alcance, ainda que com baixas taxas de transmissão e restrições de duty cycle. Apesar de todo esse fulgor, subsistem desafios nas redes LoRa, especialmente em termos de cobertura, com a ocorrência de áreas problemáticas onde as comunicações são inconsistentes, muitas vezes referidas como zonas sombra. Os motivos são diversos, que vão desde o ambiente de propagação urbano, obstrução física à estação base da rede ou locais com uma grande atenuação eletromagnética, entre outros. Nesse âmbito, este projecto concentrou-se no desenho de um protocolo Ad Hoc integrado com a rede LoRaWAN com o objetivo de otimizar a comunicação em cenários de instabilidade. Este protocolo foi projetado essencialmente para dispositivos não móveis que se baseiam exclusivamente na tecnologia LoRa para comunicação. A abordagem do Ad Hoc LoRa consiste em resolver pequenas áreas com conectividade instável, transformando nós instáveis em dispositivos Escravos que se ligam a nós retransmissores denominados de Mestres, resultando na formação de árvores de comunicação de dois saltos. Os resultados dos testes realizados revelam a eficácia do protocolo Ad Hoc LoRa na otimização da cobertura da rede e na melhoria das taxas de sucesso das mensagens transmitidas. Além disso, os resultados sugerem que o protocolo pode oferecer uma eficiência energética superior em comparação com as transmissões diretas às estações base LoRaWAN.

Palavras-Chave: LoRaWAN, Zonas Sombra, Ad Hoc, *Multihop*, Árvore de Dois Saltos

CONTENTS

LIST OF FIGURES

LIST OF TABLES

SYMBOLS AND ABBREVIATIONS

ABP	Activation By Personalization
ACK	Acknowledge
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
Ah	Ampere-hour
ALOHA	Advocates of Linux Open-source Hawaii Association
AppEUI	Application identifier
AppSKey	Application Session Key
bps	bit per second
BSL	Bootloader
BW	Bandwidth
CAD	Carrier Activity Detection
CCS	Code Composer Studio
CF	Carrier Frequency
CR	Coding Rate
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSS	Chirp Spread Spectrum
CT	Concurrent Transmission
dB	decibel
dBm	decibel mili-watt
DevAddr	Device Address
DL	Downlink
DOP	Data Operation Period

DR	Data Rate
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FHDR	Frame Header
FPort	Frame Port
FRMPayload	Frame Payload
FSK	Frequency Shift Keying
GW	Gateway
Hz	Hertz
IDE	Integrated Drive Electronics
IoT	Internet of Things
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical
LCR	Link Check Request
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low-power wide-area network
m	meter
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MHDR	MAC Header
MIC	Message Integrity Check
NCP	Network Construct Period

NwkSKey	Network Session Key
OTAA	Over-The-Air Activation
P2P	Point-to-Point
PCB	Printed Circuit Board
PDR	Packet Delivery Ratio
PPR	Percentage of Packets Received
RSSI	Received signal strength indication
SF	Spreading Factor
SFK	Software Development Kit
SNR	Signal-to-Noise Ratio
SW	Software
TDMA	Time-Division Multiplex Access
ToA	Time on Air
TTN	The Things Network
UART	Universal Asynchronous Receiver/Transmitter
UL	Uplink
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

1. INTRODUCTION

1.1. CONTEXT

In the coming years, device connectivity promises to transform the way we interact with the world, where people and industries will become both data consumers and generators. This is the IoT paradigm, which will allow heterogeneous devices to communicate and cooperate to provide intelligent services in different environments in a transparent way for the user. The expected billions of IoT devices around the world will lead to the development of intelligent systems for different applications [1]. These applications can fit into the concept of smart cities, where real-time data collection and connectivity of devices spread across the city are essential. Smart public lighting is an example of how IoT and Smart Cities can be combined to bring significant benefits. Namely, energy efficiency, improved safety, and optimization of luminaire maintenance cycles, contributing to a positive socio-economic impact on a city.

IoT applications and wireless communication technologies are two faces of the same coin. The developers design trade-offs are based on the need for high coverage combined with low bandwidth, low power requirements, small form factor and low operating costs [2]. These are the elements that identify LPWAN, which promise to become the engine of IoT applications (Figure 1.1). The objective of these networks is to provide small amounts of data over long distances, at rates of up to tens of kilobits per second (kbps), supporting thousands of devices connected to gateways (GW), thus enabling facilitating online data integration.

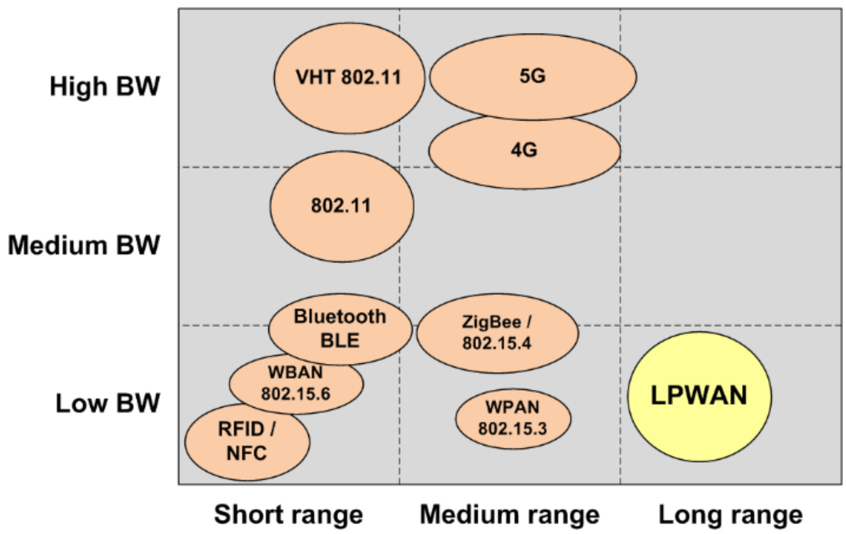


Figure 1.1 – LPWAN technologies according to range capability and bandwidth required. [3].

The IEEE 802.15.4 standard provides specifications for the physical and medium access control layers in wireless access technology for battery operated devices and is used by in sensor networks for IoT applications. However, the range on point-to-point connections is limited to hundreds of meters. For this reason, smart city solutions have boosted research into wireless technologies that allow long-range communication with energy consumption like IEEE 802.15.4 transceivers [4]. On the other hand, the objective of achieving wider coverage requires that the data transmission rate be reduced for this type of chips. LoRa is one such promising long-range, low-power technology, operating in the 868-915 MHz Industrial, Scientific, and Medical (ISM) band, enabling bitrates between 0.37 kbps and 46.9 kbps and promising ranges up to 20-25 km [5]. The medium access control protocol is called LoRaWAN. It follows a star topology, which simplifies the network and makes it robust. However, even with a large transmission range, it remains very difficult to obtain extended coverage within the range of a LoRaWAN base station, for example, due to the existence of shadow areas. Unless there is a higher density GW installation in suitable locations, the solution may involve the development of Ad Hoc networks. In this case, even if implemented with simple protocols, Ad Hoc operation may guarantee the reliability of communications [6] in LoRaWAN communications. This is on current challenge in developing solutions with the LoRa network since mesh communications are not yet supported by current LoRa technology.

1.2. OBJECTIVES

The main objective of this project is to design, implement, test and evaluate the performance of an Ad Hoc LoRa protocol. Thes proposed protocol is designed to operate in conjunction with LoRaWAN networks, with the aim of improving communication coverage and stability for non-mobile LoRa devices that face connectivity difficulties within the LoRaWAN network. With this purpose in mind, the specific objectives of this work include:

- Understand the underlying causes for unstable or non-existent connection zones in the LoRaWAN network.
- Determine appropriate indicators capable of alerting devices to their presence in areas of unstable LoRaWAN communication.
- Design an Ad Hoc protocol capable of ensuring broader and more stable coverage, while maintaining compatibility with LoRaWAN specifications for data transmission in both directions, that is, both in the uplink (UL) and downlink (DL).
- Develop a prototype with the ability to interpret all the protocol's methods and functionalities.
- Evaluate the Ad Hoc LoRa protocol and compare it with the standard operation of the LoRaWAN architecture, to demonstrate the ability to deal with the challenges of unstable connectivity in the architecture.

1.3. DOCUMENT ORGANIZATION

This document is organized as follows:

Chapter 2 presents a comprehensive theoretical context on Ad Hoc wireless networks, LoRa technology, and other concepts relevant to the understanding of the work developed. In addition, an analysis of the most recent literature on LoRa is conducted in various areas, such as the performance of the LoRa physical layer and the LoRaWAN network. Protocol implementations are also discussed, with a focus on optimizing the performance of the LoRaWAN network, as well as the development of multi-hop Ad Hoc protocols and how they impact coverage, reliability, and energy efficiency of communications.

Chapter 3 describes the protocol and communication mechanisms developed, which make it an Ad Hoc model working on the LoRaWAN network.

Chapter 4 shows the implementation of the protocol in specific scenarios in the Penela – Portugal region, and the hardware resources used. In this chapter, the performance evaluation of the protocol is also carried out, namely, on the reliability of communications in comparison with the typical LoRaWAN network.

Chapter 5 presents the conclusions of this project, along with suggestions for future work, which aim at the continuous validation and improvement of the developed protocol.

2. STATE OF ART

This chapter provides an overview of some concepts for understanding the developed protocol, as well as some relevant published works. Chapter 2.1 addresses the fundamentals of a wireless Ad Hoc network and its possible organizations. In addition, the challenges related to medium access and routing faced by devices in an Ad Hoc network will be explored. Chapter 2.2 presents work related to LoRa performance studies and Medium Access Control (MAC) protocols, as well as the development of multi-hop Ad Hoc protocols. Finally, chapter 2.3 summarizes the contributions of the chapter.

2.1. AD HOC WIRELESS NETWORKS

An Ad Hoc network is a decentralized network, where devices communicate directly with each other without relying on any pre-existing infrastructure. In this type of networks, the participation of each node is carried out through retransmissions, so that a given message reaches its destination (Figure 2.1). The organization of a wireless Ad Hoc network may be highly dynamic, due to the freedom of joining or leaving nodes. The need to adapt to new scenarios and the presence of mobility patterns are, therefore, factors for network organization to be dynamic, unstructured and heterogeneous. All these characteristics make Ad Hoc networks more complex to develop but give them high flexibility. This versatility has led to the emergence of diverse types of networks, which will be discussed further below.

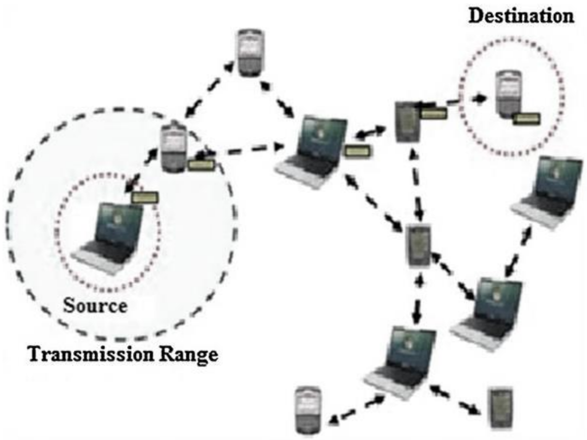


Figure 2.1 – Wireless Ad Hoc network [7].

2.1.1. Types of Wireless Ad Hoc Networks

The distinct types of wireless Ad Hoc networks are characterized by their operation and protocol. Ad hoc networks are used in specialized solutions, depending on their use. It is also possible to build hybrid networks, eliminating the possibility of each solution having exclusively one type of network.

2.1.1.1. Wireless Mesh Network (WMN)

A WMN consists of multiple mesh routers, which can forward messages between each other via wireless communication. These network elements can be equipped with more than one radio interface, improving their performance. Mesh routers that are connected to the internet are referred to in this context as gateways. As a rule, these routers have minimal mobility and, therefore, are usually installed on roofs or on public lighting posts [8]. Figure 2.2 shows the WMN architecture in a generic way, where the dashed lines represent wireless communications.

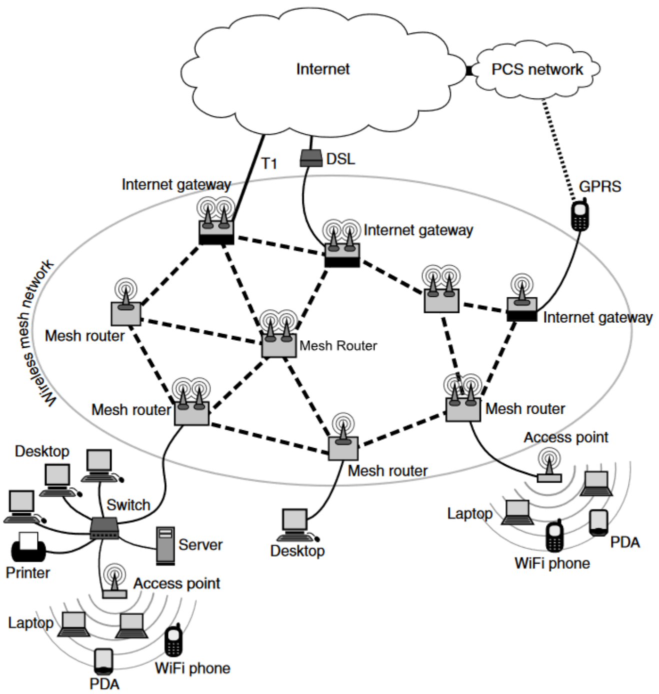


Figure 2.2 – Architecture of a wireless mesh network [8].

Figure 2.2 illustrates mesh routers serving devices (mesh clients), such as computers, telephones, WiFi access points, etc. In addition to serving these types of stations, WMNs can work with local networks such as Ethernet, Bluetooth, or sensor networks. In this way, the interoperability characteristic of mesh routers is verified. WMN may therefore be used in various scenarios. One of them is to take advantage of a number of cities physical elements, such as Internet Protocol (IP) address, in order to provide network access in a specific city area more effectively and at reduced cost.

2.1.1.2. Wireless Sensor Network (WSN)

WSN [8]–[10] are networks made up of sensor nodes randomly placed or dispersed in a certain geographic area, communicating via a wireless connection to collect, process and transmit data. These data, which can be temperature, air quality and humidity, among others, are aggregated in a special node, called a sink node, as shown in Figure 2.3. On the other hand, the network must be able to receive messages from the sink direction to the end device.

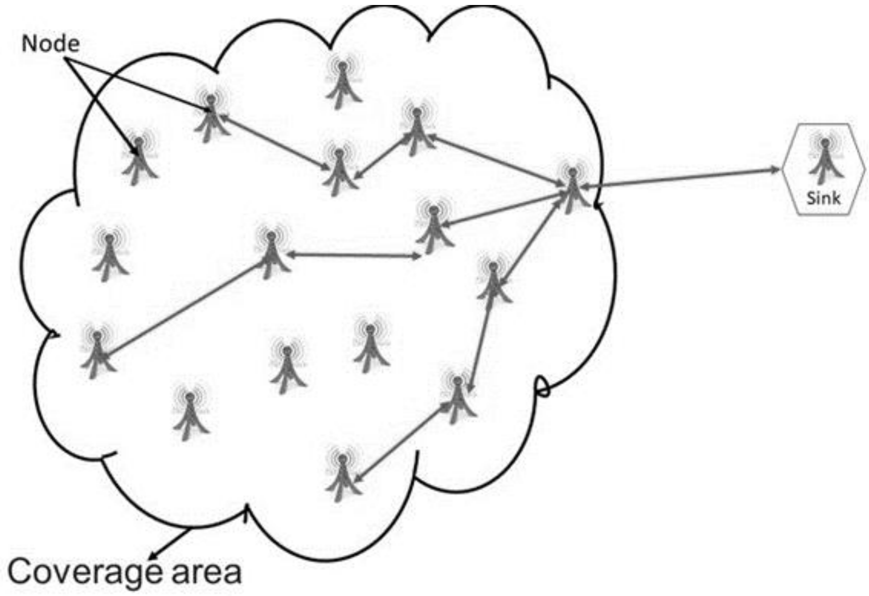


Figure 2.3 – Architecture of a wireless sensor network [9].

A WSN are characterized by their operation mode with non-mobile nodes. The main goal is to ensure communication connectivity, namely the ability to form data routing to the sink node. In this context, it is important that there is at least one path that connects any two sensors in service to the sink node. Therefore, the network must have the capacity to self-organize. On the other hand, the network must be scalable, fault tolerant and capable of efficient routing from an energy point of view since many of these devices are battery powered [10].

2.1.1.3. Mobile Ad Hoc Networks (MANET)

Mobile Ad Hoc Networks (MANET) [8], [11] are dynamically formed networks and consist of autonomous nodes that may be mobile. These devices are unpredictable, as they have the freedom to move within a network. This characteristic causes constant changes in the network organization. The difference in relation to WSNs is that the architecture change is due to movement between nodes, while in WSNs it is usually due to nodes going offline (lack of battery, hardware failure, etc.) [8].

2.1.2. Medium Access Control

In a wireless communications system, it is through the medium that information is transmitted by waves that make up its electromagnetic spectrum. Therefore, the performance of a wireless Ad Hoc network and its medium access control, or Medium Access Control (MAC), are inseparable in the design of an Ad Hoc network. Therefore, the importance of MAC protocols (chapter 2.1.2.2.) is essential. Namely, in the creation of the network structure, giving the capacity for self-organization. Also, in reliable sharing (reduction of collisions and interference), fair and efficient

[9], [11]. Due to this nature of diffusion, wireless communications face many challenges, which need to be overcome to achieve successful network operation.

2.1.2.1. Medium Access Control Challenges

Fading

Within the context of wireless communications, fading corresponds to the variation of signal energy with time, distance, frequency, among other variables. The lower the energy, the more difficult it is to distinguish between signals and noise [12], [13]. The intensity of this energy is called Received Signal Strength Indicator (RSSI) and the ratio of signal intensity over noise is called signal-to-noise ratio (SNR). There are several types of fading: Distance from the transmitter; Attenuation and obstruction of wave propagation by obstacles (Shadow Fading); Relative movement from transmitter to receiver during transmission (Doppler Fading); Wave frequency and; Natural phenomena [12]. Therefore, a wireless channel is considered time-varying and error-prone. Due to this instability, there is a possibility that a receiver will not be able to capture any information if the received signal power fades below a certain level [14].

Interference

The overlapping of waves is the cause of signals becoming corrupted, making them impossible to read. This phenomenon is called interference. Very common is interference from objects that emit waves, such as an industrial installation, or objects that are a source of wave reflection, dispersion and refraction mechanisms [12]. In the latter case, the medium is susceptible to errors due to the result of propagation in multiple paths. A good parameter for perceiving this type of phenomena is the SNR. A particular case of interference, which occurs when several elements of a network transmit simultaneously, are collisions [12]–[14].

Shadow Zones

In a wireless network, it is very common for there to be areas within the range of the transmitter with packet losses [15]. That is, there is a probability that a receiver located within these areas will not receive data messages. According to [15]., the origins of shadow zones are the main factor in signal attenuation, even if there are no obstacles or propagation in multiple paths. The presence of obstacles makes the gray area larger. In these shadow areas the SNR value drops abruptly, which causes a drop in the percentage of messages received, even if the RSSI value is above the sensitivity value.

Hidden and Exposed Nodes

In wireless Ad Hoc networks that use multi-hop communication structures, in which the sender device uses relay nodes to send messages to the recipient [16], a few challenges may be identified, namely when designing medium access control mechanism.

- Hidden nodes

In Figure 2.4 it is possible to portray the problem of the hidden node. This situation occurs when, for example, two nodes (stations A and C), which are not within range of each other, are within range of another receiver (station B). And when these two network elements transmit simultaneously, they cause a collision. This fact impacts receiver B reception ability, thus preventing data reception. This hidden terminal problem may impact the operation of multi-hop networks.

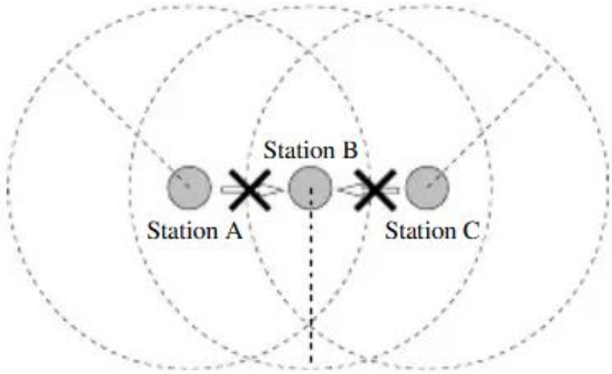


Figure 2.4 – Hidden terminal problem [16].

- Exposed nodes

Generally, medium access protocols use algorithms to reduce collisions between signals. This objective results in contention of network elements, which leads to postponed or cancelled transmissions. These mechanisms may lead to the occurrence of the exposed node situation. Figure 2.5 illustrates this problem. When node B is transmitting to A, the transmission is heard by C. Thus, C will unnecessarily delay sending the message to D to avoid interference/collisions with the transmission made by B. However, node C is beyond the range of A. Therefore, the transmission attempt by node C would not affect the reception of the message to device A.

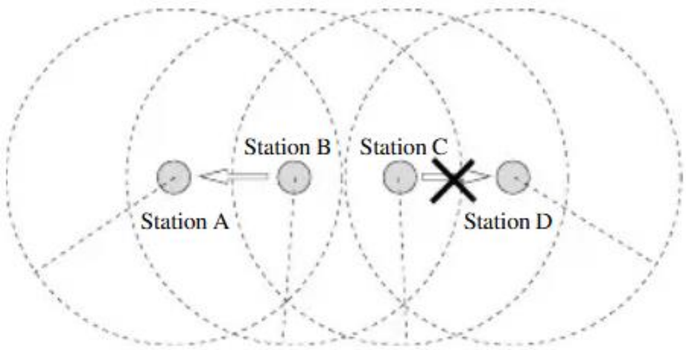


Figure 2.5 – Exposed terminal problem [16].

Network Congestion

Increased message traffic increases the likelihood of network congestion. As a result, messages may be lost, an increased latency should be expected and the appearance of the exposed node problem may be detected, thus impairing communications. Within this context, excessive retransmissions and exchange of messages between nodes are the main causes of network congestion.

2.1.2.2. MAC protocols

MAC protocols have two approaches. One is based on contention, where the nodes that need to use the medium compete and the winner can access and transmit information. The other approach is based on time slotting reservation, where time interval that allows nodes to access and transmit information whenever their turn comes, are pre attributed to a node.

- Reserve-based protocols

This type of protocol is the most complex, as a priori knowledge of the network organization and temporal synchronization between network elements is required. One of the main protocols of this approach is Time Division Multiple Access (TDMA) [17], [18]. In this scheme, the frequency channel used is divided into several time intervals (slots), which is the only time at which the node can access the medium. [18]. Figure 2.6 illustrates this division into slots for each frame. This procedure will lead to a reduction in collisions, since the various nodes in the network will never transmit information over the air at the same time, ensuring the fairness of the network. Even so, due to temporal slotting, the throughput cannot be increased beyond the use of these time slots.

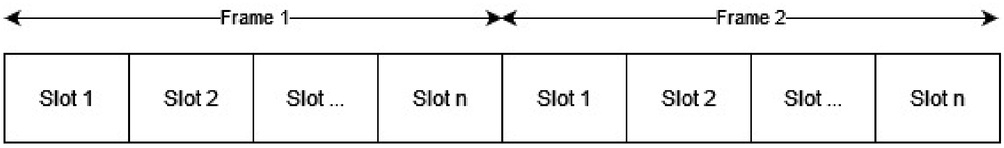


Figure 2.6 – Basic operation of the TDMA MAC protocol.

- Containment Based Protocols

There are two main protocols for this approach: Advocates of Linux Open-source Hawaii Association (ALOHA) and Carrier Sense Multiple Access (CSMA). ALOHA is the pioneering medium access protocol mechanism. The nodes access the network when they have a message ready to transmit and waited for an acknowledgment signal (ACK) from the receiver [13], [16]. But, in this type of mechanism, the probability of collisions between transmitting nodes is high. To reduce the occurrence of collisions, ALOHA was combined with the TDMA protocol known as Slotted-ALOHA [19]. Thus, a node must wait for its predefined time interval to start transmission. Slotted-ALOHA increased robustness and efficiency compared to the original ALOHA, however, it introduced the need for synchronization [16], [17]. In this way, the Slotted-ALOHA MAC protocol classification framework can be considered a hybrid by combining the two approaches.

In the CSMA [16] mechanism, before each transmission, the node "feels" the medium to avoid collisions. If there is a transmission in progress, the transmitter waits a random period before trying again. If the medium is free, the node sends the data packet [19]. This strategy only avoids collisions, not addressing the exposed and hidden node problems. To address the first, there is a CSMA/CA variant [13], [20], where a virtual detection of the environment is carried out, through two control frames. That is, the transmitter sends a Request-to-Send (RTS) frame to the receiver, which responds with a Clear-to-Send (CTS). If the sender receives the CTS, it transmits the message again after a random period. Any node other than the intended recipient receiving an RTS or CTS delays its transmissions, thus mitigating the hidden node problem. However, virtual sensing amplifies the problem of exposed nodes since all nodes that receive a CTS unnecessarily refrain from transmitting [14].

There are a variety of containment approach protocols that go beyond ALOHA and CSMA/CA. Namely, protocols that derive from these two initial mechanisms, as is the case with CSMA/CA. For example, the Multiple Access with Collision Avoidance (MACA) protocol [21], which reduces the exposed node problem. The Broadcast Medium Window (BMW) [22], which solves the hidden node problem in Broadcast-style communications.

2.1.3. Routing

In Ad Hoc networks, it is very common for communication between the sender and the receiver to pass through intermediate terminals, which function as data packet switches [23]. This sequence of interconnected nodes is called a route. The process of discovering it is called routing [23].

According to the approach in [24] to represent routing design concepts in wireless Ad Hoc networks, several central and auxiliary components are presented. Within these components, the neighbour's discovery element stands out, which plays an essential role in calculating routes, providing each node with information about connections with the remaining nodes. This information includes characteristics such as location, direction, identification, among others. It is important to highlight the direction property, as it can be bidirectional, given the ability of a node to receive and send messages to other devices [14]. Generally, there are several routes available between the sender and the recipient. Moreover, routing solutions strive to discover the best routes to use, applying metrics to different routes [14]. These metrics refer to the parameters used by routing algorithms, such as connection quality, the number of "hops", that is, the number of retransmissions between the sender and receiver, channel noise or latency. Furthermore, the route quality parameter can be added, which includes parameters such as processing and memory power, security, energy consumption, among others [24]. Again, highlight that the metrics are also directional, that is, they can present different values in each direction, with the possibility of dissymmetry in sending messages in each direction [14]. To choose the best path, it is also important to consider the route representation component. This explains how route information is stored during route discovery and selection [24]. Typically, this information is encoded in a structure called a routing table [14].

The need for relay nodes and the various components to build routing structures implies many challenges [14]. Namely, scalability [25], where the system must remain efficient in terms of network growth and guarantees in the event of transmission failures. Furthermore, there is the challenge of mitigating route changes, which happen in a short space of time, as is the case with the solution proposed in [26].

2.2. LORA TECHNOLOGY

LoRa is a physical layer wireless communication technology (Figure 2.7) for LPWAN that allows long-range transmissions with low power consumption. In the LoRa context, two distinct layers can be referred to: the physical layer, which uses a modulation technique developed by Semtech; and a MAC layer protocol called LoRaWAN, under development by the LoRa Alliance.

2.2.1. Physical Layer - LoRa

LoRa [27]–[30] is a physical layer and modulation technique developed by Semtech. LoRa enables long-range, low-power, low-throughput communications. Depending on the region in which is implemented, it operates in the ISM bands of 433, 868 or 915 MHz, (433 MHz in Asia, 433 MHz and 863 to 870 MHz in Europe, 902 to 928 MHz in the US) [31].

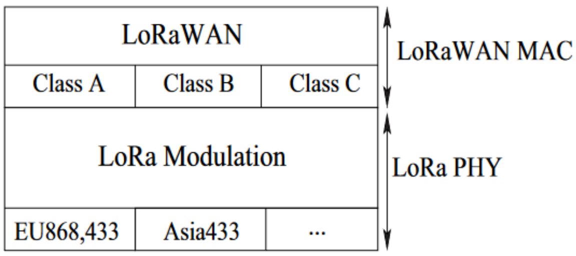
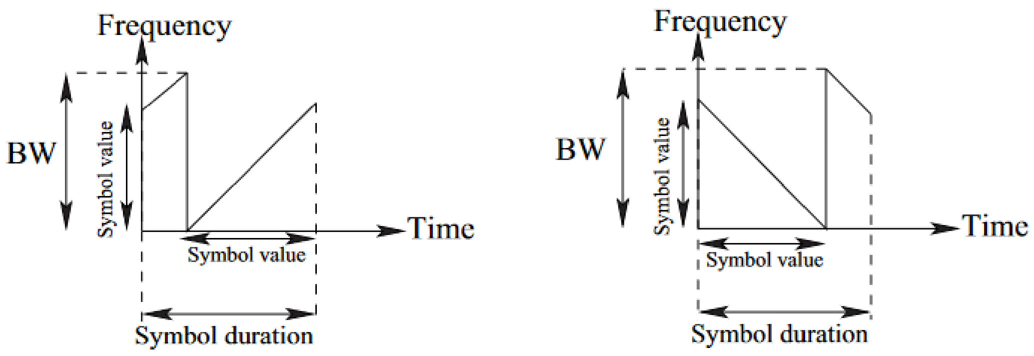


Figure 2.7 – LoRa/LoraWAN protocol architecture [31].

LoRa technology uses the Chirp Spread Spectrum (CSS) "frequency spread" modulation technique, where symbols are encoded in ascending (Figure 2.8a) or descending (Figure 2.8b) radio frequency signals. The use of CSS ensures a better power balance in communication, as well as better immunity to interference in the network. Therefore, the use of this modulation offers high performance in terms of range, increasing signal robustness and receiver sensitivity, while maintaining low power consumption. [31].



a) b)

Figure 2.8 – Examples of chirps: a) ascending chirp; b) descending chirp [31].

2.2.1.1. LoRa Parameters and Transmission Options

The LoRa radio has five possible configuration parameters: Transmission Power, Carrier Frequency (CF), Bandwidth (BW), Spreading Factor (SF), and Coding Rate (CR). These parameters can be configured in 6720 different combinations [32], which determine power consumption, noise resilience and transmission range.

- Transmission Power

The transmit power of a LoRa radio can be adjusted from -4 dBm to 20 dBm, on a 1dBm scale. By default, the transmit power of a device is typically 14 dBm [31]. The selection of this parameter influences the communication range, signal sensitivity, immunity to external interference and energy consumption, which increases with transmission power.

- Carrier Frequency

The CF represents the central transmission frequency used in a band. This can be programmed between 137 MHz to 1020 MHz, in 61 Hz steps. Depending on the LoRa chip, this range can be limited to 860 MHz to 1020 MHz [32].

- Bandwidth

BW is the range of frequencies available for transmission. A higher BW allows transmission to occur at a higher data rate (DR), leading to a shorter Time on Air (ToA) and lower sensitivity (due to the integration of additional noise). In contrast, a lower BW allows for higher sensitivity but at a lower DR. Most LoRa radios have three adjustable bandwidth values: 500 kHz, 250 kHz and 125 kHz.

- Spreading Factor

The SF defines the number of bits encoded in each symbol, determining the duration of a T_{sym} symbol as shown in the following formula:

$$T_{sym} = \frac{2^{SF}}{BW} \tag{2.1}$$

Each LoRa chirp (a T_{sym} symbol) consists of a linear frequency "sweep" (frequency variation linearly over time) [33] and can encode 2^{SF}possible values. For example, with $\mathrm{SF} = 7$, there are $2^{SF} = 128$ possible values per symbol. SF can vary in a range of 6 to 12, where SF6 is a particular case and requires special operations [28]. The duration of the "sweep" is called symbol duration, and depends on the SF as well as the bandwidth, as illustrated in Figure 2.8. SF has an influence on transmission duration, energy consumption, robustness, and communication range. The lower the SF, the higher the data rate, but the lower the immunity to interference, therefore, the shorter the range. On the other hand, a large SF increases the signal-to-noise ratio (SNR) and, therefore, the receiver sensitivity and signal range. However, it reduces the transmission rate and thus increases transmission duration and energy consumption [31].

- *Coding Rate*

CR determines the rate of the Forward Error Correction (FEC) technique code, [34] according to the following expression:

$$\mathrm{CR} = \frac{4}{(4+n)}, \text{with } n \in [1;\ 4] \tag{2.2}$$

The CR offers better protection against interference and therefore higher CR offers more robust transmission but increases ToA [35].

2.2.1.2. LoRa Physical Layer Frame

A LoRa frame starts with a preamble, which is used to keep the receiver synchronized with the transmitter. The preamble begins with a programmable sequence of ascending chirp symbols ($n_{preamble}$). Then, there are a final 4.25 LoRa symbols, where of these symbols, two encode a synchronization word and the rest indicate the end of the preamble, as illustrated in Figure 2.9. This synchronization word depends on the LoRa parameters being used by the device transmitting the packet.

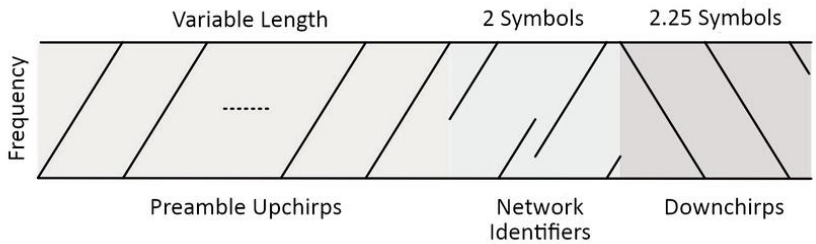


Figure 2.9 – LoRa preamble structure [36].

After the preamble, there is an optional header at a CR code rate of 4/8. This field includes a cyclic redundancy check (CRC) of the header to allow the receiver to discard packets with invalid headers. Furthermore, the header contains information about the length of the next field, the payload. This segment is limited to 255 bytes of data. At the end of the LoRa packet there is an optional 16-bit CRC payload [31]. Both the payload field and its optional CRC are encoded according to equation (2.2) (2.2). Figure 2.10 represents the LoRa packet structure.

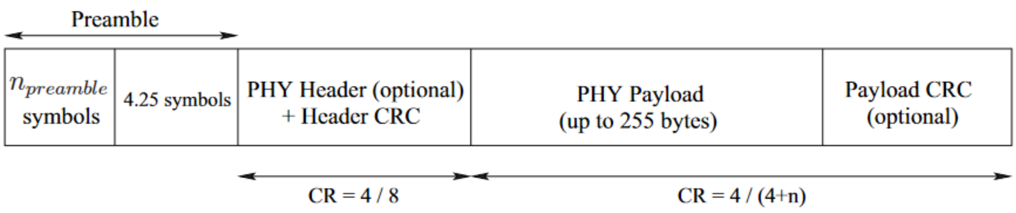


Figure 2.10 – LoRa plot structure [31].

According with [31], for a given BW, SF and CR, the time required to transmit a LoRa frame from an end device to the GW is the sum of the preamble transmission time $T_{preamble}$ with the payload $T_{payload}$:

$$T_{frame} = T_{preamble} + T_{payload} \tag{2.3}$$

The $T_{preamble}$ is dependent on T_{sym} and of the number of symbols in the preamble $n_{preamble}$:

$$T_{preamble} = (n_{preamble} + 4.25) * T_{sym} \tag{2.4}$$

Also, the $T_{payload}$ depends on T_{sym} and the number of symbols in the payload:

$$T_{payload} = n_{payload} * T_{sym} \tag{2.5}$$

where

$$n_{payload} = \max(\beta(CR + 4), 0) + 8 \tag{2.6}$$

and

$$\beta = \left\lceil \frac{8PL - 4SF + 28 + 16 - 20H}{4(SF - 2DE)} \right\rceil \tag{2.7}$$

where PL represents the payload size in bytes; $H = 0$ if the header is present, and 1 if it is not; $DE = 1$ if low data rate optimization [30], [37] is enabled, or 0 otherwise.

2.2.2. MAC Layer - LoRaWAN Protocol

LoRaWAN [5] is a MAC protocol based on LoRa technology and developed by the LoRa Alliance. It is a network that allows communication between end devices and a network server through a GW. While LoRa is a proprietary modulation from Semtech, LoRaWAN is open source. In addition to the LoRa physical layer features, LoRaWAN also optionally supports Frequency Shift Keying (FSK) modulation [31]. The LoRaWAN network operator has the autonomy to assign network channels to the various terminals. In the European context, there are three predefined channels as shown in Table 2.1. The network's GWs must always be listening to at least these three channels. According to LoRaWAN specifications, the above-mentioned three channels can be used for both UL transmissions and DL transmissions [31].

Table 2.1 – LoRaWAN standard channels U863-870 [5].

Modulation	Bandwidth $[kHz]$	Frequency Channel $[MHz]$	LoRa DR	Number of channels	Duty cycle
LoRa	125	868.10 868.30 868.50	DR0 to DR5	3	<1%

2.2.2.1. LoRaWAN architecture

The LoRaWAN network organization is the star-of-stars. According to the specification [5], the network is essentially composed of end devices, GW and a network server, as shown in Figure 2.11.

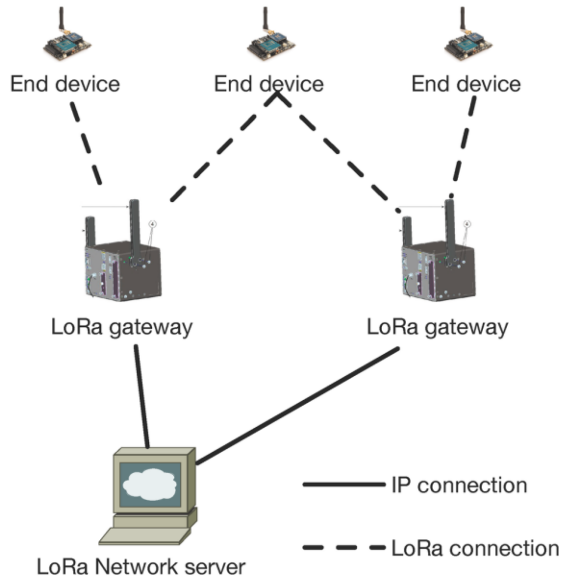


Figure 2.11 – LoRaWAN network architecture [38].

- End Devices

End devices are nothing more than sensors or actuators that can send or receive data from the network server through GW.

- LoRa Gateways

GW are access points to network nodes. All data transmitted by a node is sent to the GW visible to that network element. Each GW that receives the signal transmits it to a cloud-based network server via cellular, Ethernet, satellite, or Wi-Fi links.

- The network server

This is the LoRaWAN core element. As shown in Figure 2.11, it manages the GW through Internet Protocol communication. Of many features, the LoRaWAN network server provides mechanisms for end device authentication and authorization [5], [39], encryption [40], [41], data transmission, data rate adaptation (ADR), deletion of duplicate packages, and interface with applications.

Recently, the LoRa Alliance released a new specification [42], which adds a new node to the network with relay functionality, evolving the network beyond a star architecture. Its implementation will allow greater and robust coverage of the LoRaWAN network to all network nodes, at a minimum cost [43]

2.2.2.2. Duty Cycle

The European Telecommunications Standards Institute (ETSI) presents regulations that restrict, namely, the maximum transmission power and the duty cycle, which vary depending on the region/country.

According to the specifications [5], [37], the LoRaWAN network uses a duty cycle-based transmission type, which limits the rate at which the end device can transmit messages. This is because the duty cycle is the maximum percentage of time that a node can occupy a channel. For example, if a device transmits on a channel with a duty cycle of 1%, it can make 10 transmissions of 3.6 seconds within one hour. If it exceeds this minimum waiting time between transmissions, the node can switch transmission to another band. If the remaining channels are unavailable, the device must wait before any further transmission [31]. Table 2.2 shows the default LoRaWAN channels with their regulatory restrictions in the European framework.

Table 2.2 – Duty cycle and maximum transmission power restrictions on LoRaWAN channels in Europe [5].

Frequency [MHz]	Direction	Duty cycle	Maximum transmission power (dBm)
868.1	DL, UL	1%	14
868.3	DL, UL	1%	14
868.5	DL, UL	1%	14
869.525	DL	10%	27

2.2.2.3. LoRaWAN communications

Adaptive Data Rate

The ADR allows the network server to adapt the data transmission rate of a node, changing the SF and transmission power, to find the best compromise between energy efficiency and connection robustness. Therefore, it is possible to say that ADR strengthens the network capacity. The possibility of optimizing bandwidth, connection ToA and energy consumption allows for greater network performance and scalability.

In practical terms, it follows that network elements located close to the GW must typically use higher DR, that is, use a lower SF, and end devices further away must use a high SF. This entire algorithm is based on the SNR of the connection, the number of GW that receive the signal, the DR and the Received signal strength indication (RSSI) [44].

Device Classes

End devices in LoRaWAN can be configured into three different classes, which determine how downlink traffic is received. Each class constitutes a compromise between battery life and downlink communications latency. The LoRaWAN network therefore allows three operating classes for end devices: class A, B and C as shown in Figure 2.12.

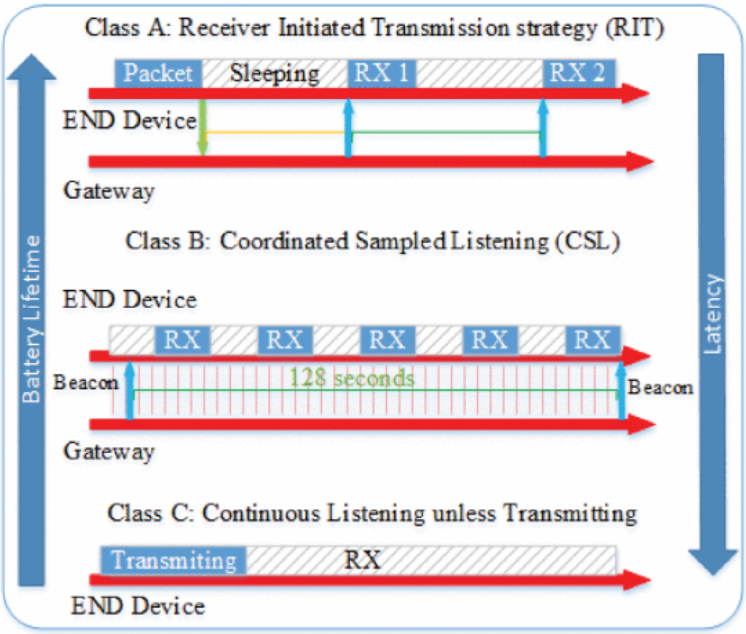


Figure 2.12 – LoRaWAN class mechanisms for end devices [45].

- Class A

In energy terms, class A is the most efficient, since end devices are "sleeping" most of the time. This class follows the ALOHA communication method, that is, whenever the end devices have data packets available, they send them. However, reception of DL data is only possible after UL communication, where only two windows (RX1 and RX2) are opened to receive data with a latency of 1 second (by default) for each of them. If there is a need to send more DL data, the node must wait for the next UL transmission. The device does not open the second reception window if the data packet was successfully received at RX1.

- Class B

In this Class B, nodes open extra reception windows (ping slots) at scheduled times, receiving a synchronized alert (beacon) from the network server through the GW. This allows the network server to know when the end device is listening. Any of these ping slots can be used by the network to initiate downlink communication.

- Class C

In this last class, the end devices are always "listening", as the reception windows are almost always continuous, closing when they transmit. This aspect of continuity leads to latency-free communication but causes an increase in energy consumption compared to the other two classes.

Network joining

Joining a LoRaWAN network requires a device to undergo an activation process in two ways: Over-The-Air Activation (OTAA) and Activation By Personalization (ABP). Network joining requires:

- Device Address (DevAddr)

It consists of a 32-bit identifier that is unique within the network. Seven bits are used as the network identifier, and 25 bits are used as the device's network address.

- Network Session Key (NwkSKey)

It consists of a 128-bit Advanced Encryption Standard (AES) encryption key that is unique across different network servers. This key, which is shared between an end node and the network server, is used to calculate, and verify the message integrity code, protecting your data [5].

- Application Session Key (AppSKey)

Like the previous key, it consists of 128-bit AES encryption. It is used by both the application server (server responsible for the LoRaWAN application layer) and the device to encrypt and decrypt the payload field of application-specific data messages. Application payloads are end-to-end encrypted between the network node and the application server but are not integrity protected. That is, a network server may be able to change the content of data messages in transit [5].

- Application identifier (AppEUI):

It is a unique 64-bit identifier, which meets the IEEE EUI64 standard [46]. It is used to identify the Join Server (server that helps connect devices to the LoRaWAN network) during activation.

As previously mentioned, joining the network respects both methods. It should be noted that regardless of the type of activation, the various elements of the network must be assigned an address that uniquely identifies them. The address is designated as DevEUI which respects the same IEEE EUI64 standard. Below is a description of the joining methods:

- OTAA

In this procedure, the end device exchanges join request and join acceptance messages. During this membership period, the network node is dynamically assigned the DevAddr address, and security keys are negotiated between the network server and the node. This procedure is repeated each time the device turns off [5] and is disconnected from the network.

- ABP

This type of activation requires that the DevAddr identifier and the two session keys, NwkSKey and AppSKey, are directly stored on the network node. When the device is turned on for the first time, communication may start immediately, without needing to exchange opt-in messages. This activation method is the least secure, as it keeps the session credentials throughout its lifetime. Furthermore, it has the disadvantage that nodes cannot change network operators without manually changing the key on the device [5].

2.2.2.4. Collisions

LoRaWAN specifications provide nodes transmission freedom in terms of time, channel choice and DR, if they respect the region's duty cycle. However, the final node cannot fully evaluate and predict the possibility of collisions. And therefore, when two LoRa transmissions overlap upon arrival at the receiver, there are several conditions that determine whether it can decode either or both transmissions (frames), or neither. These conditions depend on power, time, CF, and SF.

- Time

In a temporal frame, two frames overlap when their reception time intervals coincide. That is, two frames x and y do not overlap according to the following conditions:

$$b_x \leq a_y \wedge a_x \geq b_y \tag{2.8}$$

where the transmission starts in moment a and ends at moment b.

- Carrier Frequency

When two transmissions occur simultaneously in time but do not share the same CF, the two signals do not interfere with each other and can be successfully decoded (assuming a receiver can receive on both frequencies). The CF overlap is defined as the absolute difference between these frequencies, also considering an allowable frequency deviation, which is related to the bandwidth used. Therefore, from a frequency point of view, the following condition can be defined for the occurrence of collisions:

$$|f_x - f_y| > f_{Threshold} \tag{2.9}$$

where f_x and f_y are the x and y central transmission frequencies, and $f_{Threshold}$ is the minimum frequency offset that allows signal decoding. For example, in the case of the Semtech SX1272 module [47], the minimum offset is 60 kHz for a 125 kHz bandwidth, 120 kHz for a 250 kHz BW, and 240 kHz for a 500 kHz BW.

- Spreading Factor

The near orthogonality of the SF [48] allows the reception of several signals in parallel on the same channel, if they use different SF. Therefore, transmissions that overlap in time and frequency can be successfully decoded, if their received powers satisfy the capture effect condition (which will be discussed below). In this way, a collision is defined with the following equality:

$$SF_x = SF_y \tag{2.10}$$

where SF_x and SF_y are the value for the SF of both x and y transmitions.

- Power.

Since LoRa technology is a form of frequency modulation, there is the possibility of a stronger signal overpowering a weaker signal at the time of reception. This phenomenon is called the capture effect. However, the strengths of the received signals can be relatively close. When the difference is too small, the receiver continues to switch between the two signals, effectively not being able to decode either transmission. Therefore, packet x collides with packet y under the following conditions:

$$\begin{cases} Collision, & |P_x - P_y| > P_{Threshold} \\ No\ collision, & |P_x - P_y| \leq P_{Threshold} \end{cases} \tag{2.11}$$

where P_x is the strength of the signal received from transmission x and P_y is the strength of the signal received from transmission y and $P_{Threshold}$ is the threshold power that determines whether or not the signals overlap.

2.3. RELATED WORK

The purpose of this subchapter is to review some existing relevant works, providing a summary of some concepts and conclusions that were crucial for the development of this project. Chapter 2.3.1 presents empirical studies that evaluated the LoRa technology and its LoRaWAN MAC protocol. Chapter 2.3.2 shows the operation and results of MAC protocols integrated with the LoRaWAN network, with the aim of improving its performance. Finally, Chapter 2.3.3 shows the development of multi-hop networks to overcome the limitations of the LoRa technology.

2.3.1. Performance of LoRa Technology

LoRa technology is relatively recent, which has motivated the conduct of empirical studies to evaluate its performance. These studies aim to understand how the variation of LoRa parameters affects the behaviour of a LoRa cell or network, especially in terms of coverage, capacity, and resilience to interference. In addition, it is sought to understand how the terrain relief and urban environments influence LoRa signals. Within the MAC layer, it is intended to understand the performance and operation capability of the LoRaWAN network, including the effect of ALOHA-based medium access mechanisms, DL traffic, and duty cycle.

2.3.1.1. LoRa Physical Layer

To assess the coverage around a LoRa GW, the study of [49] conducted in a coastal city of Oulu, Finland, proceeded to mount a final device on the roof of a car and on the mast of a boat. The GW was located 24 m above sea level. The node was configured with a SF of 12 and a transmission power of 14 dBm. On land, more than 80% of the packets were successfully delivered for distances less than 5 km. However, for distances greater than 10 km, the success rate in transmission dropped to about 20%. On water, the success rate was relatively higher, reaching approximately 70% for distances between 5 and 15 km. The authors of the study concluded that, to date, this technology met the requirements of applications in smart cities and that the topography had a significant impact on reception rates.

In a study like the previous one, but conducted in an urban environment with more interference, the authors [38] evaluated the coverage of the LoRa network in Paris, France. Variations were made in the final device settings, including different SFs of 7, 9 and 12, all with the same transmission power of 14 dBm. The tests demonstrated that LoRa can provide satisfactory network coverage within a radius of up to 3 km in a suburban area with residential density. Changing the SF showed to have a significant impact on coverage. The closest test point (650 m) achieved a 100% success rate in receiving packets with a SF of 12, but this rate decreased to 84% when a SF of 7 was used. It is worth noting that at the farthest test point (3400 m), the message delivery rate was 38%, and sending packets with SF of 7 and 9 was unsuccessful.

Providing a perspective on LoRa coverage in the city of Coimbra, the authors [50] presented a set of results with different sending characteristics (SF and BW). The tests resulted in high reception rates within a radius of 2000 m. However, the city of Coimbra has an irregular relief, composed of hills. This characterization was the main factor for a test point to present the worst packet reception rate (62%). These studies have shown that a channel with favourable conditions increases the possibility of assigning smaller SFs, making the network with greater capacity.

When it comes to the UL data transfer rate that a LoRa device can achieve, a study conducted by the authors [51] revealed that a final node located in the vicinity of a LoRa GW reaches a rate of 2 kbit/s. For nodes further away, the UL transmission rate is limited to 100 bits/s. These same authors also examined the scalability of LoRa networks and observed that the network elements that need to send longer payloads should be close to the GW. In addition, the results indicated that a LoRa network can accommodate multiple devices, if all nodes send small amounts of data daily. Another factor that the authors [52] point to as limiting the scalability of the LoRa network is the distribution of the nodes, that is, the increase in the number of end devices can impact the coverage range of the network.

One of the factors that impairs the performance of the LoRa network is interference. The use of the CSS technique by LoRa, according to the simulations performed in [48], showed that it is an essential feature to combat them. However, they found that the symbols in CSS are not perfectly orthogonal. Taking this fact into account, the authors [53], [54] recorded the interference that LoRa signals are susceptible to. They investigated the behaviour when two signals coincide in time and use different and/or equal SF (with the same BW and CR). The results showed that coincident signals with different SF are lost if the difference between the power of the sent signal and the "interfering" signal is less than 16 dB. Thus, this type of interference could be combated by adjusting the transmission power levels of the nodes. However, the authors stated that this hypothesis is counterproductive, as environmental conditions, the appearance of obstacles, and the mobility of the nodes are not predictable. These findings led to the conclusion that the implementation of LoRa cells cannot be considered independent of the others, since the different SF transmissions are far from being perfectly orthogonal.

In order to combat the aforementioned interferences, the authors [55] used two methods: directional antennas and the use of multiple GWs. Based on the results of simulations, they found that both solutions increased the packet reception rate. However, the implementation of multiple GWs is more efficient than the use of directional antennas. In addition, from a practical point of view, the use of multiple GWs is more advantageous when equipping the devices with directional antennas.

To verify the phenomenon of the capture effect, which was found in Chapter 2.2.2.4, the authors [56], [57] implemented a receiver and two transmitters that sent a 32-byte data packet, with a power interval of 1dBm. Figure 2.13 shows the results of the experiment for an SF12 and BW250.

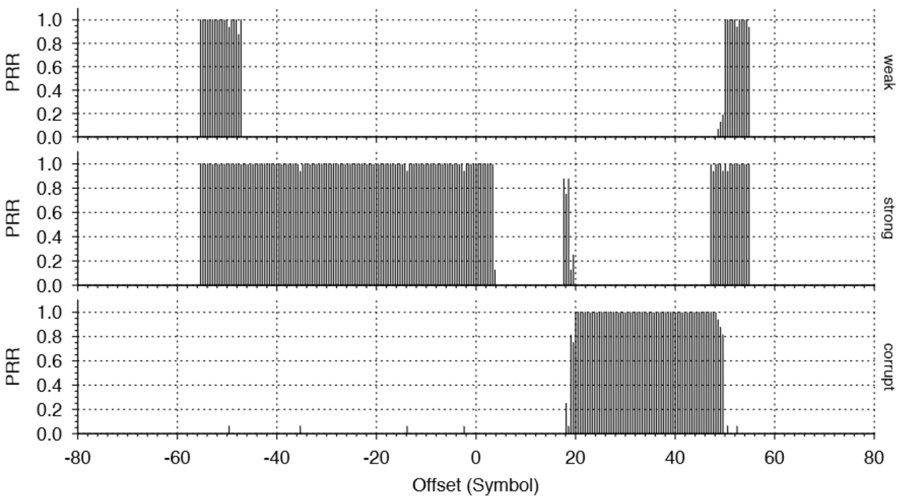


Figure 2.13 – Capture effect [56].

Based on the results of the previous figure, the authors concluded that the transmission with the highest power is successfully received when the packet is sent earlier up to a maximum of 3 symbols later than the transmitter with the lower power (capture effect). However, with an offset of more than 3 symbols until the end of the packet, no transmission is executed successfully. It is known that a receiver, from the last 5 symbols of the preamble, ignores the remaining transmissions, to reach its synchronization. The transmissions were sent with 8 symbols of the preamble. Therefore, after 3 symbols, the receiver was only listening to the transmission with the lower power, but its signal was suppressed by the transmission with the higher power, leaving the packet corrupted and both transmissions lost. Figure 2.14 shows a temporal representation after the offset of more than 3 symbols of the transmission with the highest power N2 in relation to the one with the lower power N1.

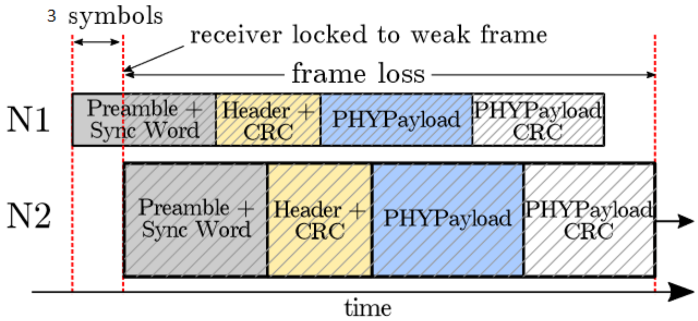


Figure 2.14 – Example of the loss of two LoRa communications through capture effect [57].

Based on the results obtained above and from Figure 2.13, it is concluded that the packets are lost if they are not protected by at least about 5 preamble symbols (in the case of a weak packet). Therefore, the following temporal window can be defined in the representation of both transmissions being corrupted:

$$[a_x + T_{sym} \times (N_{pp} - 5), b_x] \tag{2.12}$$

Where N_{pp} is the programmable number of the preamble length.

Finally, the authors [58] conducted an evaluation of packet losses in point-to-point links, also known as point-to-point (P2P), between low-altitude LoRa SX1276 [37] terminals. They conducted experiments in various environments, including urban, coastal, and forest. In all scenarios, they were able to achieve coverage ranging from several tens of meters (~100 m) to kilometres. According to the authors, these results confirmed that the LoRa technology is an interesting choice for establishing Ad Hoc wireless networks in various IoT applications.

2.3.1.2. LoRaWAN Architecture

The absence of clear channel assessment mechanisms and unregulated access to the medium (based on ALOHA) is one of the critical factors limiting the performance of the network. According to the authors [38], based on the simulation results, they analysed that the LoRaWAN network is like the ALOHA protocol, where its performance degrades according to the channel usage. Like the previous work, the work [59] showed that as the number of nodes and transmission rates increase, the percentage of messages received drops rapidly due to the higher number of collisions. It is worth noting that at a certain point, the percentage drop slowed down, due to the LoRaWAN duty cycle restriction. Thus, in a LoRaWAN network with a small number of terminals, the duty cycle is a limiting factor of the number of messages received, on the other hand, in a larger scale network, the reason that impairs its performance is collisions between packets. When it comes to mitigating this type of problem, all authors agree that the implementation of a larger number of GWs is a good solution. In addition, the implementation of UL and DL message scheduling strategies are quite viable hypotheses.

Another factor that limits the performance of the LoRaWAN network is the high traffic of DL messages. The authors [60] showed that the percentage of packets received decreased significantly if DL traffic is present, in contrast to the case of only UL messages without the need for confirmation. This problem was more evident when the number of terminals increased. According to [61], this limitation is associated with the duty cycle for DL transmissions. And, about UL under confirmation, as the network evolves, GWs begin to have difficulty sending ACKs, along with the data from the remaining DL links. Therefore, it is essential to consider the number of retransmissions in the case of UL with the need for ACK. The results obtained found that, for networks with many nodes, a high set of attempts is required. However, for networks that are not very "saturated", the authors reached values above 95% of successful ACKs, with only two retransmissions. It is worth mentioning that, with the high number of retransmissions, the results showed that the energy consumption increased significantly. In the worst case, it increased to 500%. Therefore, it is of the utmost importance to decide alternative strategies instead of LoRaWAN retransmissions.

2.3.2. LoRa MAC protocols

The implementation of MAC protocols is essential to avoid packet collisions or to improve the performance of a network. Solutions will be presented with a focus on improving the performance of the LoRaWAN network, according to the two approaches of MAC protocols: Reservation-based, where the authors implemented or simulated methods that require end devices to transmit information in a given time interval; contention-based, where the studies aimed to combat medium access through listen-before-talk protocols. It is worth noting that some of the authors listed took advantage of the existence of the Channel Activity Detection (CAD) mechanism of LoRa modems. This particularity of LoRa transmitters was designed to detect preambles transmitted through the same channel and SF.

2.3.2.1. Reservation-based protocols

It is known that the LoRaWAN network uses a medium access control protocol based on ALOHA, which has limited performance due to the high probability of collisions. To address these limitations, the authors [62] explored the Slotted-ALOHA method as a replacement for the pure ALOHA used in the LoRaWAN network. In this protocol, the channel is divided into time intervals (slots), and each end device must transmit a message only at the beginning of a slot. Synchronization of the nodes in the network is essential, and this process is facilitated by the LoRaWAN stack. The duration of the slots is determined based on the ToA of the data packets, the temporal overhead of the LoRaWAN protocol, and the need to compensate for clock offsets. The results indicated that this method had a significant impact on reducing energy consumption, doubling the network performance, and reducing message collisions by a third.

An approach adopted by many research studies has been the TDMA method, which takes advantage of its ability to reduce collisions, reliability, performance, and energy efficiency. For example, the work [63] introduced a protocol called Class S ("Slotted"), like S-ALOHA for UL transmissions, but incorporating the Class B synchronization functionality. This protocol divides time into slots large enough to accommodate the ToA associated with the largest SF used by any node. This allows allocating DL and UL messages in slots between each beacon sent by the network. Simulations showed that as the number of end devices increases, the network becomes more efficient and energy efficient compared to Class A solutions. However, this performance requires end devices to ignore some beacons; otherwise, the energy consumption would significantly exceed that of Class A devices. Therefore, the authors emphasized the need to develop an intelligent switching mechanism between the two classes to optimize the overall performance in all dimensions of the network.

Other authors [64] presented a scheduling algorithm to improve the scalability of the LoRaWAN network. In this protocol, a LoRaWAN network server schedules the SF values, frequency channels, and slots for all connections in the network. This algorithm is activated whenever the GW receives a scheduling request from a device in the network. The algorithm assigns the device a SF value based on the received signal power and then selects a channel and a time slot. These choices are made in a way to allow multiple simultaneous UL connections with the same SF value. Additionally, the authors developed a group acknowledgment (GACK) message of UL messages sent in each period, thus protecting DL traffic and improving GW capacity. All the synchronization required for the operation of this algorithm is enabled by the Class B functionalities. Simulations of this algorithm revealed a 60% increase in network capacity compared to the LoRaWAN standard (i.e., ALOHA). Additionally, they achieved a 90% packet reception rate in a network with approximately 8000 devices.

2.3.2.2. Contention-Based Protocols and CAD

The authors [65] presented a MAC protocol based on CSMA/CA, with the RTS/CTS mechanism to control access to the medium. They assumed this type of protocol, since the synchronized and scheduled approach would be difficult to execute due to the possibility of long distances between the nodes. They added a wait to send (WTS) packet to CSMA/CA, which is sent when a node receives an RTS message while receiving data from another node. The decision was motivated by the characteristics of LoRa, since higher intensity packets are not affected by interference from a lower power packet.

The CAD mechanism of LoRa modems opened the door for the development of contention-based protocols. In this sense, tests were carried out to verify the reliability of CAD for this type of application. As is the case of the study [28], where the authors demonstrated that CAD is intended only to detect the preamble in transmissions using the same channel (BW/SF). The results showed that the preamble of a transmission can be detected with a high probability (97%), while false positives with a low probability (0.092%), if the data packets have the same SF and BW parameters. Otherwise, the probability of false positives increases significantly.

The author [66] revealed a considerable probability that the CAD mechanism will identify not only the preamble, but also the transmission itself. In addition, he observed an increase in the number of false positives in CAD as the distance between the transmitting nodes increases. Based on these observations, the author proposed a LoRa protocol that adopts a modified CSMA method. In this protocol, when a node wants to transmit data, it repeatedly checks if the channel is free, performing consecutive CAD checks for a period equivalent to the maximum flight time (maximum ToA) of a packet. If all CADs do not detect any transmission, the node considers the channel free and proceeds with its transmission. However, if a CAD identifies any transmission, the node delays the transmission for a waiting period (maximum ToA) and, after that period, the process is repeated, until a maximum number of attempts is reached. The implementation of this protocol proved to be a more energy-efficient and more viable solution for LoRa networks compared to the classic CSMA protocol (as defined in the IEEE 802.11 standard).

The authors [67] compared their work to the previous work [66] and presented three improved CSMA mechanisms that take advantage of CAD. In their first approach (LoRa-BED), a node that wants to send a message checks the channel's freedom. If the channel is free, it transmits after a random time between the time interval of 0 to maximum ToA. On the other hand, if the channel is busy, the node checks the medium again after a certain delay. This time decreases gradually with each attempt to check the channel until a minimum limit is reached. In the second approach (LoRa-BEB), a node always transmits when it "feels" the channel free, that is, the CAD does not detect any data packet. If the channel is busy, the node delays its transmission after a random interval of time, where it increases with each attempt. Finally, the LoRa-BEH method is presented, which is a combination of the two previous techniques. Based on a simulation platform, the results showed better performance in all cases compared to the [66] protocol. The LoRa-BEB method is the solution with the lowest energy consumption and the lowest number of collisions.

The authors [68] used a set of previous experiments, which demonstrated the ability of CAD to also detect the payload, to propose some CSMA versions. These approaches are different from previous studies, since in the protocols presented, the node fixes itself to a random BW and SF until a message is transmitted. In contrast, the versions developed by these authors, the node uses previous information to dynamically select the best channel and SF. As is the case with the LMAC-2 approach, where nodes can change channels, according to the previous records of channel saturation (i.e., with the records of the number of collisions between LoRa signals). Changing the channel can allow the network to perform better and, from the node's perspective, the possibility that the average number of CAD per transmission and the corresponding time/energy expenditure is lower, since occupied channels are avoided. With the same purpose of equalizing the occupation of LoRa channels, the authors presented a version, called LMAC-3. The difference between LMAC-2 and LMAC-3 is that historical channel information is transmitted by the GW beacons (Class B), since they contain the channel load information. The authors demonstrated greater network reliability and lower energy consumption per delivered packet, compared to the ALOHA protocol. However, no comparison was made with existing LoRa CSMA approaches.

2.3.3. Multihop Protocols in LoRa

Ad hoc wireless networks based on LoRa can take advantage of multi-hop mechanisms, which influence network performance in terms of throughput, reliability, latency, energy consumption, and coverage. Some works propose protocols that use relay nodes with the relay functionality, while others aim to incorporate more complex routing protocols.

2.3.3.1. Routing Protocols

LoRaBlink [28] was one of the first Ad Hoc protocols with multi-hop forwarding, which operates over the LoRa physical layer and works beyond the LoRaWAN 1.0 specification. It was designed in an IoT framework, where it offers low-latency, reliable, and energy-efficient bidirectional communications. This protocol has two phases. The first is the time synchronization between nodes to define medium access through slots. During this process, the node stores the number of hops that were necessary for the synchronization message to reach it. In this way, the number of hops determines the maximum depth that the network can have. Finally, the transmission of data from the nodes to the GW takes place. The transmission order is according to the number of hops stored. Therefore, if a node has a lower hop count compared to a network element with a higher number, the latter will transmit the message in the next slot. It is worth mentioning the possibility of nodes transmitting in the same slot with the result that at least one message is decoded by a receiver with a lower number of hops. In a university context, the authors implemented six nodes and a GW and showed that 80% of the packets were delivered reliably.

The authors [6] presented a solution that combines the LoRa technology with the multi-hop Concurrent Transmission (CT) protocol. This is a type of protocol that revolutionized IEEE 802.15.4 networks and is based on a flooding forwarding. CT allows multiple nodes to transmit the same or similar packets at the same time, instead of trying to avoid collisions between packets. In the work done by the authors, they were able to first prove that the CT concept works well in the LoRa context, given some robustness to collisions between LoRa packets. However, they found that the performance of CT increases by 10 to 35% if they add a restricted random temporal delay. Finally, they tested in an indoor environment, the feasibility of a LoRa multi-hop network based on CT with the implementation of the temporal offset (delay). The results confirmed that the protocol increases the coverage of the LoRa network and achieves a reliable packet delivery rate. However, this rate decreases as the number of relays per group increases, which limits the scalability of the network. The authors did not present the energy consumption record but analysing the operation of the proposed proof of concept, it is a solution that requires a certain amount of energy, which for WSN can have no practical effects.

In [69] there is a protocol called HBEE, which also takes advantage of the CT type of communication. The authors used CT to perform a hierarchical and fast network construction. In addition, they applied an implicit routing exploration (IRE) mechanism to find the best path and developed a multi-channel and multi-path (static and dynamic) forwarding for the UL of messages. The results obtained reached a packet reception rate of 95.7% and 89.8% during the network formation phase and the normal operation phase, respectively. In addition, they found that it is a protocol with a positive energy consumption and an improvement in the scalability of the network.

From the list of Ad Hoc multi-hop protocols over LoRa, there is a type of communication called linear. It is used to extend the coverage of the LoRa network from sequential relay nodes. This linear design is used when the nodes are not randomly distributed, and therefore it is an option in underground applications, such as mines and galleries. The study [70] fits into this type of applications, where the authors developed a simple routing protocol and a synchronization mechanism to monitor the old underground water distribution systems in Siena, Italy. This protocol uses a wake-up transmission scheme, i.e., a device receives a synchronization signal from a neighbouring node so that in the following moments they can receive their data and retransmit it to the next node in the network. This entire algorithm aims to minimize energy consumption. The results showed that the proposed solution is reliable and proved that the synchronization mechanism reduces energy consumption.

In [71], the authors also considered a linear multi-hop LoRa network. Like the previous study, they developed a simple routing protocol to increase the coverage of the LoRa network and added a synchronization mechanism. In this protocol, the authors added the ability to retransmit, if the neighbouring node does not receive the sent packet. The study also showed to be an effective solution, where a success rate above 90% was reached, and above 95% in activating the retransmission functionality, but resulting in triple the latency.

The authors of [72] presented a cluster-based architecture based on SF to improve the performance of LoRa Ad Hoc multi-hop networks. The proposed approach focuses on the Tree-based SF Clustering Algorithm (TSCA), which assigns nodes to several subnetworks. The algorithm was designed to ensure the connectivity of each subnetwork and to present a ToA balance between the subnetworks. This last aspect is ensured by the Breadth-First Searching (BBFS) and Top-down Breadth First-Search (TBFS) algorithms. Based on simulations, the authors confirmed a significant performance improvement compared to SF assignment in a standard LoRaWAN network (one hop). Finally, the authors implemented practical scenarios, where they positively verified the feasibility of parallel multichannel communications.

The study [73] presents an adaptation of the Destination-Sequenced Distance Vector (DSDV) routing protocol to work on LoRaWAN. The proposed solution classifies nodes into two types: forwarding nodes, which contain routing tables and other essential information to characterize the other type of node designated as Leaf Node. According to the authors, DSDV was originally designed for mobile nodes. Thus, there was a need to simplify the protocol, since the forwarding nodes are physically static. In addition, it is a solution that requires synchronization mechanisms, which is done from class B beacons. This solution has a particularity of Leaf Nodes building a LoRaWAN packet that is attached to the multi-hop frame developed by the authors. Thus, the packet will appear on the LoRaWAN network server as being sent by the node that originated it (Leaf Node) and not from the forwarding devices. The authors tested the solution in linear and bottleneck scenarios. They conclude that the solution is feasible even for duty cycle limitations.

The authors [74] presented a LoRa-based routing protocol based on a child list, which is incorporated in the GW, to create routes. In an initial phase, the child list is empty and to fill it up, a pooling-based approach is used, where the devices listen to the GW's requests. This step allows the GW to have full knowledge of the network layout. Therefore, whenever a node asks the GW for the path to another node, the GW will give it the best guess. The results showed the increase in the packet delivery rate using the multi-hop approach, compared to the standard LoRaWAN transmission.

2.3.3.2. Relay Protocols

In contrast to the previous proposals, protocols that implement relay nodes do not require establishing routes, simply retransmitting received packets to the next devices. This type of application can be more attractive due to the lower complexity and memory requirements for devices.

The authors of [75] implemented a relay node to increase the coverage of the LoRaWAN network, adding a second layer to the network. One of the main pillars in the development of the relay node was transparency, so that the end devices do not need to be aware of the existence of the relay node. The authors proposed a simple message forwarding and an automatic and asymmetric synchronization mechanism with the rest of the network, to increase the energy efficiency of the system. The study showed that the addition of relay nodes makes energy consumption decrease. In addition, they proved that the implementation of the two-layer network increases coverage and reliability compared to the standard LoRaWAN protocol. It should be noted that the work developed fits into applications with low DR and periodic UL.

Similar to the previous work, the study [76] presents a multi-hop technique with a relay to increase network coverage and reliability without degrading its capacity. The authors found that a relay tends to perform unnecessary packet forwarding that degrades network capacity. Therefore, they developed a system in which the relay node only transmits packets from the end devices that were not heard by the GW. The simulation results showed a packet delivery rate of 92%, while a 1-layer forwarding reached a ratio of 84%.

2.4. CHAPTER CONSIDERATIONS

The state-of-the-art review of this work provided a comprehensive overview of Ad Hoc wireless networks, highlighting the distinctive aspects that characterize them. In addition, the intrinsic link between Ad Hoc networks and the performance of Medium Access Control was emphasized, addressing the challenges inherent in the diffuse nature of wireless communications. In the second part of this chapter, the main characteristics and operating modes of the LoRa technology were discussed, both at the physical layer and the MAC layer. Finally, published articles related to topics relevant to the development of this project were presented. Regarding the performance of LoRa, special attention was paid to the communication range in different environmental conditions and the scalability of LoRaWAN networks. The remaining works explored multi-hop Ad Hoc protocols with similar characteristics to the one developed in this study, which will be detailed in the next chapter, with the aim of highlighting the potential of LoRa technology for Ad Hoc networks.

3. LORA AD HOC PROTOCOL

This chapter presents the purpose and design of the protocol that works integrated with the LoRaWAN network, designated as Ad Hoc LoRa. Chapter 3.1 shows an overview of the protocol, listing its network architecture to be applied and the main reasons for its development. In chapter 3.2, the various mechanisms and strategies used in the design of the protocol, which make it an Ad Hoc network, are explained. Chapter 3.3 concludes the development of the Ad Hoc LoRa protocol.

3.1. OVERVIEW

3.1.1. Problem Identification

As highlighted in Chapter 2.2, LoRa technology is characterized by long-range connections and a robust physical layer. Furthermore, it benefits from a communication protocol that facilitates the design of data transmission and reception, due to its star topology. In this architecture, GW collects data directly from end nodes, even in situations of node mobility. However, the stability of the LoRa connection may be compromised by any obstructions in the line of sight between the device and the GW, such as buildings, dense vegetation or rough terrain, or other types of electromagnetic interference. Furthermore, this type of network model increases the probability of collisions between LoRa packets, since devices with further locations from the GW and with unstable connections require the use of a high SF, resulting in data frames with a long transmission.

Given the possibility of the existence of unstable areas within the range of a GW or the inability to join the network, a viable solution could be the implementation of relay nodes. These nodes would receive the data coming from the devices and forward it to the GW. This would help ensure broader and more stable communication coverage for LoRa devices.

3.1.2. Network Architecture

The proposed LoRa network model requires, in a first phase, that all devices are configured to operate exclusively with the LoRaWAN protocol. As noted in the previous chapter, despite the significantly wide reach of this LoRa technology, a situation may arise where a node, located in an unstable connection area, may not be able to establish a direct and firm connection with the GW. When this shadow area is identified, the nodes adopt a two-hop tree topology, with the GW as the starting point. This topology consists of individual trees, each of which is composed of a one-hop node that can connect directly to the GW, in addition to a limited number of two-hop nodes. These two-hop nodes, which previously had unstable or non-existent connections in LoRaWAN, can establish connections with the GW through a one-hop node or a relay node, as illustrated in Figure 3.1. In this context, the relay node plays a central role in the network architecture, being responsible for coordinating and ensuring reliable and efficient communications in the two-hop tree model.

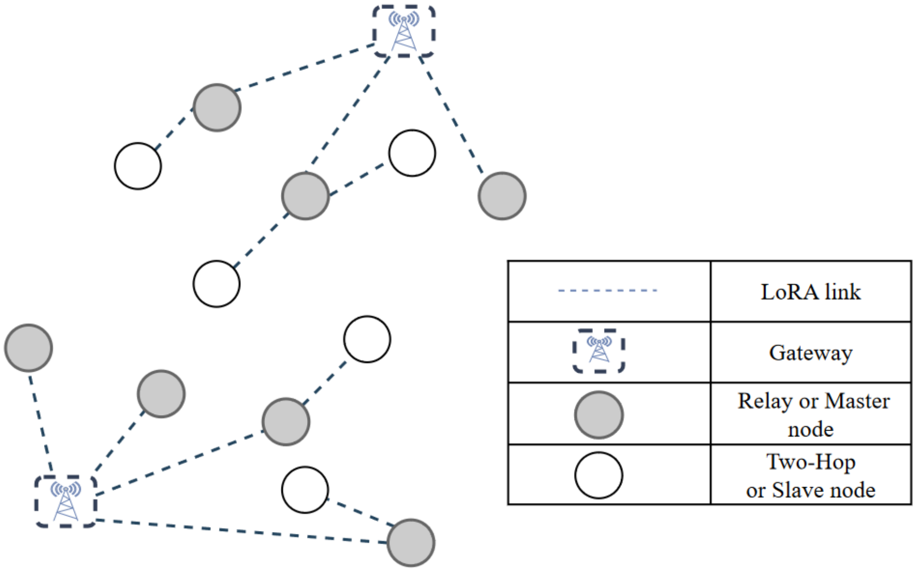


Figure 3.1 – Proposed network architecture.

Figure 3.1 shows a typical network with several two-hop links. In this example, the network consists of two GW and 12 end nodes. Seven of the twelve nodes are one-hop nodes (represented by gray circles). These seven nodes perform have a stable link to the GW using the LoRaWAN network protocol. On the other hand, the remaining four nodes (represented by white circles) are in areas of unstable or non-existent connection, and to establish communication with GW, they use the gray nodes as intermediaries routing devices. A number of nodes with stable and reliable LoRaWAN connection act as relays nodes for the nodes that have no connection.

Once the tree is formed, the proposed protocol works the same way for different trees. It is important to note that another designation used to describe the connection between the one-hop node and the two-hop node is Master and Slave, respectively.

3.2. PROTOCOL DESIGN

3.2.1. Protocol Structure

The structure of the protocol is composed of three distinct phases: a period of joining the LoRaWAN network; the Data Operation Period (DOP) and the Network Construction Period (NCP) (Figure 3.2). During the DOP phase, data from all devices in the tree is cyclically aggregated, which is then transmitted in UL to a LoRaWAN base station. In this phase, the transmission of data in DL to the devices is also handled. In the NCP phase, the nodes form a two-hop network when they are framed in a scenario that requires such a configuration.

The time of execution of the NCP phase and the periodicity of the cycles throughout the DOP is determined by the user. The moments of the NCP phase should be defined considering the environmental variations in radio frequency interference over time, in addition to considering energy considerations, since the NCP process involves an increase in energy consumption. Regarding the frequency of cycles during the DOP phase, a balance needs to be struck between energy consumption and the availability of real-time data. Figure 3.2 shows the overall protocol operation over time.

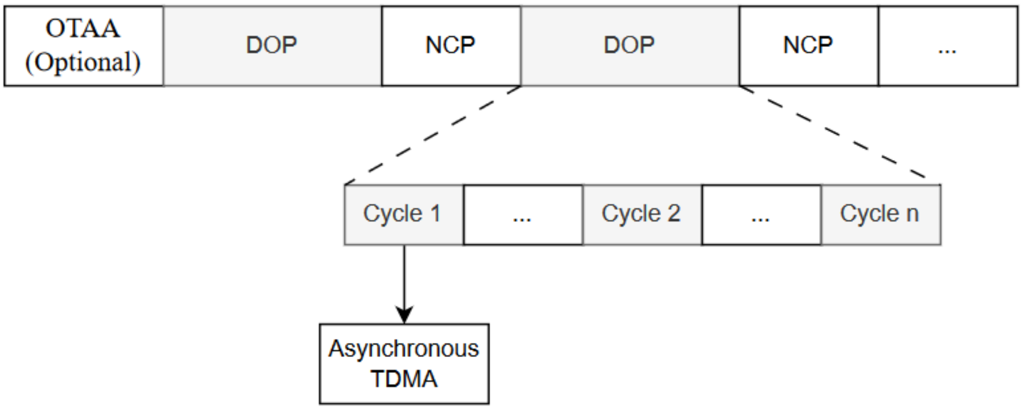


Figure 3.2 – Ad Hoc Lora protocol structure.

This protocol is characterized by its integration with the LoRaWAN network. It's therefore essential to identify nodes that do not have the ability to join the LoRaWAN network or that have a deficient operation with the GW. The moments of joining the network and the DOP play the essential role in the pursuit and achievement of these established objectives. Checking for a node's connection instability to the LoRaWAN network results in different interpretations of the structure presented in Figure 3.2. In situations where a device does not have the ability to properly connect to the LoRaWAN network, it should switch to Slave mode. In this mode, the DOP phase, which uses asynchronous TDMA, and NCP, the device acts passively, waiting for instructions coming from a node that plays the role of Master. This means that the slave is no longer involved in the active communications of the LoRaWAN network and relies on the Master node to coordinate its operations and receive the necessary instructions. The Master node, in turn, is responsible for managing all these phases of the protocol, having all the necessary conditions and resources to operate fully and efficiently in the LoRaWAN network. All of this is possible by taking advantage of the ability of the LoRa technology to switch from LoRaWAN mode to P2P mode, enabling the execution of the various methods of the protocol. Thus, the Master node plays a central role in the two-hop tree architecture illustrated in Figure 3.1, ensuring control and coordination of the operation of the Ad Hoc LoRa protocol thus enabling the complete integration of all nodes with the LoRaWAN network.

3.2.2. Physical Layer and Frame Format

The LoRaWAN network and the Ad Hoc protocol use the same radio physical layer technology, they present however, different transmission mechanisms, as described in Table 3.1. In the Ad Hoc protocol, the LoRa device, operating in P2P mode, uses a fixed SF and a fixed transmission power, with the aim of simplifying the implementation and operation of the system. Increasing the number of symbols in the preamble of the LoRa plot, indicated in Table 2.1, plays a relevant role in the performance of the NCP, as will be detailed in chapter 3.2.4.1. On the other hand, LoRaWAN network devices can use the ADR mechanism. By activating it, the LoRaWAN network server can optimize the node's data transmission rate by adjusting the SF and transmission power, which results in better network performance.

Table 3.1 – LoRa physical layer parameters for the LoRaWAN and Ad Hoc LoRa network.

Parameter	LoRaWAN (EU863-870)	LoRa Ad Hoc
SF	7 - 12	7-12
Transmission Power	Variable	14 dBm
BW	125 kHz	125 kHz
Preamble (symbols)	8	Variable
CR	4/5	4/5

In terms of the LoRa packet format, both a device operating in the LoRaWAN network and Ad Hoc protocol packets use the format defined by Semtech. However, they differ in payload organization, as shown in Figure 3.3. In the context of LoRaWAN [5], the packet includes a one-byte MAC header field (MHDR) at the start position, which contains relevant information such as the message type and the LoRaWAN protocol version. The frame header field (FHDR) is used in both UL packets and DL packets and contains the address of the receiving/sending device, playing a fundamental role in routing and controlling communication between the device and the LoRaWAN network. In turn, the port field (FPort) is used to specify one of the 223 available ports, allowing the type or purpose of the data transmitted by the devices to be identified. The application payload is inserted into the MAC frame payload encryption field (FRMPayload). Moreover, the maximum number of bytes in the payload is 51, as explained in chapter 3.2.4.1. Data integrity in LoRaWAN is checked through a message integrity check using the MIC (Message Integrity Check) field.

Regarding the developed Ad Hoc protocol, the payload format is simpler. It presents a nineteen-byte header that includes information such as the identification of the sender and receiver, the type of packet (for example, data or network formation commands) and the length of the payload frame. Depending on the type of packet, the payload contains a variable or fixed number of bytes of data.

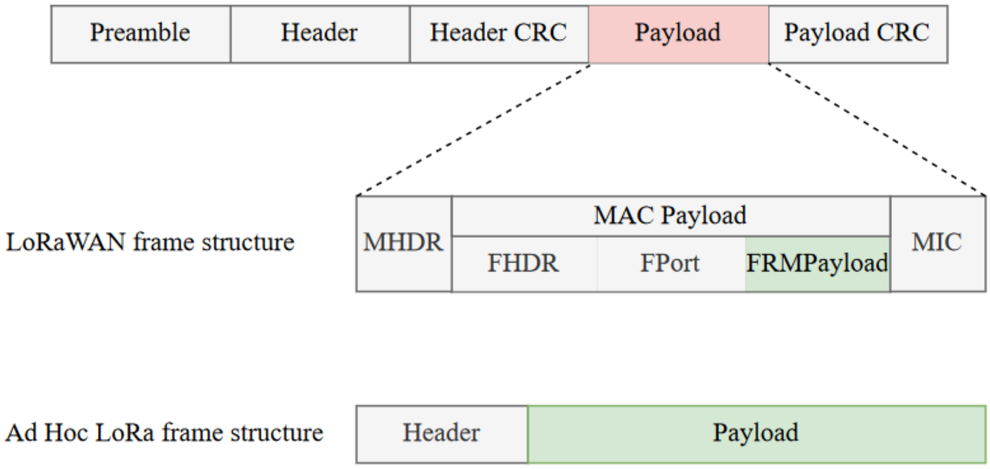


Figure 3.3 – Comparison between the format of the LoRaWAN network and the Ad Hoc protocol.

3.2.3. LoRaWAN Integration

The Ad Hoc protocol has been proposed to be integrated with LoRaWAN technology. This protocol focuses on improving areas of unstable connection and shadowing within the LoRaWAN infrastructure. This makes it possible for devices with specific limitations to participate in the LoRaWAN network in a controlled manner and adapted to their capabilities. Therefore, the network joining process and instability check, which are incorporated into the DOP phase as well as the joining stage, align with the overall objective of effective integration with the LoRaWAN network.

3.2.3.1. Period for Joining the LoRaWAN Network

The Ad Hoc protocol was developed with the aim of transparently integrating with the LoRaWAN network, with the adhesion phase being fundamental for this integration. However, this initialization moment is only relevant in the case of the OTAA method, which marks the beginning of the use of LoRaWAN functionalities. This includes MAC commands, data transmission to cloud platforms and data reception through UL and DL commands. If the user chooses the ABP activation method for their application, the protocol continues to be viable, but this initialization period is not part of the protocol operating architecture. Consequently, instability checking algorithms will not be applied during this phase, as will be detailed in the next chapter.

OTAA mode requires the join process to be carried out and this is a more complex and important aspect because it is the only time that a device needs to receive information from the network. The join process is also critical because the timing of the reception windows allows only two opportunities to receive an acknowledgment of input (join ACK) after the device transmits the join request. Considering the complexity of this network entry process, the importance of this timing is magnified if many devices try to connect to the network in a short period of time. Therefore, a strategy was developed that allows end devices to gain access to the LoRaWAN network with the fewest possible number of attempts, also resulting in positive implications for the energy consumption of these devices.

The strategy adopted in this protocol is based on the use of back-off transmissions, in which a suggested schedule [77] of 15 seconds, 30 seconds, one minute, five minutes, 30 minutes and 60 minutes was implemented (repeating after 60 minutes). This progressive back-off schedule follows a sequence of progressively longer wait times after each transmission failure. Initially, the back-off is 15 seconds. If the transmission is unsuccessful, the device waits a random amount of time between 15 seconds and the next maximum back-off interval (30 seconds) before attempting to retransmit again. The process continues with back-off intervals of one minute, five minutes, 30 minutes, and 60 minutes, repeating after 60 minutes. With each retransmission attempt, random waiting allows the device to choose a time within the maximum back-off interval, which avoids collisions between devices. This introduction of randomness into the retransmission waiting time ensures that devices do not retransmit at the same time after back-off, significantly reducing the chances of collisions and increasing the robustness of the communication.

Therefore, this back-off approach helps to avoid collisions and congestion during a process that is complex and bandwidth-heavy, such as the join procedure. By allowing devices to choose random retransmission times, the strategy improves communication efficiency and reduces transmission overlap, which is essential in the objective of the proposed Ad Hoc protocol, i.e., in identifying areas where LoRaWAN coverage is weak or inconsistent.

3.2.3.2.Stability check

The development of a protocol integrated with LoRaWAN may be a response to improve network connectivity in environments where shadow zones and unstable connections occur. Within this context, it is essential that devices that integrate this protocol can verify whether they have an unstable connection environment. In this case, this responsibility falls on the nodes that operate in standard mode, that is, the Masters, since they are the elements that are in direct contact with the LoRaWAN network. To meet this requirement, two moments play a fundamental role in evaluating the quality indicators of the connection to the LoRaWAN network: the network joining phase and the DOP.

The LoRaWAN network joining phase, especially when the OTAA activation mode is selected, plays an important role in taking advantage of the LoRaWAN architecture, enabling network integration. As a result, failure at this stage may compromise the achievement of this objective. Furthermore, the failure of the join procedure indicates that the device is in an unstable communication zone. Based on this understanding, a limit was established for the number of attempts for the join procedure. When this limit is exceeded, the device transitions from Master to Slave. In this mode, the node stops making new joins and assumes a passive stance in relation to a potential Master accessible on the network, according to the algorithm illustrated in Figure 3.4.

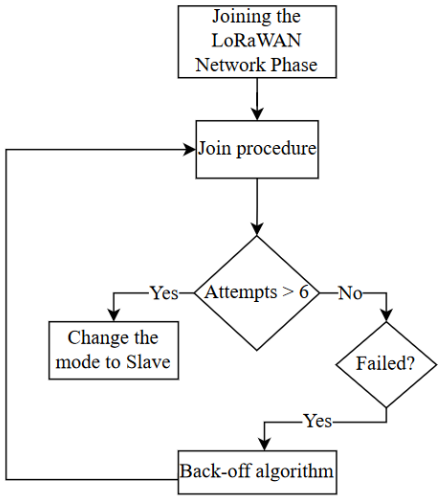


Figure 3.4 – Verification of stability during the adhesion phase of the LoraWAN network.

The other moment of stability verification is the DOP phase, where the Masters, regardless of whether they incorporate Slaves or not, carry out periodic data transmissions on the LoRaWAN UL channel. At this stage, stability analysis is improved using the MAC Link Check Request (LCR)a command, which is sent together with UL data transmission, playing a fundamental role in evaluating connection conditions. The LCR command is a feature of the LoRaWAN protocol, designed to provide information about the quality of the link between the device and the GW in the network. By sending an LCR command, the device requests the GW to perform a communication link quality check. The base station immediately responds to the device with a MAC Link Check Ans (LCA) command, which includes two parameters: The Demodulation Margin, representing the signal margin in dB of the most recent LCR command, indicating the quality level of the received signal. A value of zero indicates that the frame was received at the minimum demodulation threshold (0 dB or no margin), while a higher value, such as 20, indicates that the frame was received with a 20 dB margin above this threshold. On the other hand, the Gateway Count parameter reports the number of GWs that received the most recent LCR command. This provides information about network coverage and GW redundancy in the area where the device is located. The higher the GW count value, the greater the robustness and availability of the network in the region. At the current stage of protocol development, not all this information is used to assess the stability of the LoRaWAN network. Instead, the method used is based on the LCA command reception count, allowing the calculation of the ratio between the number of LCA messages received and the number expected in response. Based on this ratio, the device can assess possible instability in the region of the LoRaWAN network in which it is located. If the evaluation is negative, the node changes the mode to Slave, as illustrated by the algorithm in Figure 3.5. It is worth highlighting that the ratio calculation only starts after the transmission of 50 UL messages, to allow the device to accumulate enough data to make a reliable assessment.

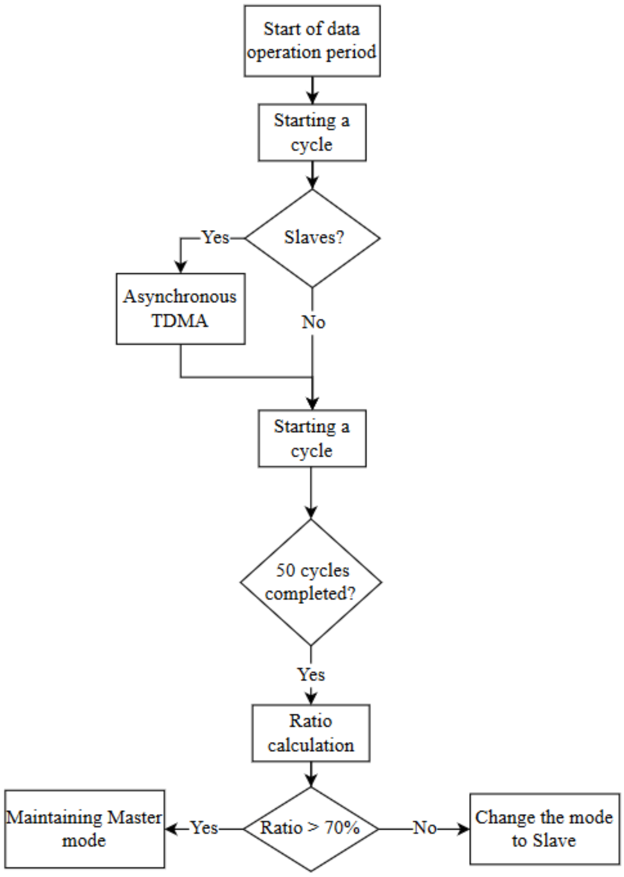


Figure 3.5 – Stability check during the DOP phase.

It is important to note that frequently performing LCR has the disadvantage of requiring a little more of the LoRaWAN network resources, which can result in network overload and a reduction in its capacity for message transmission, in addition to having negative implications on efficiency. energy of the system.

3.2.4. Network Construction Period

As mentioned in chapter 3.2.1, the role played during this NCP varies according to the node's operating mode. Devices with stable LoRaWAN connectivity act as Masters, coordinating this phase of the protocol, while devices in Slave mode respond to instructions coming from the Master node.

The NCP activation moment is initiated by the Master by transmitting the INIT command, marking the beginning of the network construction process. The INIT is a broadcast message (as illustrated in Figure 3.6), sent to all devices in Slave mode, and serves as the starting point for joining the two-hop tree, allowing Slaves to connect to a Master. Thus, when Slaves receive the INIT command, this triggers the transmission of a JOIN message, indicating that the node in Slave mode has the appropriate conditions to be part of its subnet. However, there are two scenarios in which the Slave does not respond to the Master's INIT: first, when it is already associated with another tree, where the Master of that tree offers better connection conditions, based on the SNR metric of the INIT message; and second, when it has already received an ACK_JOIN message from the current Master. This last message has the purpose of informing the Slave that the Master has received his membership request. As a result, the Slave does not need to respond to any more INITs during this NCP period, which reduces message traffic and avoids unnecessary energy expenditure. After the Master sends the ACK_JOIN, it resends a new INIT message, allowing other nodes in Slave mode to enter the tree. The first phase of the NCP is completed when the Master sends three consecutive INITs without receiving JOIN responses, which indicates that there are no more nodes within the Master's reach to join its subnet. Figure 3.6 presents a brief sequence of the described process, showing the basic operation and types of communication of the commands used in the first phase of the NCP.

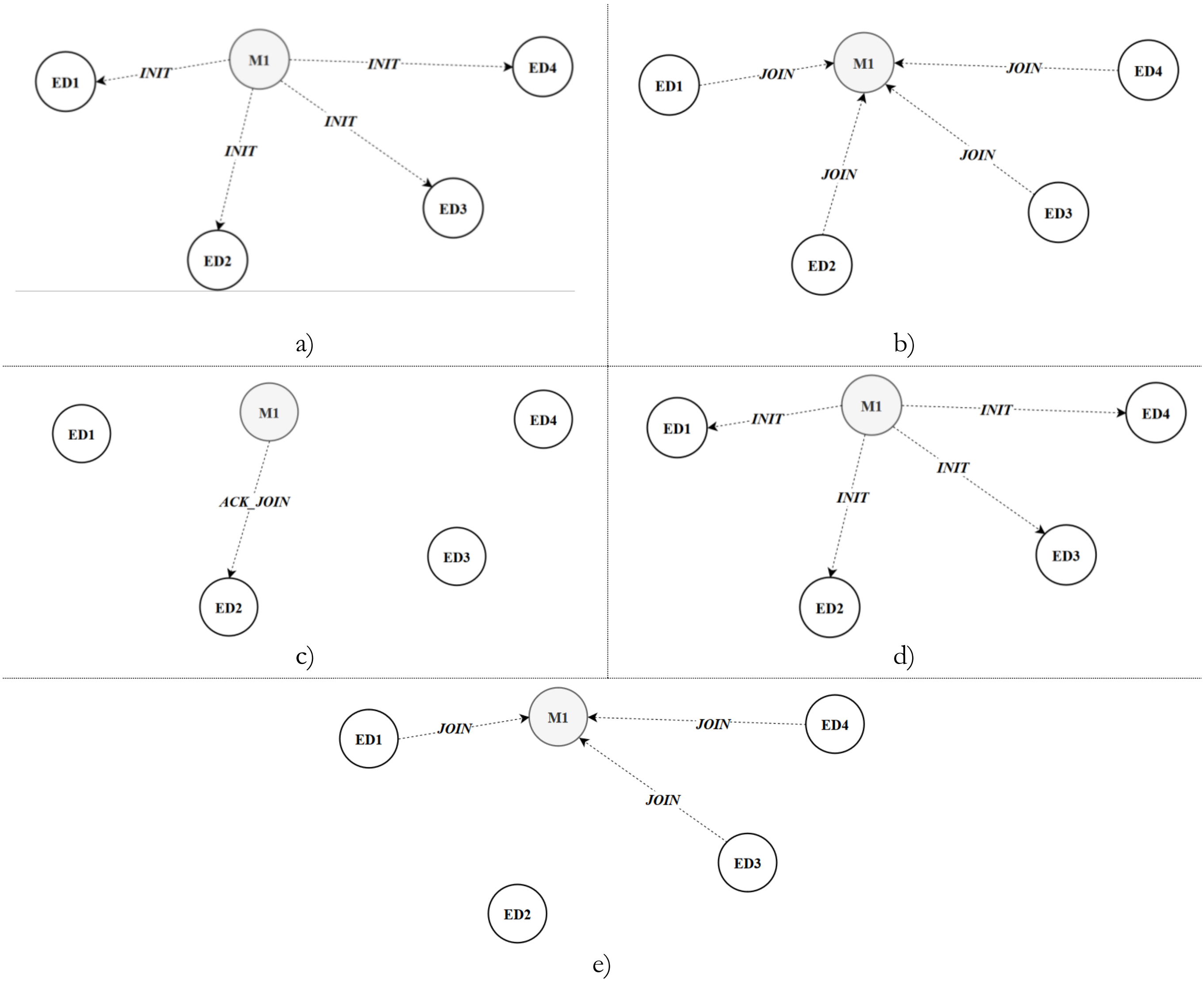


Figure 3.6 – Sequence of the first phase of the NCP. Points a) and d) represent the broadcast communication of the INIT command; points b) and e) the sending of the JOIN message type; and point c) the unicast transmission of the ACK_JOIN message.

In the next phase of the NCP, the Master organizes a list of Slaves that have requested to join its subnet, based on the SNR metric. It is important to mention that the Master has a limited capacity to accommodate Slaves in its subnet, and therefore carefully selects a few of the best nodes to be included in the tree. Once the devices have been selected, the Master sends individual CON messages to each Slave, informing them about the time slot to be occupied during the DOP phase. After sending the CON message, the receiving Slave responds with an ACK_CON to confirm receipt of the message and, consequently, the allocation of the timeslot. If the ACK_CON is not received, the Master makes up to three consecutive attempts to send the CON message to the same Slave. If after this number of attempts there is no response, the Master moves on to the next Slave on the list.

This NCP step is essential to ensure that the allocated Slaves receive the necessary instructions for transmitting and receiving data during the DOP. Furthermore, the careful selection of Slaves based on the SNR metric makes it possible to optimize the performance and efficiency of communication in the subnet. In illustrative terms, Figure 3.7 matches the described process.

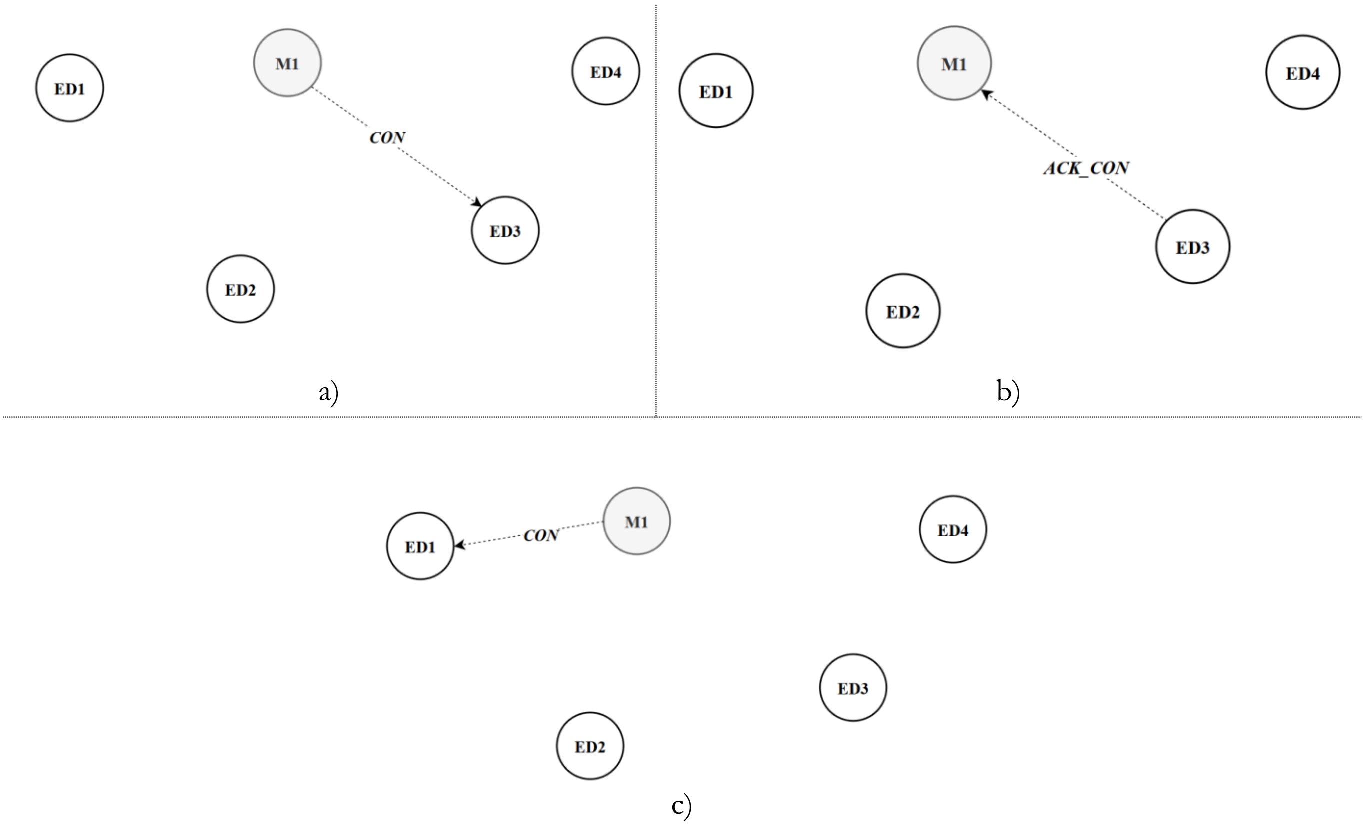


Figure 3.7 – Sequence of the second phase of the NCP. Points a) and c) indicate the sending of CON messages to the Slaves on the list; and point b) the sending of the ACK_CON command.

Considering the functionality that selects Slaves based on the SNR metric, it is important to consider the hypothesis that the Masters who established the network in the first place may lose their Slaves. This occurs when these Slaves choose to associate with another Master once they notice an improvement in connection conditions. The protocol corrects this, executing the following NCP phase, where the first Masters who carried out the construction can reach other Slaves.

3.2.4.1. Limitation on the number of slaves

The proposed protocol is developed to work in conjunction with LoRaWAN technology and as mentioned in chapter 3.2.2, the devices take advantage of the ADR mechanism. This allows LoRaWAN communication to dynamically operate at the lowest possible data rate, known as DR0 [77], which uses an SF12 and a bandwidth of 125kHz. This situation leads to the worst case in terms of data length in the payload field, limiting the number of data bytes to 51. As will be discussed in chapter 3.2.5, during the DOP phase, a Master combines the data received from all Slaves in a single LoRaWAN package. Therefore, it is essential that the number of Slaves supported by the Master does not exceed the maximum payload allowed by LoRaWAN. Figure 3.8 illustrates the relationship between the number of Slaves and the payload size per Slave.

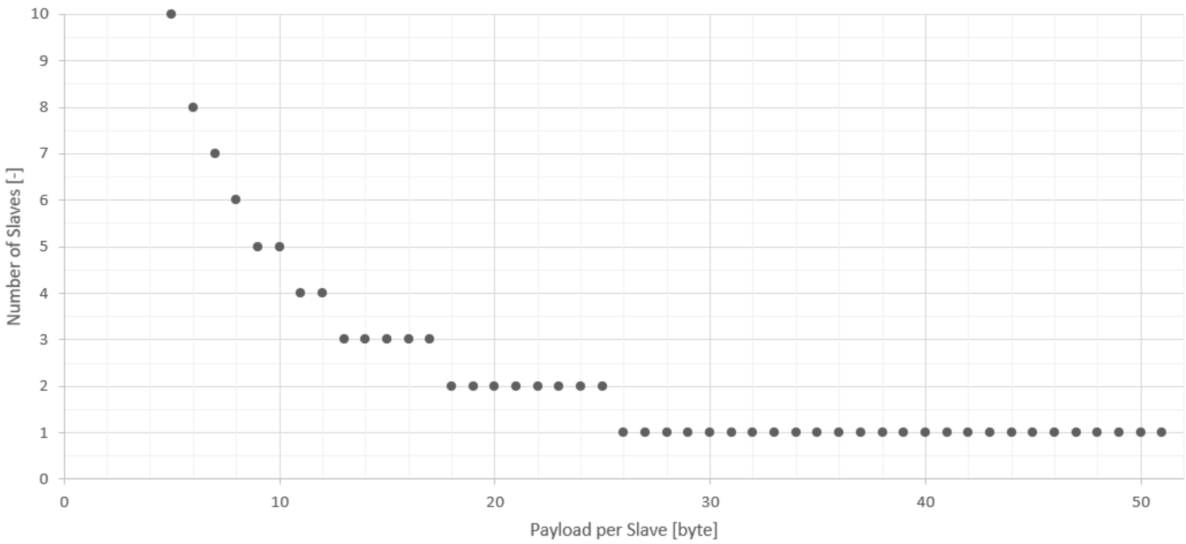


Figure 3.8 – Relationship between the number of Slaves and the corresponding possible payload size.

In Figure 3.8 it is possible to analyse that the increase in the number of Slaves results in a decrease in the maximum length of the payload that can be sent. On the other hand, if there is a need to transmit a greater amount of data, this implies a reduction in the number of two-hop nodes that can be accommodated in the Master. Therefore, there needs to be a balance between the number of Slaves that can be supported and the amount of data they can transmit. It is important to note that, in the same LoRaWAN package that accommodates data from all nodes in the tree, it is also necessary to include data from the Master itself. To achieve a balance, based on the graph in Figure 3.8, the Masters' data is as important as the Slaves', since both have the same importance in terms of data transmission. Taking all these considerations into account, a maximum limit of two Slaves that the Master can accommodate was established. This implies that each node in the network is restricted to transmitting a maximum of 25 bytes.

3.2.4.2. Mechanism in Packet Collision Moments

During the network construction process, it is possible for simultaneous transmissions from several nodes to occur, especially when Slave nodes request to join the tree, as illustrated in Figure 3.6 b. In this case, simultaneous transmissions can occur because multiple nodes are sending JOIN messages to the Master at the same time. This situation can result in data collisions, causing lost requests and the need for retransmissions. These collisions impact the efficiency of the NCP, as the affected nodes need to wait for a new suitable moment to carry out their transmissions, that is, wait for a new INIT to be sent from their Master. However, the scenario may occur where the JOIN transmission is repeatedly lost, resulting in the inability of Slave nodes to connect to the network during the construction process, since sending INIT is limited to three attempts at each time of the NCP. All of this can compromise the adequate formation of the network, resulting in delays in the joining of new nodes and, consequently, reducing the efficiency of the protocol.

To overcome the problem of simultaneous transmissions, it was essential that the protocol presented strategies for controlling access to the medium. To achieve this goal, a CAD-based packet collision avoidance mechanism was developed. This CAD functionality is present in the latest LoRa transmitters and is designed to detect the LoRa frame preamble of other devices on a given radio frequency channel [47]. However, some studies have also revealed CAD's ability to detect payload chirps with satisfactory performance, as mentioned in chapter 2.3.2.2. This way, it can check whether the channel is free or busy before starting to transmit a message, avoiding collisions between packets transmitted by different devices on the same network.

To take advantage of the use of CAD, random delays were introduced, where each device can choose a transmission moment (w) within a random range but restricted to the temporal length of the preamble. This range corresponds to the preamble time of a message with minimum w ($w = 0$), as illustrated in Figure 3.9. This limitation was established because CAD was designed to effectively detect only this time interval. During this random interval, the devices wait for a waiting period r proportional to the T_{CAD} channel activity detection time and the randomly chosen transmission moment w. This random waiting time r is computed as follows:

$$\mathrm{r} = \mathrm{w} \times T_{CAD} \tag{3.1}$$

where T_{CAD} represents the CAD activity time and w is a random number chosen within a restricted time length of the preamble.

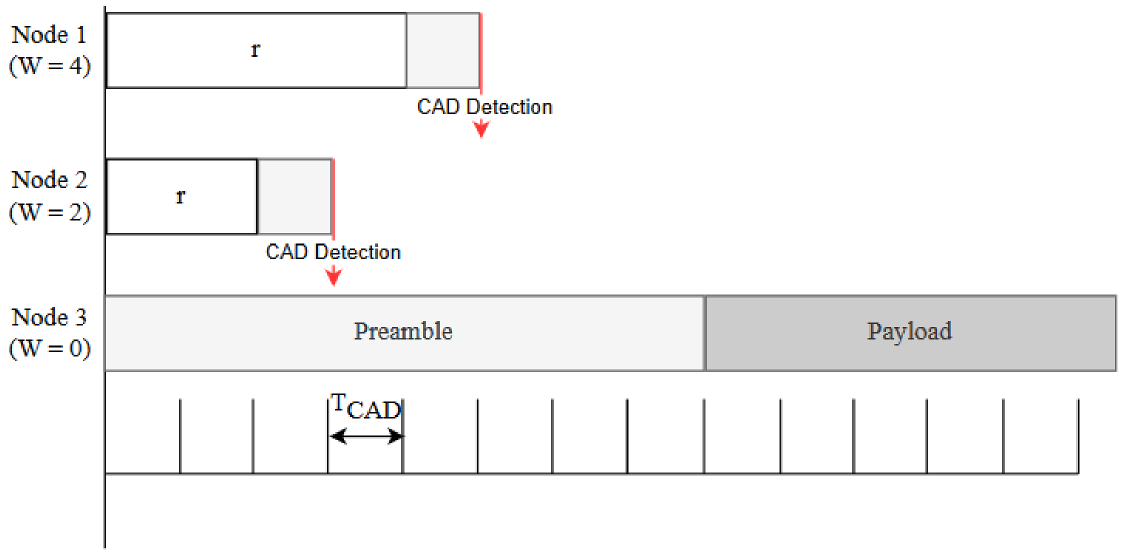


Figure 3.9 – Mechanism for simultaneous messages.

Figure 3.9 illustrates the random choice of transmission by three nodes, respecting the random range corresponding to the message preamble time with $w = 0$. It is possible to observe that the nodes that started transmitting the message later compared to node 3 ended up cancelling their transmissions due to the CAD functionality.

T_{CAD} was chosen as a reference due to the risk of message collisions that could occur with shorter time intervals. If devices started their transmissions earlier than the time required for the CAD to detect channel activity, the probability of collisions would increase. It should be noted that the time required for CAD detection may vary according to the LoRa modulation configurations used in [47]. The graph below, illustrates the observed typical CAD detection time, expressed as a multiple of the LoRa symbol, for a given SF configuration.

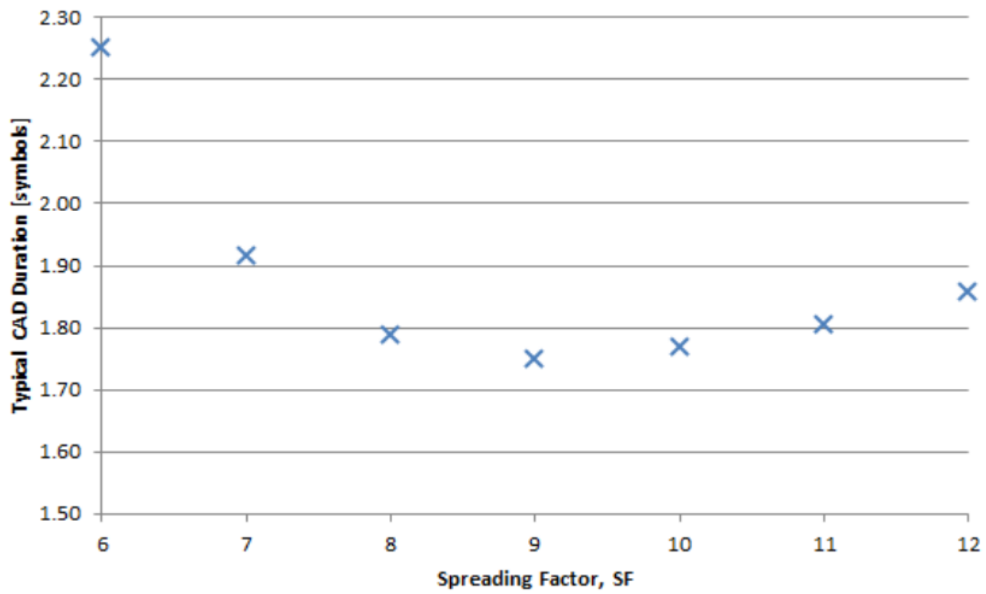


Figure 3.10 – T_{CAD} as a function of SF [47].

Based on the analysis of the graphs presented in the previous figure, it was established that the value of T_{CAD} would be equal to twice the time per symbol, T_{sym}:

$$T_{CAD} = 2 \times T_{sym} \tag{3.2}$$

Considering equations (2.1) and (2.4), the maximum number of moments (n_{CAD}) that the random band ($T_{preamble}$) can accommodate is presented as follows:

$$n_{CAD} = \frac{T_{preâmbulo}}{T_{CAD}} = \frac{(n_{preamble} + 4.25) * T_{sym}}{2 \times T_{sym}} = \frac{n_{preamble} + 4.25}{2} \tag{3.3}$$

This ratio represents the maximum number by which w can vary. The n_{CAD} value is designed depending on the specific application of this protocol. If many slaves are observed on the network, it may be necessary to increase the value of n_{CAD} to void an excess of simultaneous transmissions, which could compromise the time for new nodes to join. Therefore, adjusting the number of symbols in the preamble ($n_{preamble}$) is essential to achieve the appropriate value of n_{CAD}, allowing this developed mechanism to guarantee efficient construction of the tree and reduced risk of collisions and delays in the network formation process.

3.2.5. Data Operation Period

The DOP represents a specific time interval within the protocol structure (Figure 3.2) in which network nodes can perform data transmission efficiently and reliably. This phase covers both UL and DL transmissions. Furthermore, when nodes incorporate the proposed network architecture, the asynchronous TDMA process is used. Otherwise, the devices simply transmit their data from a UL LoRaWAN channel. This medium access operation ensures the organization and efficiency of transmissions from nodes in the network, occurring cyclically.

The implementation of asynchronous TDMA in DOP is based on dividing time into fixed intervals called timeslots, where each device has a designated time window to transmit or receive data. However, unlike traditional synchronous TDMA, devices are not synchronized in a specific time loop. Instead, asynchronous TDMA uses a wake-up mechanism, in which devices wait for a beacon to begin their data transmissions. In this dynamic, the Master's role is to coordinate access to the communication channel, sending the beacon to the Slave nodes. The Slave devices, in turn, receive the activation signal from the Master and transmit the data according to the timeslot previously sent in the NCP phase. During this TDMA phase, the Master collects data from the Slave devices, which are later sent, together with the Master's own data, to an online server through the UL LoRaWAN channel. Figure 3.11 illustrates the structure of the data message used by Slave devices in response to the beacon. Furthermore, the illustration addresses the possibility that the activation signal sent by the Master contains DL information previously stored for its Slaves. This approach allows the Master to simultaneously send data destined for Slaves (whether unicast or broadcast addresses) together with the beacon, resulting in an optimization of communications efficiency during the DOP.

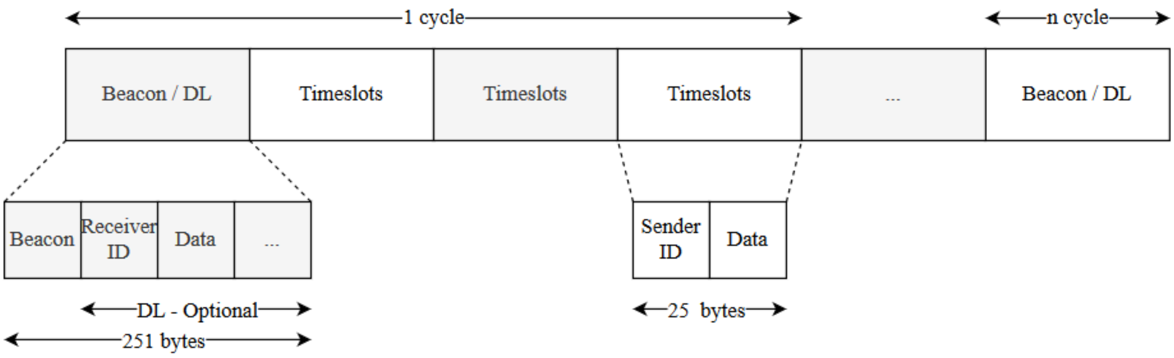


Figure 3.11 – Structure of the activation signal and DL and data messages for UL.

Figure 3.12 exemplifies the operation of asynchronous TDMA using the P2P LoRa radio. In this scenario, the Master broadcasts an activation beacon with a network broadcast address to activate all its Slaves. After sending the beacon, the master opens a reception window in which it accepts all data received from the Slaves through its P2P LoRa modem. Finally, the Master organizes all the data and forwards it to a LoRaWAN GW.

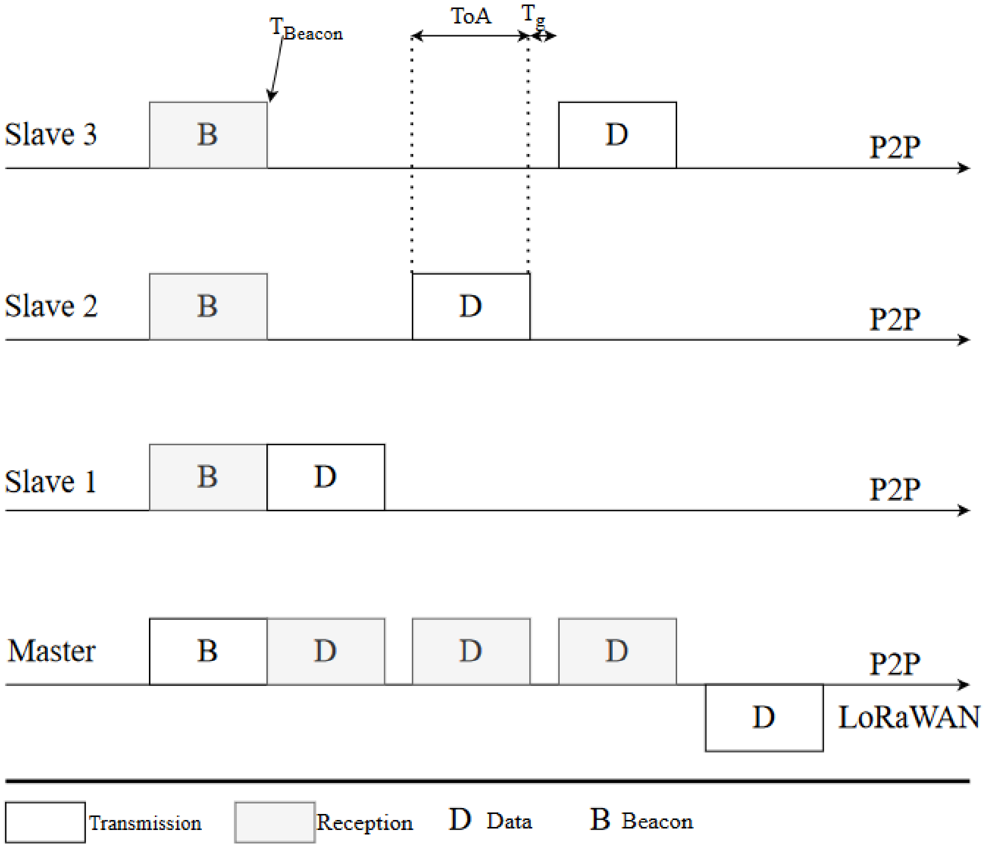


Figure 3.12 – Overview of the asynchronous TDMA process.

3.2.5.1. Slot allocation

The use of an activation signal, treated as a *beacon*, allows all slaves of a given Master to be relatively synchronized with each other. Based on this principle, each Slave occupies *slots* according to the number previously assigned in the NCP phase (N_{slot}). The moment a Slave is activated by the Master is captured as T_{beacon} Using this information, each node calculates the start of its own time slot as follows:

$$T_{NextSlot} = T_{beacon} + (\mathrm{ToA}_{Max} + T_g) \times N_{slot} \tag{3.4}$$

Equation (3.4) describes how Slaves should start transmitting data packets. The expression $\mathrm{ToA}_{Max} + T_g$ represents the slot size, as shown in Figure 3.12. This length of time accounts for the maximum time in air, ToA_{Max}, calculated based on equations (2.3) a (2.7), or from the simulator provided by Semtech[78], and includes a pre-defined guard interval, T_g, of 50ms. The ToA_{Max}time is the largest possible LoRa packet, considering the largest number of payload bytes defined, considering Figure 4.8, and the characteristics of the physical layer for the Ad Hoc protocol (Table 3.1). As far as T_g is concerned, it ensures that the time window is wide enough for transmission and to compensate for any clock synchronization discrepancies.

3.3. FINAL REMARKS

In this chapter, the protocol and its communication mechanisms that qualify it as Ad Hoc were presented. The design of the protocol had as its main objective to mitigate the so-called shadow zones, providing devices with insufficient or null communication in the LoRaWAN network with the ability to adhere to a network architecture called a two-hop tree, autonomously. This approach enables these nodes, indirectly, to connect to the LoRaWAN network, taking advantage of the reliability of the asynchronous TDMA method.

4. IMPLEMENTATION AND RESULTS

In this chapter, the analysis and evaluation of the protocol developed in the previous section will be carried out, at the level of communication reliability. Chapter 4.1 shows the characteristics of the hardware used to interpret the Ad Hoc LoRa protocol and its ability to integrate throughout the entire LoRaWAN stack. In chapter 4.2, a set of tests is carried out with the devices designed in chapter 4.1, operating exclusively in the LoRaWAN network, in order to explore and understand their limitations. On the other hand, chapter 4.3 presents the results of the devices operating with the Ad Hoc LoRa protocol. These results allow an evaluation of its reliability compared to the data obtained in the tests in which the developed protocol was disabled. In chapter 4.4**Erro! A origem da referência não foi encontrada.**, a f inal summary of the results obtained is presented.

4.1. HARDWARE AND SYSTEM ARCHITECTURE

Interpreting all the features of the Ad Hoc LoRa protocol and evaluating its performance required specific hardware support. Regarding the implementation of the LoRaWAN architecture, this need was achieved with a GW called The Things Outdoor Gateway (TTOG) with the WAPS-232N model, as shown in Figure 4.1. This GW provided by Browan Communications supports the various network servers and has the following technical specifications:

Table 4.1 – GW TTOG WAPS-232N technical specifications.

Parameter	Description
RF transmission power	0,5 Watts (up to 27 dBm)
Reception sensitivity	Up to -142 dBm
RF transmitter	SX1301 with SX1257
LoRaWAN compatibility	Version 1.0.3
Number of channels	16

Figure 4.1 – Gateway LoRaWAN TTOG WAPS-232N.

Protocol implementation and the various carried out experiments, a simple prototype was developed based on a Texas Instruments microcontroller, the MSP430FR6047. This microcontroller is part of the MSP430 family, known for its compact size, low power consumption and low-level programming. Although the MSP430 family has some limitations, such as limited internal memory capacity, the MSP430FR6047 proved to be a suitable choice for executing the developed protocol and for the remaining software (SW) related to the Universal asynchronous receiver/transmitter (UART) communication interface, as shown in the following technical details in Table 4.2:

Table 4.2 – MSP430FR6047 technical specifications.

Parameter	Description
Power supply voltage	2.2 V – 3.6 V
Frequency	16 MHz
FRAM	256 kByte
RAM	8 kByte
Bootloader (BSL)	UART

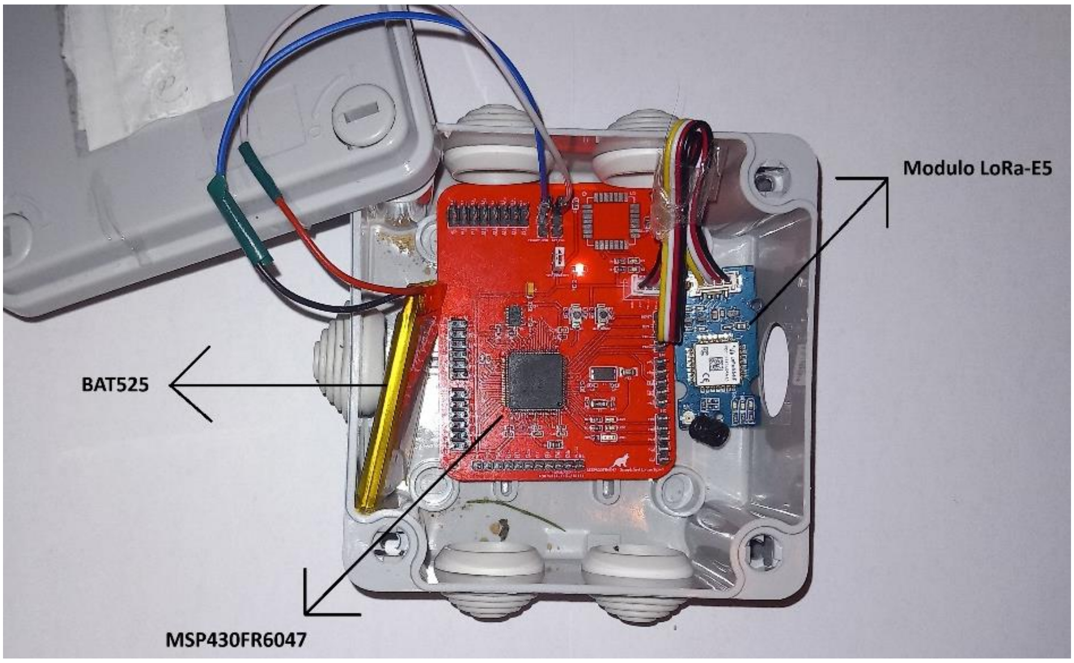


Figure 4.2 – Prototype developed for the experimental implementations.

The MSP430FR6047 microcontroller is embedded on a printed circuit board (PCB) (Figure 4.2) that essentially contains four LEDs, buttons, input/output (I/O) pins and pins to software emulation and debugging through the development tool and Integrated Drive Electronics (IDE) programming Code Composer Studio (CCS). Furthermore, this PCB has a Grove connection compatible with the LoRa-E5 module. This Grove device is a LoRa radio module based on the STM32WLE5JC with an ARM Cortex M4 technology and an SX126X LoRa transmitter. The connection between the PCB and the module is established through the Grove connector, where communication is carried out through the UART, and control is carried out using AT commands. This modem can work with the LoRaWAN network, but it also can communicate directly with other device using P2P mode. This aspect is essential for the protocol to be able to integrate with the LoRaWAN network, given the constant need to switch between these modes of operation. To power the entire system, a chargeable lithium polymer battery (BAT525 NIMO) with a capacity of 1100 mAh and a voltage of 3.7 V was used.

This is an Ad Hoc protocol integrated into the LoRaWAN network. As such, the network developed by the protocol must be capable of incorporating with the LoRaWAN stack, as shown in Figure 4.3.

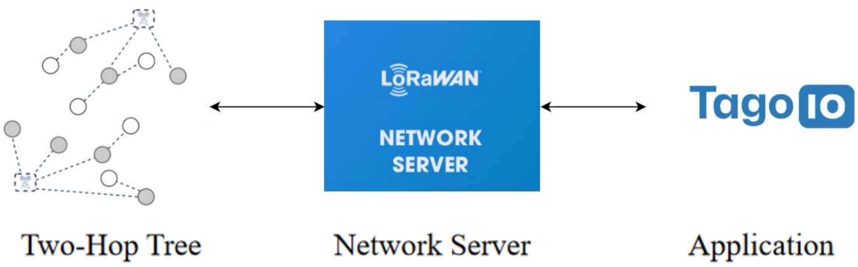


Figure 4.3 – Implementation of the network in the entire LoRaWAN stack.

It is important to note that all data collected by the GW was forwarded to a network server provided by The Things Network (TTN). TTN plays a fundamental role in the LoRaWAN network infrastructure, functioning as an intermediary element that connects devices to the internet and application servers. These application servers have several functions, including data storage, analysis, visual presentation of data, notifications, among others. The relationship between the TTN and the application servers was established through integration with TagoIO, which acts as an application server in the LoRaWAN stack. TagoIO offers storage, visualization, and integration services for LoRaWAN devices, as well as processing power by running scripts in node.js or python 3.x directly on TagoIO. With this configuration it is possible to observe and calculate several parameters with the aim of evaluating the performance of the protocol and the typical architecture of the LoRaWAN network.

4.2. TYPICAL LORAWAN ARCHITECTURE - ONE HOP

To understand and evaluate the capabilities and limitations of the LoRaWAN architecture, mainly in its physical layer, and subsequently for comparison purposes, a series of practical tests were conducted. In these tests, several nodes were placed in specific scenarios and operating conditions, which challenged the reliability of communications in both directions, i.e. UL and DL. Figure 4.4, Figure 4.5 and Figure 4.6 show, respectively, the geographic location of the installed nodes and the distance to the GW LoRaWAN, as well as the topographic view in which they are inserted.

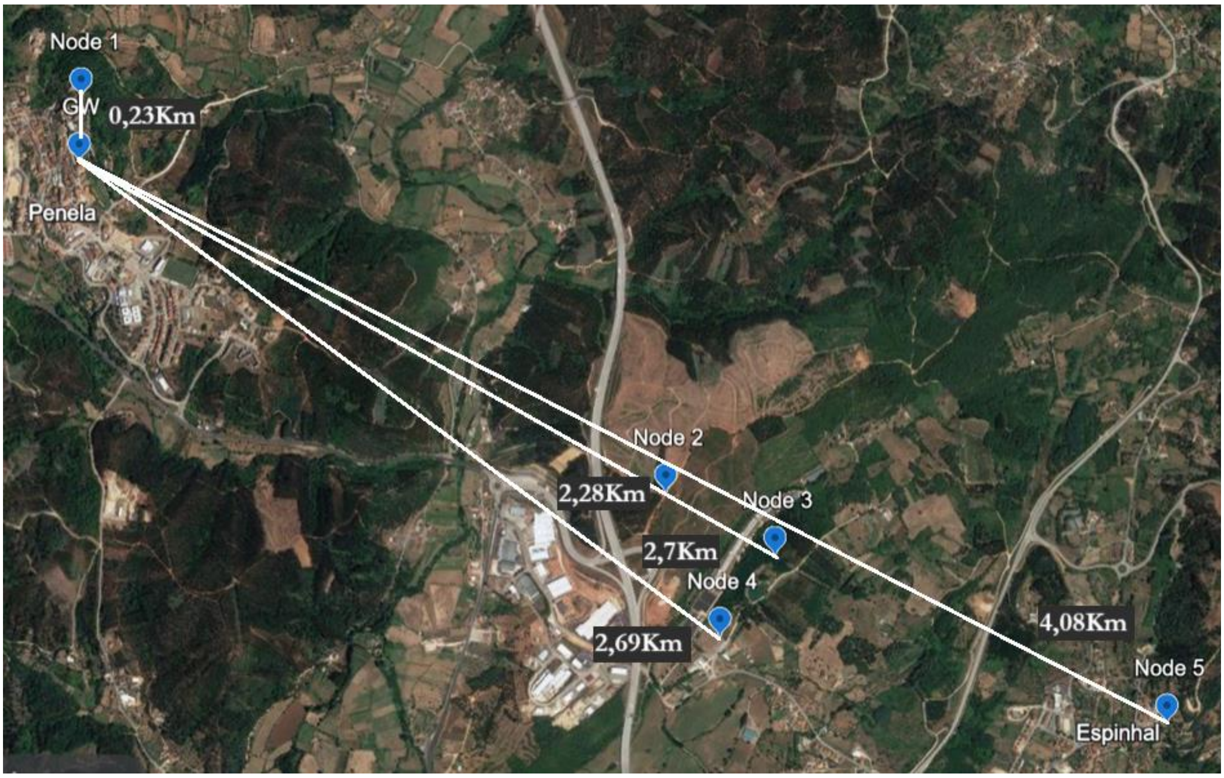
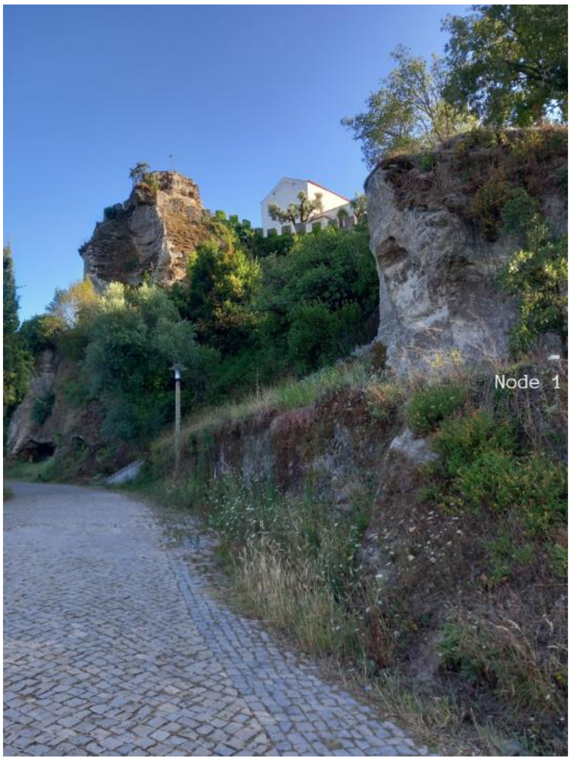


Figure 4.4 – Location of the end devices and the LoRaWAN GW.



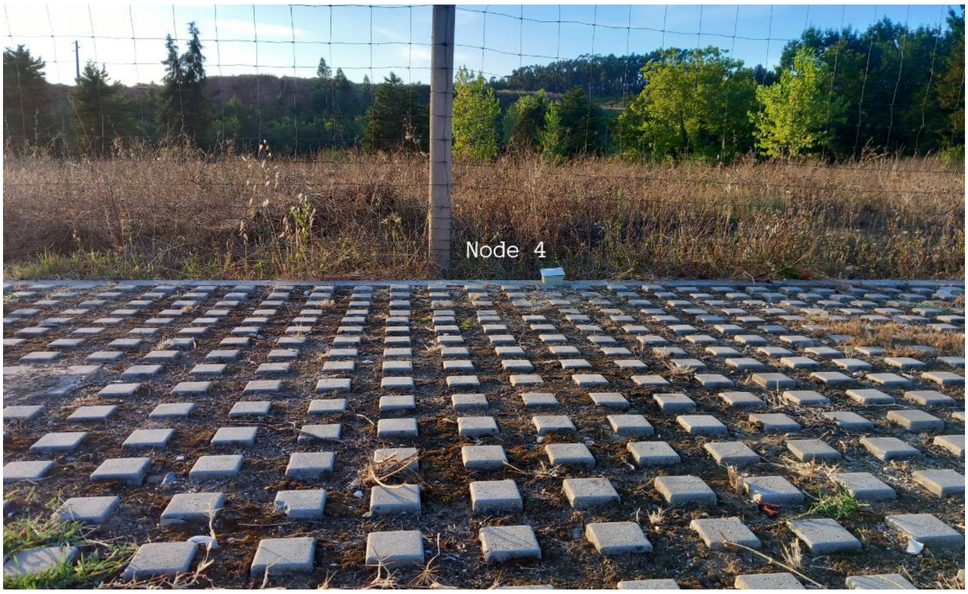
a)

b)

c)

d)

Figure 4.5 – Details of the scenarios and devices implemented in the experiment: a) end device 1; b) line of sight between the GW and device 2; c) end device 3; d) node 5 and its line of sight to the GW.



e)

Figure 4.6 – Node 4 scenario implemented in the experiment.

Each node was programmed to send UL with a 2-minute interval over 24 hours, accounting for a total of 720 transmitted messages. Moreover, the network end devices tested their performance in different SFs from 7 to 12. The content of each message consisted of a payload 10 bytes long, and the remaining physical layer parameters followed the indications in Table 3.1.

To evaluate the reliability of communications in the UL and DL directions, the percentage of packets received (PPR) metric was used. This metric is calculated as the proportion between the number of packets received by a device (#Received) and the number of packets that should have been received (#Expected) within a specific evaluation period, T, as evidenced by equation (4.1)

$$PPR = \frac{\sum_T (\#Received)}{\sum_T \#Expected} \times 100\% \qquad (4.2)$$

Within this context, the PPR is calculated separately for the UL and DL direction. The PPR in the DL direction is calculated by the microcontroller and represents the rate of successful responses to MAC LCR commands. On the other hand, the PPR in the UL direction is calculated with the help of the TagoIO platform, taking advantage of its processing capacity. This metric represents the proportion of UL messages successfully received by the GW. The use of TagoIO also allowed the collection of all previous metrics, as well as the SNR and RSSI indicators of the messages transmitted by the nodes shown in Figure 4.4. All these elements were recorded in relation to SF variations, as shown in Figure 4.7 to Figure 4.11.

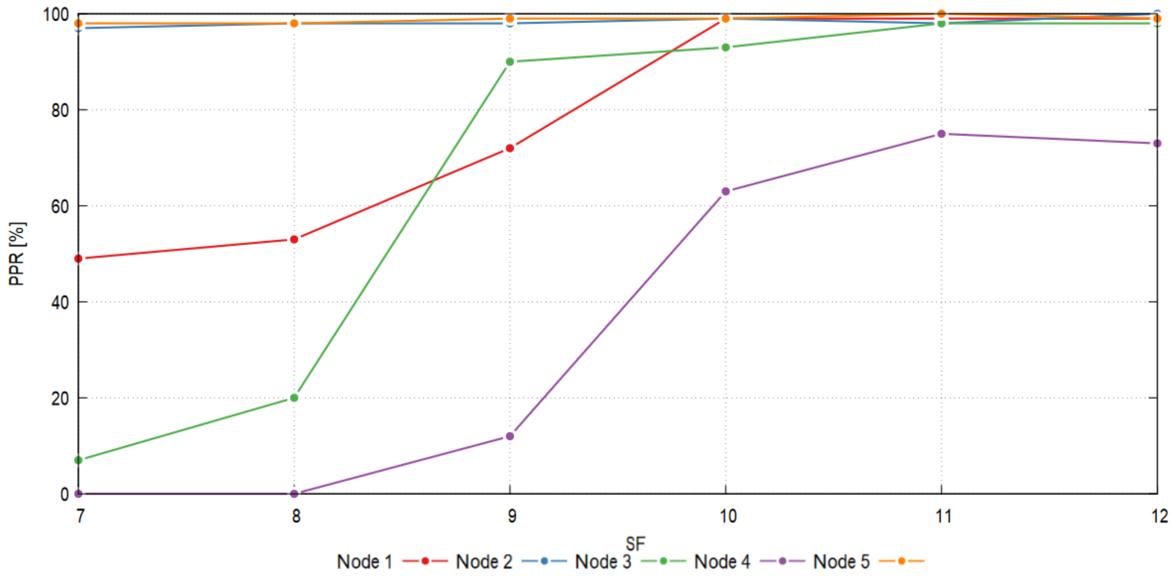


Figure 4.7 – PPR of the nodes' UL messages as a function of SF.

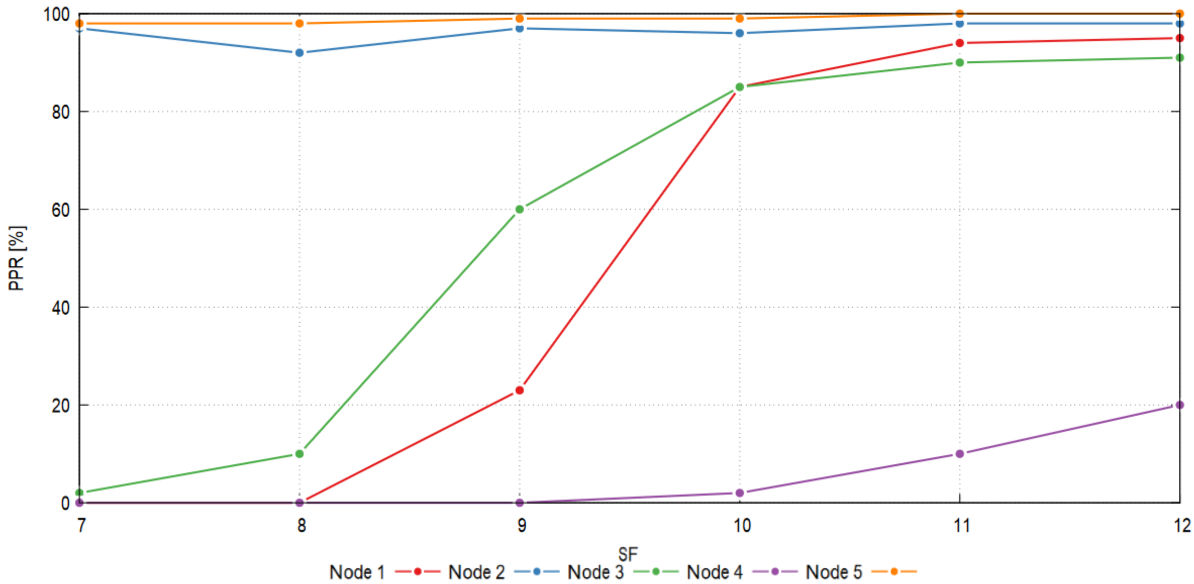


Figure 4.8 – PPR of DL messages on the various devices depending on the SF.

Cross-referencing the results obtained in Figure 4.7 and Figure 4.8 and the scenarios in Figure 4.6 allows some conclusions. One of them is the influence that relief, vegetation, or infrastructure had on connecting a node to the LoRaWAN network. For example, in Figure 4.9 b) and d), it is observed that nodes 2 and 5, which have line of sight to the LoRaWAN base station, achieved a PPR of around 100% throughout the applied SF. On the other hand, devices 1, 3 and 4 presented lower PPR in the lower SF due to obstacles, such as vegetation, relief, and infrastructure, such as the castle in the case of node 1 scenario. However, as the SF increased, PPR also followed the trend. These results confirm that higher SF transmissions provide better penetration capability, overcoming natural and artificial obstacles. It is worth noting that the PPR difference between devices 3 and 4, which are in the same area, differs due to the presence of more hills and denser vegetation in the radio path to the GW. Finally, the results in Figure 4.8 showed that success in receiving DL is more limited for devices located in areas of instability, as evidenced by the behaviour of nodes 1, 3 and 4. This observation indicates that the device, even if it presents good UL transmission indicators, may not have the ability to receive DL messages.

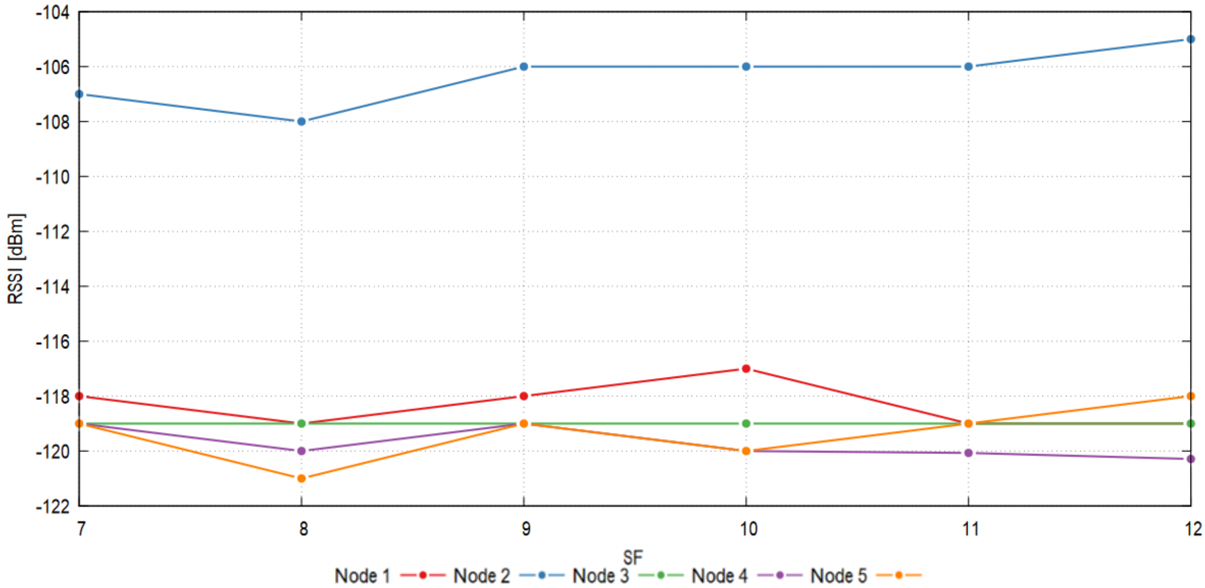


Figure 4.10 – RSSI of UL messages from the various nodes depending on the SF.

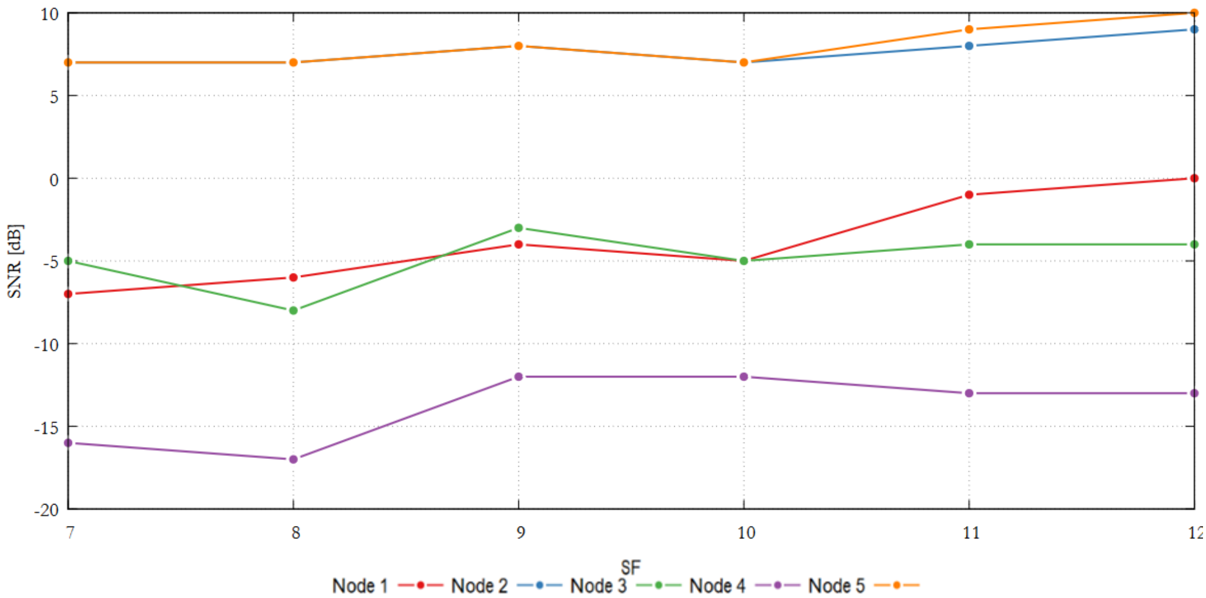


Figure 4.11 – RSSI of UL messages from the various nodes depending on the SF.

Regarding the RSSI and SNR results of UL transmissions, some conclusions were obtained, although they are not completely clear and definitive. In the case of RSSI, it can be observed that the values obtained were almost always higher than the sensitivity of the LoRa modem. As far as your analysis is concerned, device 2 showed the strongest signal compared to the others. This observation suggests that the signal may be blocked or attenuated by obstacles in devices with weaker signals. However, node 5, which has line of sight with the GW, presents RSSI values like those of devices that do not have this line of sight, justified by the greater distance between node 5 and the GW. Distance is, therefore, another factor that influences RSSI results. Regarding the SNR results, they indicate that devices without line of sight to the LoRaWAN base station present lower values compared to those that have this direct vision, as is the case with devices 1, 3 and 4. This suggests that devices with line of sight, can maintain a more favourable signal-to-noise ratio. However, with increasing SF values, both metrics did not sow the expected improvement. This suggests the possibility that other factors, such as variable weather conditions or possible inappropriate adjustments to the node antennas for the different tests, may have influenced the results. However, experiences have made it clear that these metrics do not provide a complete picture for evaluating communications in a specific scenario. However, they are useful elements, especially the SNR analysis as it detects the characteristic attenuations of shadow areas.

In this sense, after carrying out these field tests, the most reliable indicator to evaluate the quality of communications is the PPR metric of DL messages. This metric not only allows to clearly identify whether a node is in an unstable connection zone in the LoRaWAN network, but also determines its ability to receive DL. This is extremely important for applications that depend on the ability to receive remote configurations. Therefore, in accordance with the objective of this project, which aims to develop a protocol for non-mobile applications that require DL reception, it became evident that the PPR of DL messages is a valuable indicator to allow devices to autonomously determine whether they are in an unstable connection zone or not.

4.3. LORA AD HOC PROTOCOL - TWO-HOP TREE

To evaluate the performance of the Ad Hoc LoRa protocol and compare it with the operation of the typical LoRaWAN architecture, the distribution of nodes in the test area followed the same arrangement as in Figure 4.4, except for node 5, which was relocated to the upper position of the castle, as illustrated in Figure 4.5 a). During testing with the protocol, all nodes operated with SF7. Regarding the overall functioning of the protocol, as shown in Figure 3.2, an interval of 2 minutes was established for cycles during the DOP phase and an interval of 5 hours for the NCP phase.

The first step in evaluating the protocol was the network construction phase, in which its configuration was defined with a value of $n_{CAD} = 8$, which was considered adequate due to the reduced number of slaves foreseen in the test scenario. But before carrying out the NCP, the prototype followed the structure of the protocol, where the first moment of operation was the LoRaWAN joining process, since it was decided to configure the nodes to work with the OTAA activation method. Almost all nodes managed to join the network, although some faced difficulties, but managed to join within the maximum number of attempts established (Figure 3.4). The only exception was node 4, which resulted in the operation mode being changed to Slave. Subsequently, the DOP phase was executed, during which the stability check algorithm (Figure 3.5) was applied to determine whether the devices should maintain the Master function or change the operating mode to Slave. These settings were established when the NCP was first started, and Figure 4.12 shows the connections created after the network construction phase was completed.

Figure 4.12 – Node localisation and the formation of two-hop trees after the NCP phase.

Figure 4.12 illustrates the result of the NCP, which led to the formation of two two-hop trees. This means that there were nodes with unstable communication that connected to a one-hop relay node. An example of this is the transformation of node 1 into Slave, using node 5 as Master.

The second phase of evaluating the Ad Hoc LoRa protocol consisted of verifying the performance of the DOP, analysing the PPR in the UL transmissions of the nodes that constituted the two-hop trees. The tests were carried out over two days, resulting in a total of 1440 messages transmitted in all phases of the DOP, with a data length of 10 bytes. The results are illustrated in Table 4.3.

Table 4.3 – PPR of UL messages with SF7 operation.

Node	Distance (Hop)	PPR (%)
1	2	99,97 (48,73)
2	1	98,06
3	2	97,93 (7,12)
4	2	97,66 (0)
5	1	99,97

It is noted that the value in parentheses indicates the PPR when the node transmitted directly to the GW. The results in the table demonstrate that the formation of the two-hop tree had a positive impact on the PPR of the Slaves, compared to direct transmission to the GW. In addition, it is observed that the PPR of the Slaves were practically like those of their Masters, indicating a good connection between them. Therefore, the DOP phase seems to have worked as designed. However, a challenge arises when there is the possibility of interference/collision of messages from other nodes in the same phase, and how this interference can impact the results is a matter to be considered.

Another perspective of analysing the results of Table 4.3 involves comparing the PPR of the UL messages to operate only with LoRaWAN architecture and the PPR obtained with the operation of the Ad Hoc LoRa protocol, especially about Slave nodes. Figure 4.11 presents the PPR of the UL transmissions when the transmission in the two-hop tree was performed with SF7 and when a direct transmission with the GW was executed with several SF.

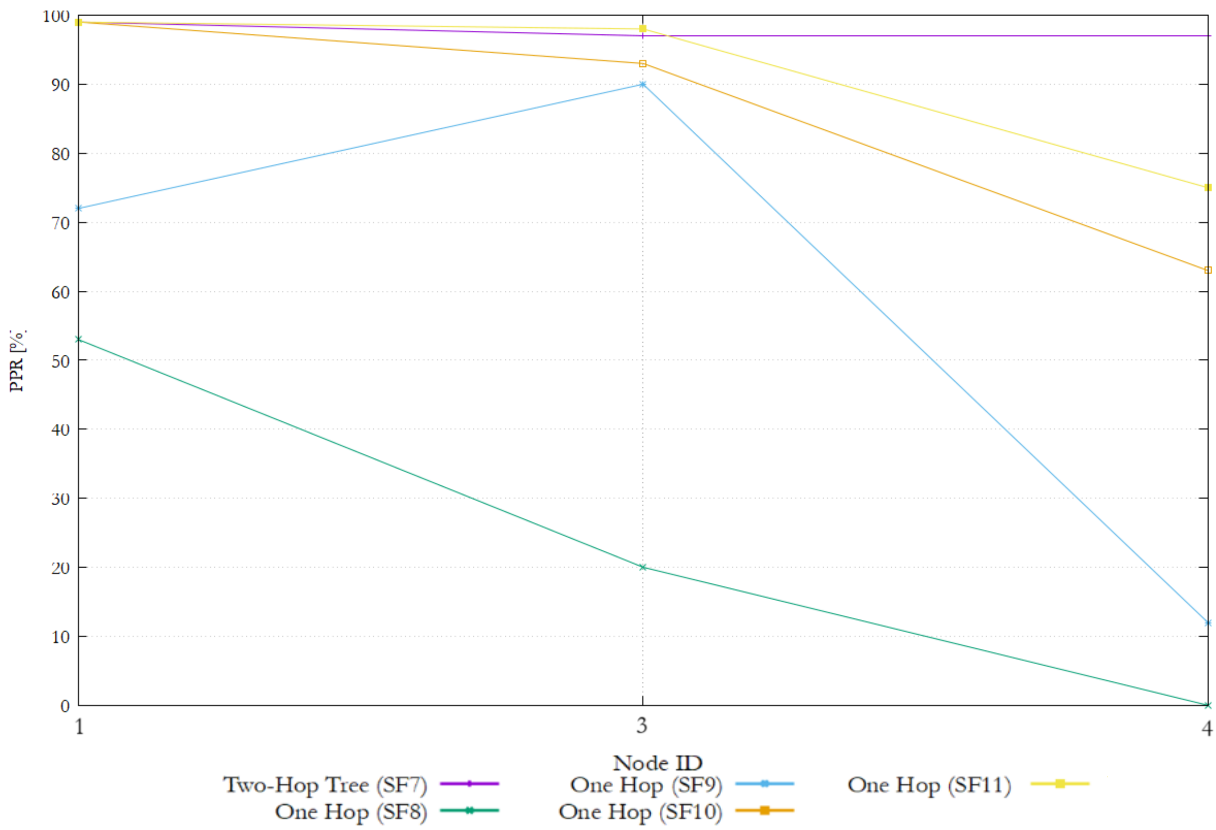


Figure 4.13 – PPR of UL messages from Slave nodes under the LoRaWAN protocol and Ad Hoc LoRa.

The graph in Figure 4.13 shows that even nodes classified as Slaves that used a higher SF, such as SF10, had an improvement in lower PPR compared to the percentages obtained when these nodes operated in the two-hop tree. This suggests that the Ad Hoc LoRa protocol offers greater reliability in the UL messages received by the GW. Moreover, although an energy analysis of the protocol has not been performed, there is a likelihood that transmissions within the two-hop tree will be more energy efficient. It is possible to verify this because, as shown in the previous Figure 4.13, all transmissions of the developed protocol were carried out with the SF with the lowest energy expenditure, while direct transmissions needed to use SF with higher energy requirements to achieve the same success rate in receiving packages.

4.4. CHAPTER CONSIDERATIONS

In this chapter, a set of tests was performed to evaluate the performance of the Ad Hoc LoRa protocol and compare it to the standard operation of LoRaWAN. The tests conducted highlighted the impact of blocking the line of sight between a base station and an end device on the appearance of shadow areas. In addition, they showed the ability of the protocol to fill in small shadow areas in the Penela region. An increase in the reliability of communications was observed compared to the typical operation of LoRaWAN, as well as the likelihood that the protocol will reduce energy consumption compared to the LoRaWAN network.

5. CONCLUSION AND FUTURE WORK

In this chapter, the conclusions and future work of the developed work are presented, which open new opportunities for research.

5.1. CONCLUSION

The main objective of this project was to develop and analyse an Ad Hoc protocol integrated with the LoRaWAN network to optimize communication, particularly in scenarios with connectivity challenges. This protocol was designed for devices with no mobility capability, which exclusively use the LoRa radio technology for communication. It was developed with the purpose of improving the reliability of communication in LoRaWAN networks, adopting a network architecture based on two-hop trees. In this model, nodes play the role of Master or relay, where they are responsible for coordinating all phases of the protocol, including tree building and data flow control (Asynchronous TDMA). On the other hand, there is the Slave role, which has no direct connection to the LoRaWAN network and only responds to the various instructions of the best Master chosen by it. The allocation of these roles is determined by the quality of the connection of each node to the LoRaWAN GW, giving this protocol an Ad Hoc character, since decisions are made autonomously.

One of the main objectives was to understand the underlying reasons for the emergence of unstable LoRaWAN connection areas, where packet losses occur within the range of a GW. The results obtained indicated that the lack of line of sight with the LoRaWAN base station is the main cause that increases the probability of there being zones with unstable communication. In addition, these initial tests allowed to identify the best indicator to detect these areas of communication instability, being the PPR metric of the DL messages. This metric has proven to be an effective indicator for assessing the stability of the LoRaWAN network and identifying areas where communication is facing problems.

In the performance analysis of the Ad Hoc LoRa protocol, tests demonstrated the ability to mitigate small areas where direct communication with the LoRaWAN base station was limited. The protocol allowed the formation of two-hop trees, in which nodes with unstable communication became Slaves, connecting to a Master node. This resulted in significant improvements in the percentages of successfully received packets in the UL messages, providing an effective solution for areas with unstable connectivity. In the comparative analysis between the UL messages transmitted by the Slave nodes with the Ad Hoc LoRa protocol and the UL messages of these same nodes operating exclusively in LoRaWAN, it was evident that the Ad Hoc LoRa protocol offered more reliable communication. Additionally, these results suggested another important consideration: the likelihood that transmissions under the protocol's operation may be more energy efficient compared to direct transmissions.

5.2. FUTURE WORK

The following are some points that should be explored to continuously validate and improve the developed protocol in the face of some limitations:

- Perform tests in simulated scenarios, focusing on the validation of the protocol at large scale. It is worth remembering that the current development stage of the protocol aims primarily to solve small areas of limited connectivity. Therefore, it will be essential to understand how the increase in the number of devices can impact the different phases of the protocol and the NCP performance.
- Investigate algorithms for interference control. Study adaptive systems that can automatically adjust parameters in the various phases of the protocol in response to interference. Consider strategies such as dynamic channel switching, transmission power adaptation, synchronization mechanisms, and medium access protocols.
- Optimize the NCP. During the analysis, it was hypothesized that the NCP results could be optimized in terms of the layout of the trees throughout a scenario. Even though the selection of Slaves and Masters is based on the SNR metric, there is apartment to investigate other approaches to tree construction. This could involve considering different metrics, exploring communication between Masters, or examining other hypotheses that could lead to a network architecture with even more robust connections.
- Implement redundancy and fault tolerance mechanisms to ensure the continuity of operation. Currently, the protocol can switch the mode of operation from Master to Slave, but it does not have the ability to return to the default mode. Therefore, in the case of failures in the Master nodes or if a Slave has not received any invitation to join a tree, the node is lost from a communication standpoint.
- Optimize energy consumption. There is an aspect in the LoRaWAN coverage instability verification algorithms that is the constant and unique resource of the LCR. This functionality, in addition to stealing resources from the LoRaWAN network, increases energy consumption. To counteract these aspects, the solution would be to improve the algorithm, balancing the need for link monitoring with the efficiency of network resources and device energy. In this context, the determination of when nodes should operate as Masters or Slaves can be optimized by considering additional criteria or specific scenarios.
- Develop a security mechanism. Explore additional security measures to protect device communications, especially in the exchange of messages at the Ad Hoc LoRa protocol level.
- Improve protocol control: For the development of the protocol's SW, sequential programming was used, which, although functional, it may be advantageous to explore more efficient and flexible alternatives. One

possibility would be the implementation of a system based on function pointers, where specific functions are assigned to actions at runtime. This approach opens the door for the asynchronous execution of tasks, simplifying the expansion of the protocol and making it easier to incorporate new features to meet different scenarios.

- Develop Software Development Kits (SDKs). Create custom SDKs to facilitate the integration and implementation of the Ad Hoc LoRa protocol in devices with different applications.

These proposals are intended to address the limitations of the current protocol and to further improve its performance and reliability. They are also aligned with the overall goal of the project, which is to develop a robust and efficient protocol for LoRaWAN networks with connectivity challenges.

BIBLIOGRAPHICAL REFERENCES

[1] J. R. Cotrim e J. H. Kleinschmidt, «LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication», *Sensors*, vol. 20, n. 15, p. 4273, Jul. 2020, doi: 10.3390/s20154273.

[2] Nick Jones, «Top 10 IoT Technologies for 2017 and 2018», Jan. 2016.

[3] S. Barrachina-Muñoz, B. Bellalta, e A. Bel, «HARE: Supporting Efficient Uplink Multi-Hop Communications in Self-Organizing LPWANs», *Sensors*, vol. 18, n. 1, p. 115, Jan. 2018, doi: 10.3390/s18010115.

[4] M. Cattani, C. Boano, e K. Römer, «An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication», *Journal of Sensor and Actuator Networks*, vol. 6, n. 2, p. 7, Jun. 2017, doi: 10.3390/jsan6020007.

[5] N. Sornin, M. Luis (Semtech, T. Eirich (IBM), T. Kramp (IBM), e O. Hersent (Actility), «LoRaWAN Specification V1», 2015.

[6] C.-H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, e H. Morikawa, «Multi-Hop LoRa Networks Enabled by Concurrent Transmission», *IEEE Access*, vol. 5, pp. 21430–21446, 2017, doi: 10.1109/ACCESS.2017.2755858.

[7] G. S. Tomar, L. Shrivastava, e S. S. Bhadauria, «Load Balanced Congestion Adaptive Routing for Randomly Distributed Mobile Adhoc Networks», *Wirel Pers Commun*, vol. 77, n. 4, pp. 2723–2733, Ago. 2014, doi: 10.1007/s11277-014-1663-9.

[8] Shih-Lin Wu e Yu-Chee Tseng, Eds., *Wireless ad hoc networking : personal-area, local-area, and the sensory-area networks*. Broken Sound Parkway NW: Auerbach Publication, 2007.

[9] A. Djedouboum, A. Abba Ari, A. Gueroui, A. Mohamadou, e Z. Aliouat, «Big Data Collection in Large-Scale Wireless Sensor Networks», *Sensors*, vol. 18, n. 12, p. 4474, Dez. 2018, doi: 10.3390/s18124474.

[10] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, e E. Cayirci, «A survey on sensor networks», *IEEE Communications Magazine*, vol. 40, n. 8, pp. 102–114, Ago. 2002, doi: 10.1109/MCOM.2002.1024422.

[11] M. Conti e S. Giordano, *Mobile ad hoc networking: Milestones, challenges, and new research directions*, IEEE Commun. Mag., vol. 52. 2014.

[12] Andreas F. Molisch, *Wireless Communications*, 2.ª ed. 2011.

[13] H. Wu e Y. Pan, *Medium access control in wireless networks*, vol. 8. Nova Publishers, 2008.

[14] André Fialho Ferreira Rosa, «Communication Primitives for Wireless Ad Hoc Networks», NOVA University, Lisboa, 2021.

[15] R. Aguirre *et al.*, «The grey area in wireless communications: A multiplatform experimental study», em *2014 IEEE Latin-America Conference on Communications*

(LATINCOM), IEEE, Nov. 2014, pp. 1–6. doi: 10.1109/LATINCOM.2014.7041867.

[16] M. G. Rubinstein, I. M. Moraes, M. E. M. Campista, L. H. M. K. Costa, e O. C. M. B. Duarte, «A Survey on Wireless Ad Hoc Networks», em *Mobile and Wireless Communication Networks*, Springer US, pp. 1–33. doi: 10.1007/978-0-387-34736-3_1.

[17] C. Seo, «Comparative analysis for MAC-Level protocols for ad-hoc wireless networks», 2007.

[18] A. Sgora, D. J. Vergados, e D. D. Vergados, «A Survey of TDMA Scheduling Schemes in Wireless Multihop Networks», *ACM Comput Surv*, vol. 47, n. 3, pp. 1–39, Abr. 2015, doi: 10.1145/2677955.

[19] A. D. G. Figueiredo, «Medium access control in LoRa networks with multiple low-cost gateways», Mestrado em Engenharia Eletrónica e Telecomunicações, Universidade de Aveiro, 2021. Acedido: 28 de Fevereiro de 2023. [Em linha]. Disponível em: http://hdl.handle.net/10773/31278

[20] Xin Wang e K. Kar, «Throughput modelling and fairness issues in CSMA/CA based ad-hoc networks», em *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, IEEE, pp. 23–34. doi: 10.1109/INFCOM.2005.1497875.

[21] P. Karn, «MACA-a new channel access method for packet radio», em *ARRL/CRRL Amateur radio 9th computer networking conference*, London, Canada, 1990, pp. 134–140.

[22] K. Tang e M. Gerla, «MAC reliable broadcast in ad hoc networks», em *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277)*, IEEE, pp. 1008–1013. doi: 10.1109/MILCOM.2001.985991.

[23] José Legatheaux Martins, *Fundamentos de Redes de Computadores Ilustrados com Base na Internet e nos Protocolos TCP/IP*, Nova.FCT Editorial. 2018. Acedido: 3 de Março de 2023. [Em linha]. Disponível em: https://legatheaux.eu/book/cnfbook-pub.pdf

[24] M. Lee *et al.*, «A new taxonomy of routing algorithms for wireless mobile ad hoc networks: The component approach», *Communications Magazine, IEEE*, vol. 44, pp. 116–123, Dez. 2006, doi: 10.1109/MCOM.2006.248174.

[25] A. Iwata, Ching-Chuan Chiang, Guangyu Pei, M. Gerla, e Tsu-Wei Chen, «Scalable routing strategies for ad hoc wireless networks», *IEEE Journal on Selected Areas in Communications*, vol. 17, n. 8, pp. 1369–1379, 1999, doi: 10.1109/49.779920.

[26] «G. He. "Destination-Sequenced Distance Vector (DSDV) Protocol". In: Networking Laboratory, Helsinki University of Technology (2002), pp. 1–9.»

[27] R. S. Sinha, Y. Wei, e S.-H. Hwang, «A survey on LPWA technology: LoRa and NB-IoT», *ICT Express*, vol. 3, n. 1, pp. 14–21, Mar. 2017, doi: 10.1016/j.icte.2017.03.004.

[28] M. Bor, J. Vidler, e U. Roedig, «LoRa for the Internet of Things», *EWSN*, pp. 361–366, Jan. 2016.

[29] Semtech, «AN1200.22 LoRa Modulation Basics».

[30] U. Noreen, A. Bounceur, e L. Clavier, «A study of LoRa low power and wide area network technology», em *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, IEEE, Mai. 2017, pp. 1–6. doi: 10.1109/ATSIP.2017.8075570.

[31] S. Abboud, «Study and improvement of long range communication technologies for wireless sensor networks», 2020.

[32] M. Bor e U. Roedig, «LoRa Transmission Parameter Selection», em *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, Jun. 2017, pp. 27–34. doi: 10.1109/DCOSS.2017.10.

[33] Y. Jiang, L. Peng, A. Hu, S. Wang, Y. Huang, e L. Zhang, «Physical layer identification of LoRa devices using constellation trace figure», *EURASIP J Wirel Commun Netw*, vol. 2019, n. 1, p. 223, Dez. 2019, doi: 10.1186/s13638-019-1542-x.

[34] «Ulysse Coutaud, Martin Heusse, Bernard Tourancheau. Fragmentation and Forward Error Correction for LoRaWAN small MTU networks. International Conference on Embedded Wireless Systems and Networks, EWSN, Feb 2020, Lyon, France. pp.289–294. hal-02861091».

[35] D. Zorbas, G. Z. Papadopoulos, P. Maille, N. Montavont, e C. Douligeris, «Improving LoRa Network Capacity Using Multiple Spreading Factor Configurations», em *2018 25th International Conference on Telecommunications (ICT)*, IEEE, Jun. 2018, pp. 516–520. doi: 10.1109/ICT.2018.8464901.

[36] M. Xhonneux, J. Tapparel, A. Balatsoukas-Stimming, A. Burg, e O. Afisiadis, «A Maximum-Likelihood-Based Two-User Receiver for LoRa Chirp Spread-Spectrum Modulation», *IEEE Internet Things J*, vol. 9, n. 22, pp. 22993–23007, Nov. 2022, doi: 10.1109/JIOT.2022.3186732.

[37] Semtech, «SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceive».

[38] A. Augustin, J. Yi, T. Clausen, e W. Townsley, «A Study of LoRa: Long Range & Low Power Networks for the Internet of Things», *Sensors*, vol. 16, n. 9, p. 1466, Set. 2016, doi: 10.3390/s16091466.

[39] F. Marlind e I. Butun, «Activation of LoRaWAN End Devices by Using Public Key Cryptography», em *2020 4th Cyber Security in Networking Conference (CSNet)*, IEEE, Out. 2020, pp. 1–8. doi: 10.1109/CSNet50428.2020.9265530.

[40] I. Butun, N. Pereira, e M. Gidlund, «Analysis of LoRaWAN v1.1 security», em *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, New York, NY, USA: ACM, Jun. 2018, pp. 1–6. doi: 10.1145/3213299.3213304.

[41] F. Marlind e I. Butun, «Activation of LoRaWAN End Devices by Using Public Key Cryptography», em *2020 4th Cyber Security in Networking Conference (CSNet)*, IEEE, Out. 2020, pp. 1–8. doi: 10.1109/CSNet50428.2020.9265530.

[42] LoRa Alliance, «LoRaWAN Relay Specification TS011-1.0.0 ». Setembro de 2022.

[43] «Brady Amiot. (2023) LoRa Alliance® Announces New Relay Feature that Extends LoRaWAN® Coverage for Metering, Utilities, Smart Cities and Industrial Applications - LoRa Alliance®. Retrieved February 02, 2023, from https://lora-alliance.org/lora-alliance-press-release/lora-alliance-announces-new-relay-feature-that-extends-lorawan-coverage-for-metering-utilities-smart-cities-and-industrial-applications/».

[44] D.-Y. Kim, S. Kim, H. Hassan, e J. H. Park, «Adaptive data rate control in low power wide area networks for long range IoT services», *J Comput Sci*, vol. 22, pp. 171–178, Set. 2017, doi: 10.1016/j.jocs.2017.04.014.

[45] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, e J.-C. Prevotet, «Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility», *IEEE Communications Surveys & Tutorials*, vol. 21, n. 2, pp. 1561–1581, Fev. 2019, doi: 10.1109/COMST.2018.2877382.

[46] «RA Guidelines for Use of EUI, OUI, and CID - eui.pdf. (2023) Retrieved February 15, 2023, from https://standards.ieee.org/wp-content/uploads/import/documents/tutorials/eui.pdf».

[47] Semtech Corporation, «SX1272/73 - 860 MHz to 1020 MHz Low Power Long Range Transceiver», Jan. 2019.

[48] B. Reynders e S. Pollin, «Chirp spread spectrum as a modulation technique for long range communication», em *2016 Symposium on Communications and Vehicular Technologies (SCVT)*, IEEE, Nov. 2016, pp. 1–5. doi: 10.1109/SCVT.2016.7797659.

[49] J. Petäjäjärvi, K. Mikhaylov, M. Pettissalo, J. Janhunen, e J. Iinatti, «Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage», *Int J Distrib Sens Netw*, vol. 13, n. 3, p. 155014771769941, Mar. 2017, doi: 10.1177/1550147717699412.

[50] R. Oliveira, L. Guardalben, e S. Sargento, «Long range communications in urban and rural environments», em *2017 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, Jul. 2017, pp. 810–817. doi: 10.1109/ISCC.2017.8024627.

[51] K. Mikhaylov, J. Petäjäjärvi, e T. Hänninen, «Analysis of the Capacity and Scalability of the LoRa Wide Area Network Technology», 2016.

[52] O. Georgiou e U. Raza, «Low Power Wide Area Network Analysis: Can LoRa Scale?», Out. 2016, doi: 10.1109/LWC.2016.2647247.

[53] D. Croce, M. Gucciardo, S. Mangione, G. Santaromita, e I. Tinnirello, «Impact of LoRa Imperfect Orthogonality: Analysis of Link-Level Performance», *IEEE Communications Letters*, vol. 22, n. 4, pp. 796–799, Abr. 2018, doi: 10.1109/LCOMM.2018.2797057.

[54] D. Croce, M. Gucciardo, S. Mangione, G. Santaromita, e I. Tinnirello, «LoRa Technology Demystified: From Link Behavior to Cell-Level Performance», *IEEE Trans Wirel Commun*, vol. 19, n. 2, pp. 822–834, Fev. 2020, doi: 10.1109/TWC.2019.2948872.

[55] T. Voigt, M. Bor, U. Roedig, e J. Alonso, «Mitigating Inter-network Interference in LoRa Networks», Nov. 2016.

[56] M. C. Bor, U. Roedig, T. Voigt, e J. M. Alonso, «Do LoRa Low-Power Wide-Area Networks Scale?», em *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, New York, NY, USA: ACM, Nov. 2016, pp. 59–67. doi: 10.1145/2988287.2989163.

[57] R. B. Sorensen, N. Razmi, J. J. Nielsen, e P. Popovski, «Analysis of LoRaWAN Uplink with Multiple Demodulating Paths and Capture Effect», em *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, IEEE, Mai. 2019, pp. 1–6. doi: 10.1109/ICC.2019.8761142.

[58] G. Callebaut e L. Van der Perre, «Characterization of LoRa Point-to-Point Path Loss: Measurement Campaigns and Modeling Considering Censored Data», *IEEE Internet Things J*, vol. 7, n. 3, pp. 1910–1918, Mar. 2020, doi: 10.1109/JIOT.2019.2953804.

[59] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia, e T. Watteyne, «Understanding the limits of LoRaWAN», Jul. 2016, doi: 10.1109/MCOM.2017.1600613.

[60] N. Varsier e J. Schwoerer, «Capacity limits of LoRaWAN technology for smart metering applications», em *2017 IEEE International Conference on Communications (ICC)*, IEEE, Mai. 2017, pp. 1–6. doi: 10.1109/ICC.2017.7996383.

[61] A.-I. Pop, U. Raza, P. Kulkarni, e M. Sooriyabandara, «Does Bidirectional Traffic Do More Harm Than Good in LoRaWAN Based LPWA Networks?», Abr. 2017.

[62] T. Polonelli, D. Brunelli, A. Marzocchi, e L. Benini, «Slotted ALOHA on LoRaWAN-Design, Analysis, and Deployment», *Sensors*, vol. 19, n. 4, p. 838, Fev. 2019, doi: 10.3390/s19040838.

[63] L. Chasserat, N. Accettura, e P. Berthou, «Short: Achieving Energy Efficiency in Dense LoRaWANs through TDMA», em *2020 IEEE 21st International*

Symposium on «A World of Wireless, Mobile and Multimedia Networks» (WoWMoM), IEEE, Ago. 2020, pp. 26–29. doi: 10.1109/WoWMoM49955.2020.00019.

[64] J. Lee, W.-C. Jeong, e B.-C. Choi, «A Scheduling Algorithm for Improving Scalability of LoRaWAN», em *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, Out. 2018, pp. 1383–1388. doi: 10.1109/ICTC.2018.8539392.

[65] R. Oliveira, L. Guardalben, M. Luis, e S. Sargento, «Multi-Technology Data Collection: Short and Long Range Communications», em *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, IEEE, Set. 2017, pp. 1–6. doi: 10.1109/VTCFall.2017.8288231.

[66] C. Pham, «Investigating and experimenting CSMA channel access mechanisms for LoRa IoT networks», em *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, Abr. 2018, pp. 1–6. doi: 10.1109/WCNC.2018.8376997.

[67] S. Ahsan, S. A. Hassan, A. Adeel, e H. K. Qureshi, «Improving Channel Utilization of LoRaWAN by using Novel Channel Access Mechanism», em *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, Jun. 2019, pp. 1656–1661. doi: 10.1109/IWCMC.2019.8766700.

[68] A. Gamage, J. C. Liando, C. Gu, R. Tan, e M. Li, «LMAC», em *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, New York, NY, USA: ACM, Set. 2020, pp. 1–13. doi: 10.1145/3372224.3419200.

[69] S. Hong, F. Yao, Y. Ding, e S.-H. Yang, «A Hierarchy-Based Energy-Efficient Routing Protocol for LoRa-Mesh Network», *IEEE Internet Things J*, vol. 9, n. 22, pp. 22836–22849, Nov. 2022, doi: 10.1109/JIOT.2022.3185619.

[70] A. Abrardo e A. Pozzebon, «A Multi-Hop LoRa Linear Sensor Network for the Monitoring of Underground Environments: The Case of the Medieval Aqueducts in Siena, Italy», *Sensors*, vol. 19, n. 2, p. 402, Jan. 2019, doi: 10.3390/s19020402.

[71] L. Mai e M. Kim, *Multi-Hop LoRa Network with Pipelined Transmission Capability*. 2019.

[72] G. Zhu, C.-H. Liao, T. Sakdejayont, I.-W. Lai, Y. Narusue, e H. Morikawa, «Improving the Capacity of a Mesh LoRa Network by Spreading-Factor-Based Network Clustering», *IEEE Access*, vol. 7, pp. 21584–21596, 2019, doi: 10.1109/ACCESS.2019.2898239.

[73] J. Dias e A. Grilo, «Multi-hop LoRaWAN uplink extension: specification and prototype implementation», *J Ambient Intell Humaniz Comput*, vol. 11, n. 3, pp. 945–959, Mar. 2020, doi: 10.1007/s12652-019-01207-3.

[74] H.-C. Lee e K.-H. Ke, «Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation», *IEEE Trans Instrum Meas*, vol. 67, n. 9, pp. 2177–2187, Set. 2018, doi: 10.1109/TIM.2018.2814082.

[75] M. DIOP e C. PHAM, «Increased flexibility in long-range IoT deployments with transparent and light-weight 2-hop LoRa approach», em *2019 Wireless Days (WD)*, IEEE, Abr. 2019, pp. 1–6. doi: 10.1109/WD.2019.8734228.

[76] D. Tanjung, S. Byeon, J. Huh, D. H. Kim, e J. D. Kim, «Opportunistic and On-Demand Network Coding-Based Solutions for LPWAN Forwarding», *Sensors*, vol. 20, n. 20, p. 5792, Out. 2020, doi: 10.3390/s20205792.

[77] « LoRaWAN 1.0.2 Specification (July 2016), Sections 7 and 18.4, LoRaWAN 1.0.3 Specification (March 20, 2018), Section 7 and 18.4.».

[78] Semtech, « Design Support LoRa Calculator».

APPENDIX A

AD HOC WIRELESS NETWORK FOR LONG RANGE APPLICATIONS

J. R. Craveiro Ferreira (1), J. Pedro Amaro. Pestana (1)(2), C. I. Faustino Agreira (1)(3)(4)

IPC/ Instituto Superior de Engenharia de Coimbra – Departamento de Engenharia Eletrotécnica, Coimbra, Portugal (joaorc19ferreira@gmail.com)
CERNAS – Research Centre for Natural Researchers (amaro@isec.pt)
SUScita - Research Group on Sustainability, Cities and Urban Intelligence,
INESC Coimbra, Coimbra Portugal, cif@isec.pt

EXTENDED ABSTRACT

The Long Range (LoRa) technology has been gaining popularity, becoming one of the most promising and frequently used technologies among Low Power Wide Area Networks (LPWANs). Highly compatible with Internet of Things (IoT) applications, LoRa enables long-range communications, albeit with low transmission rates and duty cycle constraints. Despite all this enthusiasm, challenges persist in LoRa networks, especially in terms of coverage, with the occurrence of problematic areas where communications are inconsistent, often referred to as shadow zones. The reasons are diverse, ranging from the urban propagation environment, physical obstruction to the network base station, or locations with significant electromagnetic attenuation, among others. In this context, this work focused on designing an Ad Hoc protocol integrated with the LoRaWAN network to perfect communication in unstable scenarios. This protocol was designed for non-mobile devices that rely exclusively on LoRa technology for communication. The Ad Hoc LoRa approach aims to address small areas with unstable connectivity by transforming unstable nodes into Slave devices that connect to relay nodes called Masters, resulting in the formation of two-hop communication trees. The test results reveal the effectiveness of the Ad Hoc LoRa protocol in optimizing network coverage and improving the success rates of transmitted messages. Furthermore, the results suggest that the protocol may offer superior energy efficiency compared to direct transmissions to LoRaWAN base stations.
Index terms: LoRaWAN, Shadow Zones, Ad Hoc, Multihop, Two-Hop Tree

REFERENCES

[1] J. R. Cotrim e J. H. Kleinschmidt, «LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication», Sensors, vol. 20, n. 15, p. 4273, Jul. 2020, doi: 10.3390/s20154273.
[2] Nick Jones, «Top 10 IoT Technologies for 2017 and 2018», Jan. 2016.
[3] S. Barrachina-Muñoz, B. Bellalta, e A. Bel, «HARE: Supporting Efficient Uplink Multi-Hop Communications in Self-Organizing LPWANs», *Sensors*, vol. 18, n. 1, p. 115, Jan. 2018, doi: 10.3390/s18010115.
[4] M. Cattani, C. Boano, e K. Römer, «An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication», *Journal of Sensor and Actuator Networks*, vol. 6, n. 2, p. 7, Jun. 2017, doi: 10.3390/jsan6020007.
[5] N. Sornin, M. Luis (Semtech, T. Eirich (IBM), T. Kramp (IBM), e O. Hersent (Actility), «LoRaWAN Specification V1», 2015.
[6] C.-H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, e H. Morikawa, «Multi-Hop LoRa Networks Enabled by Concurrent Transmission», IEEE Access, vol. 5, pp. 21430–21446, 2017, doi: 10.1109/ACCESS.2017.2755858.
[7] G. S. Tomar, L. Shrivastava, e S. S. Bhadauria, «Load Balanced Congestion Adaptive Routing for Randomly Distributed Mobile Adhoc Networks», Wirel Pers Commun, vol. 77, n. 4, pp. 2723–2733, Ago. 2014, doi: 10.1007/s11277-014-1663-9.
[8] Shih-Lin Wu e Yu-Chee Tseng, Eds., Wireless ad hoc networking : personal-area, local-area, and the sensory-area networks. Broken Sound Parkway NW: Auerbach Publication, 2007.
[9] A. Djedouboum, A. Abba Ari, A. Gueroui, A. Mohamadou, e Z. Aliouat, «Big Data Collection in Large-Scale Wireless Sensor Networks», Sensors, vol. 18, n. 12, p. 4474, Dez. 2018, doi: 10.3390/s18124474.
[10] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, e E. Cayirci, «A survey on sensor networks», IEEE Communications Magazine, vol. 40, n. 8, pp. 102–114, Ago. 2002, doi: 10.1109/MCOM.2002.1024422.
[11] M. Conti e S. Giordano, Mobile ad hoc networking: Milestones, challenges, and new research directions, IEEE Commun. Mag., vol. 52. 2014.
[12] Andreas F. Molisch, Wireless Communications, 2.a ed. 2011.