Experimental Insights into the Performance of LoRa/LoRaWAN Radio Interface in Smart City Deployments

Luis Pires * and José Martins *

Posted Date: 5 November 2024

doi: 10.20944/preprints202411.0254.v1

Keywords: IoT; LPWAN; LoRaWAN; LoRa; Spreading Factor; Collision Effects, Interference, Payload Size

 doi:10.20944/preprints202411.0254.v1

Article

Experimental Insights into the Performance of LoRa/LoRaWAN Radio Interface in Smart City Deployments

Luis Miguel Pires [1,2,*] and José Martins [1,3,*]

[1] Technologies and Engineering School (EET), Instituto Politécnico da Lusofonia (IPLuso), Lisbon, Portugal
[2] Department of Electronical Engineering, Telecommunications and Computers (DEETC), Instituto Superior de Engenharia de Lisboa (ISEL), Lisbon, Portugal
[3] Department of Systems and Informatics (DSI), Setúbal School of Technology, Instituto Politécnico de Setúbal (IPS), Setúbal, Portugal
* Correspondence: luis.pires@ipluso.pt (L.M.P.); jose.manuel.martins@ipluso.pt (J.M.)

Abstract: IoT ecosystem extends beyond country borders and application domains, combining thousands of versatile devices that differ in terms of their structures, capabilities, and available resources. It is therefore not surprising that the landscape of wireless communication technologies and the degree of IoT devices available today is excessively broad and diverse and the reliability of LoRaWAN networks can be affected by factors such as collisions, interference, and varying signal strengths. Interference between networks leads to frame collisions and consequent packet loss. Frame collisions occur when two or more packets overlap in time and frequency and use the same Long Range (LoRa) parameters, i.e. the same Spreading Factor (SF), Bandwidth (BW) and Carrier Frequency (CF). When most devices use the same configuration, collision probability is higher. The probability of frame collisions is also affected by traffic characteristics, particularly the periodicity of the transmission and the payload size. Larger payload sizes and more frequent transmissions accumulate with higher Time on Air (ToA) and channel occupancy [1]. Transmission powers and the location of the gateways also influence this situation. The aim of this experimental work is to verify the effects of collisions and interference in Long Range Wide Area Network (LoRaWAN), focusing on how SFs and payload sizes influence signal transmission quality in an inter-SF interference scenario. This research is crucial for smart cities, where numerous IoT devices are deployed to monitor and manage urban infrastructure. Reliable and efficient communication networks are essential for the seamless operation of Urban IoT (UIoT) systems. In this context, the integration of IoT, along with other systems such as cyber-physical systems and cloud computing, necessitates robust and scalable communication networks to ensure efficient data transmission and network reliability. LoRaWAN, with its long-range and low-power capabilities, is already a widely adopted technology for connecting numerous devices and can be seamlessly integrated across large urban environments. In such environments, inter-SF interference can significantly impact the performance of LoRaWAN networks. The choice of SFs and packet lengths directly affects ToA. When multiple devices operate near gateways, using different SFs and varying packet lengths can lead to increased latency and longer ToA. This, in turn, raises the risk of packet loss, especially in scenarios with a low signal-to-interference ratio (SIR). Such limitations pose challenges to the scalability of the network, particularly in Non-Line-Of-Sight (NLOS) situations, where obstacles like vegetation or buildings (or field walls) can further degrade signal quality. Our work validates measuring performance indicators like Received Signal Strength Indicator (RSSI), ToA, and Packet Delivery Ratio (PDR) to assess network reliability. By analyzing ToA in relation to RSSI and different data sizes, and examining RSSI for different SFs and data sizes, we gain a comprehensive understanding of the network's performance. Additionally, we evaluate packet loss through PDR to understand the reliability of packet transmission. These metrics are essential for optimizing the performance and reliability of LoRaWAN networks, which will impact various smart city applications such as environmental monitoring, smart metering or smart buildings. We conclude that in an environment with inter-SF interference, the choice of SFs and packet lengths impacts ToA, leading to packet loss in the NLOS scenario.

Keywords: IoT; LPWAN; LoRaWAN; LoRa; spreading factor; collision effects; interference; payload size

 doi:10.20944/preprints202411.0254.v1

1. Introduction

Since the 1990s, the Internet of Things (IoT) has become an integral part of our daily lives. Articles predict that there will be around 22 billion IoT devices by 2025, highlighting the exponential technological development observed in recent decades. Beyond the development of new IoT devices and their versatile applications, there is a growing need to automate, control, and simplify processes across various economic sectors. Today, it is evident that almost everything produced in industry (with few exceptions) utilizes IoT devices to enhance efficiency, reduce costs, and lower energy consumption. The primary goal of introducing these devices is to keep them running continuously, thereby alleviating high energy burdens and accelerating mass production.

In smart city scenarios, the application of IoT has elevated the challenges faced and simultaneously improved the lives of residents. IoT is shaping smart cities by integrating various devices and technologies, reducing the need for human intervention. This integration promotes sustainable living, increases comfort, and enhances productivity for the population. Various domains benefit from IoT in smart cities, including transportation, energy management, healthcare, and environmental monitoring. Additionally, innovative integrations with blockchain and IoT technologies are emerging. However, challenges such as privacy, security, and scalability must be addressed, especially in new applications like Industry 4.0 (advanced manufacturing), smart financing, and intelligent transportation (connected mobility).

Not all applications require the same level of security or quality of service (QoS). Understanding QoS in networking is essential for effective traffic management. Different IoT services have varying QoS requirements based on factors such as functionality (e.g., monitoring, control, data processing and analysis), message type (occasional, regular, or interactive response), data rate (low or high), latency, reliability, security (encryption, authentication, access control), and scalability (efficiently managing the growing number of devices).

In this context, the trend is towards increasing the number of End Devices (EDs) and Gateways (GWs) in networks, offering different types of services and generating various types of messages (i.e., different payloads co-existing). During the network design process, critical variables include determining the optimal placement of GWs and EDs. Factors such as coverage, interference, and signal strength must be considered, along with assessing the desired coverage area and density to balance coverage and capacity. Additionally, the successful deployment of devices depends on various factors, including data rate, payload frequency, and battery life. These can be detailed as follows:

- Data Rate: Low data rate schemes allow more devices to share the network but affect payload size and latency.
- Payload Frequency: Devices transmitting frequently (e.g., every hour) consume more resources.
- Battery Life: Longer battery life requires efficient power management, significantly influenced by data rate and payload frequency.

These challenges are particularly relevant for smart city applications such as traffic management systems, environmental monitoring, and smart building automation. To address these issues, advanced interference management techniques and adaptive SF selection algorithms can be employed to optimize network performance and ensure reliable communication. Interference management techniques, such as dynamic channel allocation and interference cancellation, help minimize the impact of overlapping signals from multiple devices. These techniques dynamically adjust the communication parameters to reduce collisions and improve signal clarity.

Adaptive SF selection algorithms, on the other hand, dynamically choose the optimal SF for each device based on real-time network conditions. By analyzing factors such as signal strength, distance from the gateway, and current network load, these algorithms can assign the most suitable SF to each device. This ensures efficient use of the available spectrum, reduces latency, and enhances overall network reliability.

In this context, studying how specific SFs (7, 9, and 12), along with payload lengths (14, 32, and 51 bytes), influence signal transmission, collisions, and interference in a smart city deployment is even more relevant to ensure reliable data transmission in challenging conditions. More in detail:

 doi:10.20944/preprints202411.0254.v1

- Optimization of Network Performance: Understanding how different SFs and payload sizes affect signal transmission can help in fine-tuning the network for optimal performance. This can lead to more efficient use of the available spectrum and better overall network reliability.
- Interference Management: By studying these parameters, we gain a better understanding of how to manage interference, which is crucial in a dense urban environment where many devices might be transmitting simultaneously.
- Adaptive Techniques: The data from such a study can aid in developing more effective adaptive SF selection algorithms and interference management techniques. This can help dynamically adjust communication parameters to minimize collisions and improve signal clarity.
- Real-World Application: In a smart city, various applications (e.g., traffic management, environmental monitoring, smart lighting) have different requirements. Understanding the impact of SFs and payload sizes can help customize the network to meet these diverse needs.

These results will highlight the critical need to optimize SFs and packet lengths to enhance network reliability and scalability. As the number of connected devices in a smart city grows, the ability to manage collisions and interference becomes increasingly important. Studying these factors can help design a scalable network that can handle future growth. By addressing these challenges, LoRaWAN can better support the diverse and demanding communication needs of smart cities, ensuring efficient data transmission and robust connectivity in urban environments.

In the design of a LoRaWAN network, it is quite important to carefully weigh trade-offs among these key variables and network capacity [7]. Additionally, precise configuration of parameters—such as spreading factors, bandwidth, transmit power, and duty cycling—has a significant impact on LoRaWAN performance [8]. Besides the geographical arrangement of GWs and EDs, interference—both internal within the network and external from other sources—plays a pivotal role and managing it well will be crucial for a LoRaWAN network Efficiency [9,10]. Consequently, the design and implementation of these IoT LoRaWAN networks present a series of challenges, making their study a wide field of experience and interest. The reliability and quality of service in these networks will, this way, significantly influence their overall performance and scalability.

In our research, we explore interference effects related to the SF and Collision Effects in the 868 MHz LoRaWAN Radio Interface. We create real-world scenarios with devices transmitting varying information at different distances, potentially leading to packet overlap and increased packet loss probability. Our study involves practical tests, including approximately 500 field measurements between a gateway and a LoRa device, which we detail in this paper. If simulations tools are valuable during network projects, field tests remain decisive. And correctly setting LoRaWAN parameters is fundamental for achieving optimal network performance and to substantiate design considerations, measuring performance indicators will be necessary. This way, metrics such as RSSI, ToA, and PDR will be used to test the reliability and quality of service of a LoRaWAN link in real-world scenarios. Validating these metrics to ensure a good quality of LoRa signals will be a key factor in our experiment.

In this study, validating the performance indicators within the proposed scenarios could extend their applicability to other types of scenarios with a different scale. As said before, the designer's theoretical choices regarding LoRa parameters significantly impact network performance and scalability.

Among the various parameters considered, the SF, for example, may not be as obvious as it seems [11]. Depending on the selected parameters (and the presence of neighboring networks), both intra-SF interference and inter-SF interference can occur. This way managing both types of interference will be essential for optimizing network efficiency and scalability [12,13] and designers should conduct field tests to validate their choices and optimize their networks. These measurements will also shed light on the importance of the SF and the impact of overlapping SFs within the same channel, particularly concerning interference and collisions. Detailing:

SF:

- SF determines the signal's bandwidth and data rate.
- Higher SF (e.g., SF12) provides better resistance to interference but increases airtime, while lower SF (e.g., SF7) allows faster data rates but can be more susceptible to interference. A low SF spreads

 doi:10.20944/preprints202411.0254.v1

the signal across a broader frequency range due to longer chirps, impacting interference susceptibility.

- PDR can reflect how well the chosen SF copes with interference and collisions.

Interference:

- High interference can degrade signal quality, leading to packet loss and reduced reliability and quality of service.
- RSSI helps detect interference by measuring signal strength. A sudden drop in RSSI may indicate interference.

Collisions:

- Collisions occur when multiple devices transmit simultaneously. When two or more devices attempt to send data at the same time, their signals can interfere with each other, leading to packet loss. And ToA helps estimate collision timing. Longer ToA can indicate more collisions.
- Optimizing SF (and duty cycle) can minimize collisions.
- PDR quantifies successful packet delivery despite collisions.

After the designer has made theoretical choices for a network, utilizing measuring performance indicators such as RSSI, ToA, and PDR becomes essential for validating those decisions. By adjusting the SF, monitoring RSSI and ToA and analyzing PDR, LoRaWAN networks can effectively mitigate interference and manage collisions.

So, these metrics validate the practical feasibility of theoretical choices, ensuring that the network performs as expected in real-world scenarios.

To simulate real-world behavior, we transmitted packets with different SFs and data sizes in a pseudo-random manner. These transmissions overlapped within the same channel, creating an inter-SF interference scenario. By doing so, we explored the theoretical orthogonality between these parameters. Even though we transmitted from a single source, this approach allowed us to model the behavior of multiple devices within a LoRa network.

Different possibilities of orthogonalize transmissions were set. This way Carrier Frequency (868.2 MHz), Code Rate (CR) of 4/5 and BW 125 kHz were fixed, while testing different SFs (7, 9, 12). Our goal was to increase the likelihood of packet loss by adjusting the emitted power and shortening the transmission distance while transmitting packages of different SFs and different payload sizes. This deliberate interference was intended to create a significant impact, as discussed in the previous study by D. Croce et al. [14] where in their analysis of LoRa modulation, they demonstrated that collisions between packets of different SFs can indeed lead to packet loss, particularly when the received interference power is strong enough.

In Section 2, we present related work. In Sections 3 and 4, we will discuss the fundamental mechanisms and concepts of LoRa technology, exploring their impact on network performance. We also analyze the causal relationships between various factors affecting network efficiency and summarize the challenges specific to LoRaWAN networks. Section 5 describes the specific experimental environment and methods and provides a discussion of the results. Finally, Section 6 presents our conclusions.

2. Related Work

IoT is characterized by ongoing growth and innovation. It has moved beyond its initial stage of basic connected devices and has transformed into a sophisticated ecosystem of interconnected sensors, devices, and platforms. Understanding interference and collisions in real-world scenarios is essential for achieving successful scalability when deploying efficient LoRaWAN networks. However, this scalability faces a significant challenge due to the use of a variant of the Aloha protocol in its Medium Access Control (MAC) layer. As the number of devices (EDs and GWs) increases, performance degrades rapidly. Therefore, making balanced and informed choices and tuning the physical layer (PHY) parameters becomes crucial. These decisions will significantly impact LoRaWAN performance and help mitigate the limitations introduced by the pure Aloha protocol, ultimately enhancing LoRaWAN scalability, reliability, and overall service quality.

Several studies related to the theme under study in this paper have been conducted.

 doi:10.20944/preprints202411.0254.v1

Jetmir Haxhibeqiri et al. [15]in their study focuses on assessing the scalability of LoRaWAN networks in terms of the number of end devices per gateway. They performed measurements to understand the interference behavior between two physical end nodes. Their conclusion was that even under concurrent transmission, one of the packets can be received under certain conditions. Based on these measurements, the researchers created a simulation model. When the number of nodes increases up to 1000 per gateway, the losses can be up to 32%. However, with a lower application layer duty cycle (below the allowed radio duty cycle of 1%), losses decrease further. While this study provides a solid basis and is important, our objective differs. We aim to establish real-world scenarios and investigate the impact of interference and packet length on the scalability of LoRaWAN networks, with the goal of enhancing their reliability and overall quality of service.

In another study on scalability, Bor et al. [16] investigated the relationship between physical layer parameter settings (such as bandwidth, coding rates, spreading factor, and center frequency) and the capacity of LoRa networks. Their research focused on scenarios where devices communicate directly with a sink node, eliminating the need for complex multi-hop networks. LoRa offers various communication options, allowing transmitters to choose from Center Frequency (CF), SF, BW, and CR. Through simulations, the researchers demonstrated that the choice of physical layer parameters impacts the number of LoRa nodes that can access the channel simultaneously, thereby limiting the network's capacity. However, effective scalability can be achieved in LoRa networks through dynamic communication parameter selection and/or the use of multiple sinks.

Lavric et al. [17] also address challenges posed by the IoT concept, including scalability and sensor integration. They focused on LoRa communication technology, which is considered an ideal solution for these issues. In their empirical evaluation, they analyze communication collisions in various scenarios. Despite an increased packet payload, communication resistance to interferences remained relatively unaffected. In a subsequent stage of the experiment, they employed a LoRa Traffic Generator with new Software Defined Radio (SDR) technology. And despite using orthogonal variable spreading factor techniques within the same communication channel, they concluded collisions between LoRa packets significantly impact communication performance showing that different spreading factors also exhibit conflict and greatly reduce LoRa performance. Moreover, the authors find that packet length is not a key factor affecting LoRa performance. Our study aims to demonstrate the opposite.

Other researchers have already explored the reliability of communication links in smart cities. They considered various distances between end nodes and base stations, along with different spreading factors. Some early studies were conducted by S. Kartakis et al. [18] and M. Centenaro et al. [19]. In [18] they analyzed standard technologies like LoRa, Sigfox, NB-IoT, and LTE-M. Their findings highlighted the potential of these Low-Power Wide-Area Network (LPWAN) technologies for cost-effective and energy-efficient IoT applications. However, real-world performance remains an ongoing area of investigation. In turn, [19] describe LPWANs as an emerging wireless connectivity paradigm. These networks utilize low-rate, long-range transmission technologies in unlicensed sub-GHz frequency bands. The star topology of LPWANs offers advantages over established paradigms, particularly for Smart Cities applications, emphasizing efficiency and effectiveness.

In a work aimed to study the LoRaWAN Performance Evaluation, Sanchez-Iborra, R. et al. [20] investigated three distinct scenarios—urban, suburban, and rural. They emphasized the importance of evaluating deployment scenarios for successful system implementation. They achieved that propagation conditions significantly impact LoRaWAN performance, and a balance between network robustness and transmission data rate is essential. However, their study did not explore all parameter configurations, leaving some details about the relationship between physical layer parameters and LoRa performance unspecified.

Regarding interference and robustness, B. Reynders et al. [21] compared Chirp Spread Spectrum (CSS) modulation with Binary Phase-Shift Keying (BPSK) in terms of robustness and interference. Despite symbols not being perfectly orthogonal, CSS demonstrated robustness against interfering signals. However, in long-range communication, relying solely on robustness is insufficient due to the considerable impact of propagation losses. While robustness is important and does help in

 doi:10.20944/preprints202411.0254.v1

dealing with weakened signals due to propagation losses, other strategies (e.g. such as increasing transmission power, using directional antennas, employing repeaters, or using ADR) might be necessary to ensure reliable communication and are often needed to address the significant impact of these losses in long-range communication. These measures, combined with the inherent robustness provided by CSS technology, make LoRaWAN well-suited for long-range, low-power communication applications. Also a solution like deploying more gateways can improve coverage (reduces the distance between end devices and gateways), but the challenge of scalability of the networks becomes a major question.

Qingjie Guo et al. [22] in their study aim to understand how physical layer parameters impact LoRa packet reception performance and energy efficiency. Their study was conducted to an evaluation experiment under a negative Signal-to-Noise Ratio (SNR). They clarified the specific details of the relationship between physical layer parameters (such as bandwidth, spreading factor, and coding rate) and LoRa packet reception performance. Their study also examined the effect of packet length on reception performance. Their conclusion was that, for large amounts of data, longer packets outperformed shorter ones. In the end and considering both physical layer parameters and packet length, the authors proposed a transmission scheme that balances reliability, delay, and energy consumption. Yet, the paper lacks specific scenarios such as Line-of-Sight (LOS), NLOS, or different distances. That we propose in our study. And without these scenarios, it would be quite challenging to assess the study's impact in real-world applications.

As previously mentioned, our study diverges from the related previous research. We aim to obtain important details regarding the influence of various SFs on LoRaWANs packet reception performance over the same channel, while also considering different packet length settings. Additionally, we propose validating the measuring performance indicators introduced in the study's introduction—namely, RSSI, ToA, and PDR—within the proposed scenarios. This validation aims to assess the practical feasibility of theoretical decisions made by the designer and to evaluate the reliability and quality of service of our link. By doing so, we gain insights into how these results will impact performance and scalability in other networks. Our focus lies not on simulations but on conducting real-world field tests.

3. LoRa Technology

LoRa is a LPWAN technology owned by Semtech [23] based on CSS modulation.

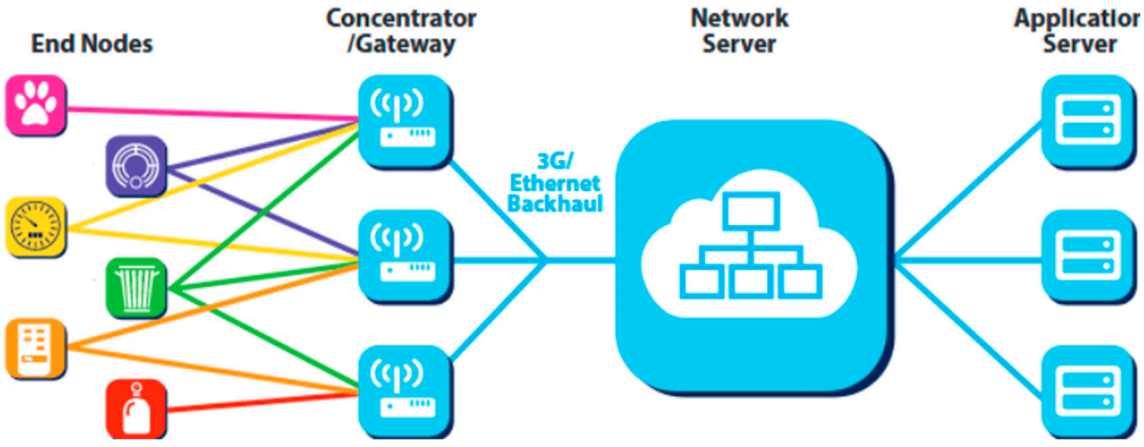

Figure 1. Lora Network (adapted from [24]).

This architecture exemplifies a scalable IoT solution where data is collected from various field devices (End Nodes), transmitted through an intermediate infrastructure (Concentrators/Gateways and Network Server), and finally utilized in specific applications (Application Servers). This approach ensures efficient data management and the ability to scale the network as needed.

 doi:10.20944/preprints202411.0254.v1

The frequencies used may vary depending on the region, as they are unlicensed, those being: 433 MHz and 868 MHz for Europe [24]. LoRa is highly efficient in terms of power usage, wireless data transfer and license-free sub-gigahertz radio frequency bands, which is why it is often used in IoT systems.

3.1. LoRa Basics

The LoRa network uses CSS Modulation, which is a spectral spreading technique. Spread spectrum techniques use a greater communication bandwidth than the original signal band to combat fading and shadowing problems. Fading can be originated in reasons like, signal strength variations (due to obstacles), reflections or interference and shadowing can be originated walls, hills or other objects blocking the signal and causing attenuation.

By spreading the signal, the impact of fading and shadowing will be minimized. Even if part of the spectrum is affected, other parts remain usable.

As written before the LoRa modulation technique (CSS) essentially consists of varying the frequency of a given wave. In chirp modulation, the frequency of the transmitted signal changes linearly over time. This allows LoRa signals to be robust against interference and noise. Frequency will increase linearly in the case of an up-Chirp and decrease in the case of a down-Chirp. Figures 2 and 3 show a graphical representation of this variation.

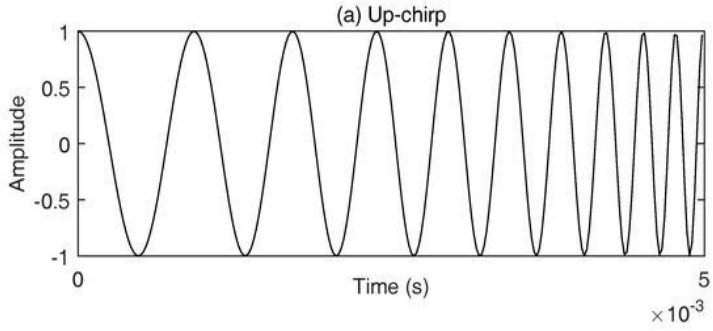

Figure 2. Graphical representation of an up-Chirp

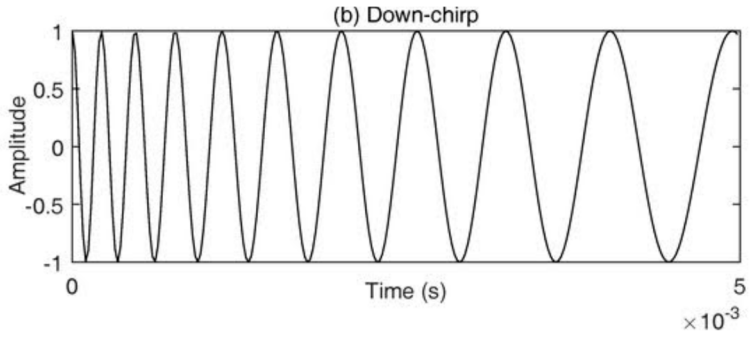

Figure 3. Graphical representation of a Down-Chirp.

Figure 4, below, shows the representation of an up-chirp for its frequency as a function of time.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

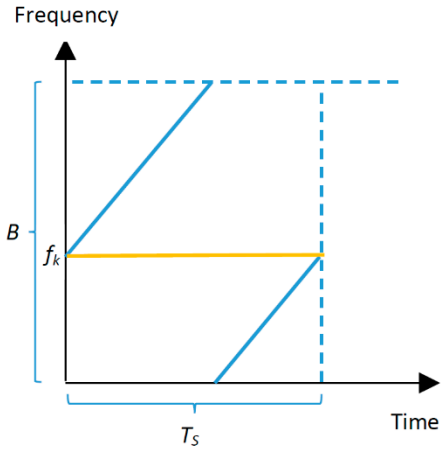

Figure 4. Representation of an up-chirp, where *B* represents the Bandwidth and *Ts* the symbol time (adapted from [25]).

By observing Figure 5 we can draw some conclusions about a chirp. There is an increasing, linear variation in frequency over time. Also, an interesting thing about chirps is that the maintenance of a constant bandwidth over their duration means that even as the frequency changes, the overall width of the frequency band that the chirp occupies remains the same. This property is quite important for the operation of a LoRa network and is one of the reasons why it's able to provide long-range communication with low power consumption.

When growth reaches the upper end of the frequency band (*fmax*), there is a "jump" to the minimum frequency end (*fmin*). The slope of these chirps (rate at which the frequency changes) is determined by the SF. A higher SF results in chirps with a slower slope, while a lower SF results in chirps with a steeper slope.

Looking at Figure 5, we can obtain the expression (1) for the bandwidth of this symbol,

$$BW = f_{max} - f_{min}[Hz] \quad (1)$$

Equation (2) below, shows that the symbol time depends not only on the bandwidth but also on the spreading factor (Figure 5).

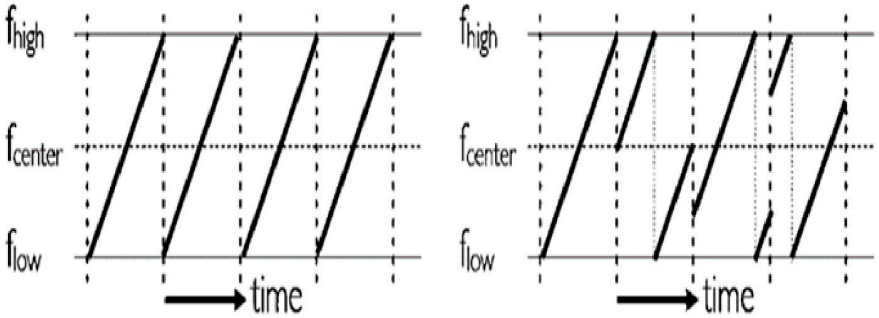

Figure 5. SF defines the number of bits that can be encoded by a symbol (at left an unmodulated signal and at right a modulated one) (adapted from [26]).

In the modulated signal of Figure 5 we could also see 4 symbols represented, each one having a time duration that we can further represent by *Ts*, and *Ts* can be expressed by [23]:

$$T_s = \frac{2^{SF}}{BW}[s] \quad (2)$$

This formula tells us that if the band is fixed the higher the SF the higher the symbol time. For example, if BW=125 kHz and SF=7 (7 bits in a symbol), *Ts* will be:

 doi:10.20944/preprints202411.0254.v1

$$T_s = \frac{2^7}{125000} = 0.001024[s], \text{ or } 1.024\ [ms]$$

To the same BW if the SF=9 the *Ts* will be:

$T_s = \frac{2^9}{125000} = 0.004096[s]$, or 4.096 $[ms]$ (4 times higher than the previous example)

Increasing *Ts* means the message transmission time (ToA) will also increase (and this way, bigger distances will be achieved). Furthermore, the number of chips per chirp is given by 2^{SF} [23]. The chip count is given by the development seen in [23]:

The symbol rate can be given by:

$$\mathrm{R_s} = \frac{1}{T_s} = \frac{BW}{2^{SF}}[symbols/s] \quad (3)$$

And 2^{SF} representing the number of chips per chirp [23].

As an example, being BW=125 kHz and SF=7, *Rs* will be:

$$\mathrm{R_s} = \frac{125000}{2^7} = 976{,}56[symbols/s]$$

So, if, as the example before, SF increases from 7 to 9, and the symbol time (*Ts*) increases by 4 times, it means the symbol rate *Rs* (being the inverse of *Ts*) will be reduced by 4 times.

The BW equals the chip rate, just changing the units (Hz per Chips/s) and the formula (3) could also be written in the form of:

$$\mathrm{R_s} = \frac{1}{T_s} = \frac{Rc}{2^{SF}}[symbols/s] \quad (4)$$

So, the chip rate is given by:

$$R_c = R_s * 2^{SF}[chips/s] \quad (5)$$

To note that the chip rate (*Rc*) is always higher than the Symbol Rate (*Rs*) because multiple chips can form one symbol.

Also, a very common term, is the chirp rate. The chirp rate (and like the chip rate) is also equal to the bandwidth, being measured in chirps per second (chirps/s). The difference is not in the numbers but in the definition: while the chip rate can be defined by the number of chips transmitted per time unit, the chirp rate will be defined by the rate of change of the frequency of a signal. This means that the chirp rate measures how quickly the frequency of the signal is changing at any given point in time. In Figure 5, and as an (illustrative) example, the slope of the spectrogram of each symbol can give us the chirp rate (rate of change of frequency).

One of the most important expressions in characterizing a LoRa signal is expression (6) [23], which correlates some of the most important factor's characteristic of signals from this technology.

$$R_b = SF * \frac{\left[\frac{4}{4+CR}\right]}{\left[\frac{2^{SF}}{BW}\right]}[bits/s] \quad (6)$$

where:

- R_b, bit rate (or data rate) [bit/s]
- BW, Bandwidth [Hz]
- CR, Code Rate (varies between 1 and 4)
- SF, Spreading Factor

This expression defines the nominal binary rate of a LoRa signal according to its CR, SF and BW.

 doi:10.20944/preprints202411.0254.v1

3.1.1. Spreading Factor

The SF is a parameter in the LoRa modulation scheme that affects the data rate, range, and processing time. A higher SF means a longer range and a lower data rate, while a lower SF means a shorter range and a higher data rate. The SF is one of LoRas most important parameters and essentially represents the speed at which a chirp changes frequency. For higher SFs we have a slower frequency change, which means that each chirp will also have a longer symbol time than signals with lower SFs.

Table 1 tells us that higher SF results in a higher number of chips per chirp (or a higher symbol count), and a lower SF results in a lower number of chips per chirp (or a lower symbol count). This implication takes to the conclusion that a higher symbol count (means a longer transmission time for each symbol) results in a lower data rate (Rs). On the other hand, a lower symbol count leaves to a higher data rate.

Table 1. Relationship between SF, Rs, chips per chirp and Rc, for a 125 kHz BW.

SF	R_s $[symbols/s]$	Chips per Chirp	$R_c[chips/s]$
7	976,56	128	125000
8	488,28	256	125000
9	244,14	512	125000
10	122,07	1024	125000
11	61,04	2048	125000
12	30,52	4096	125000

Another important factor to consider is the importance of SF for the data rate of a LoRa signal. In expression (6) we can see the direct implication this has on this output.

A key characteristic in LoRa is orthogonality. Orthogonality allows different Spreading Factors (SFs) to coexist in the same channel without interfering with each other. This is because different SFs result in different data rates, which in turn produce signals with different slopes (rate of change of frequency versus time) when viewed in the frequency-time plane. However, this orthogonality is not perfect. When the bandwidth is fixed, different SFs can cause packet loss if the interference power received is strong enough. This imperfect orthogonality can significantly deteriorate the performance, especially on the higher SFs. Moreover, there can be combinations of SF and bandwidth which would have the same slope as other combinations, and thus not be as fully orthogonal from them. This could potentially lead to more problems, especially when SFs are close to each other.

3.1.2. Code Rate

The CR refers to the ratio associated with error detection and correction for the Hamming code used by LoRa. The CR can take 4 different values: 4/5, 4/6, 4/7 and 4/8, and these ratios being equivalent to the H(5,4)...H(8,4) codes [23]. For the values 4/5 and 4/6 only error detection is possible, while for 4/7 and 4/8 its possible error detection and correction [25]. These ratios correspond to the number of data bits and the number of redundant bits for error detection, e.g. for a 4/5 CR, there are 4 data bits and 1 bit for error detection. For CRs with more redundant bits (i.e., decreasing of the coding rate), the bit rate will decrease in practical terms, since for the same binary output we can have a variable number of redundant bits and, consequently, a variable number of data bits [23].

Figure 6 shows that for CRs with a higher number of redundancy bits, the bit rate will decrease, as would be expected.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

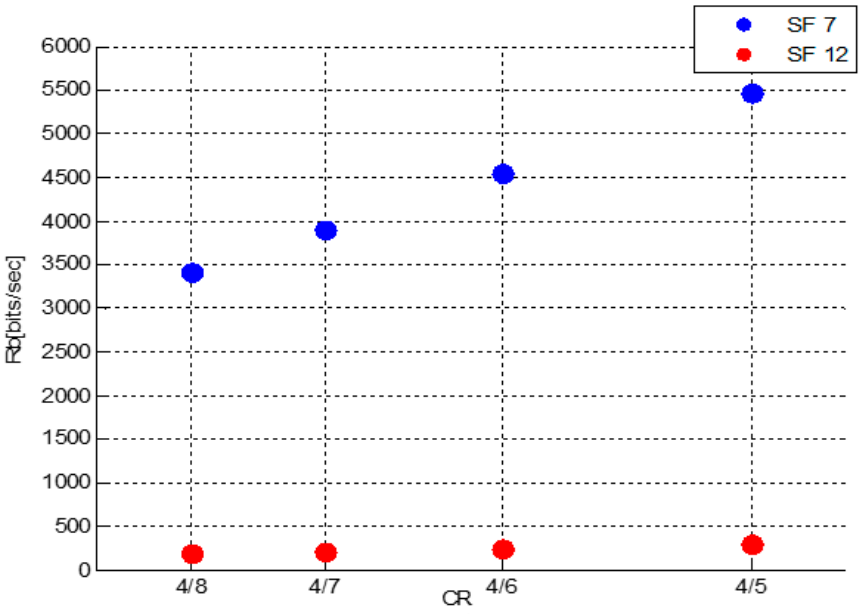

Figure 6. Bit rate according to SF and varying CR, for a bandwidth of 125 kHz.

Another parameter that was studied in the previous section is the SF, and again in this situation there are implications in terms of bit rate for higher SFs. A higher SF increases the signal's ability to resist interference (effectively increasing the range), but it also reduces the data rate. In this case we can once again see a much lower bit rate for a high SF, but it should be kept in mind that a CR of 4/8 when compared to one of 4/5 will also cause a considerable decrease in bit rate. A higher CR (more redundant bits) provides better error correction at the expense of data rate.

So, in a scenario where long range and robust error correction are needed, we might opt for a higher SF and CR, even though this would result in a lower data rate. On the other hand, if high data rate is the priority and the devices are close to each other, a lower SF and CR might be more suitable.

The choice of SF and CR will therefore depend on specific network communication needs.

3.1.3. Bandwidth

The BW used in LoRa can be 125 kHz, 250 kHz and 500 kHz (the latter not used in Europe).

Producing the graphical progression again based on the previous expressions, Figure 7 shows the graphical result of equation 6 for two different SFs.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

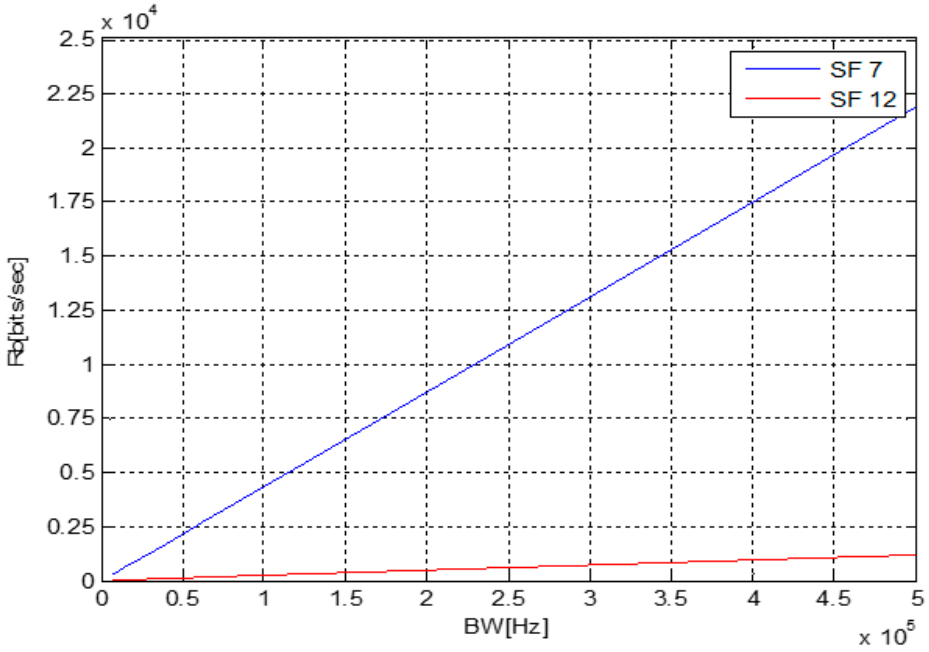

Figure 7. Bit rate to SF=7 and 12 and varying BW, for a CR of 4/5.

Looking at the graph in Figure 7, it's clear from the outset that when the bandwidth increases, the data rate of the link also increases. This means that a given amount of data can be transmitted in a shorter amount of time, reducing the ToA. A shorter ToA has several advantages. For one, it reduces the likelihood of the signal suffering from interference, as the signal is "on air" for less time and thus has less opportunity to collide with other signals. Additionally, effects such as fading or noise have less time to impact the signal, potentially improving the quality of the received signal. However, it's important to note that increasing the bandwidth also increases the potential for interference with other signals, as it requires a larger portion of the frequency spectrum. Once again, the correlation and impact that SF, CR and BW have on data rate becomes increasingly clear, as does the influence of each parameter on reducing the likelihood of the signal being affected by interference. If, on the one hand, an SF12 is used for communication over long distances, a high CR must be used so that the signal is more robust, the tradeoff being the fact that we have a lower binary data rate (which can be manipulated through the bandwidth used). Therefore, when choosing signal specifications for communication the balancing of these three parameters is crucial.

3.1.4. Frame format and Duty Cycle

LoRa uses a specific packet format (Figures 8 and 9) for data transmission [27].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

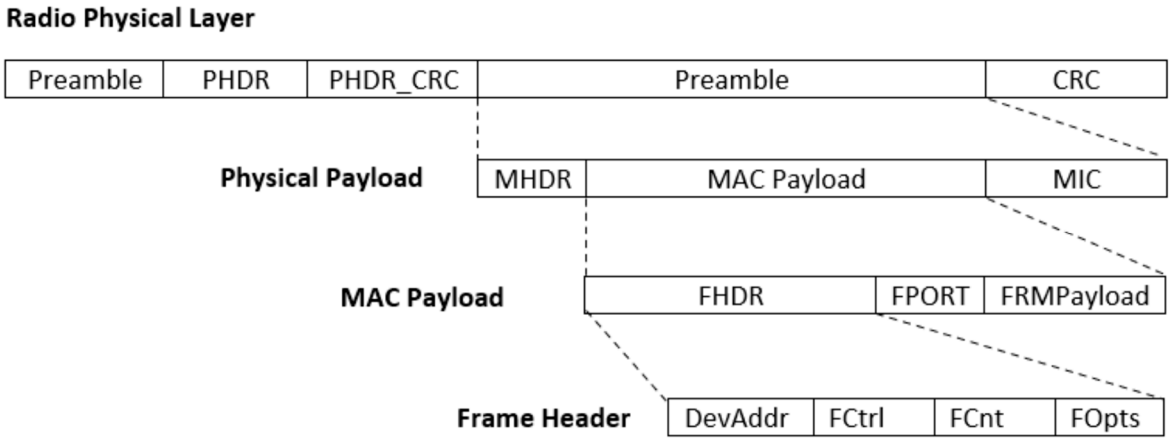

Figure 8. Fields of a LoRaWAN Data Message (adapted from [27]).

Figure 8 represents the structure of packets in LoRa and LoRaWAN communications.

In summary, the packet structure consists of the following components: Radio Physical Layer (Contains the Preamble, PHDR, and PHDR_CRC), Physical Payload (includes the MHDR, MAC Payload, and MIC), MAC (Payload: Consists of FHDR, FPort, and FRMPayload) and Frame Header (includes Comprises DevAddr, FCtrl, FCnt, and FOpts).

This structured approach ensures reliable and secure data transmission over LoRa and LoRaWAN networks, enabling effective communication for IoT devices.

There are two types of packet formats in LoRa: explicit and implicit. In explicit mode, a LoRa packet can be described as following:

- Preamble: Used to synchronize the receiver with the transmitter. It consists of 8 symbols for all regions, but the radio transmitter adds another 4.25 symbols, resulting in a final preamble length of 12.25 symbols.
- PHDR (Physical Header): An (optional) field that contains information about payload size and CRC (Cyclic Redundancy Check). It's only present in explicit mode.
- PHDR_CRC (Header CRC): An (optional) field that contains an error detecting code for correcting errors in the header.
- PHYPayload: Contains the complete frame generated by the MAC layer. The maximum payload size varies by Data Rate (DR) and is region-specific.
- CRC: An (optional) field that contains an error detecting code for correcting errors in the payload of uplink messages.

The PHDR and PHDR_CRC are encoded with the Coding Rate of 4/8, while the PHYPayload and CRC are encoded with one of the CR: 4/5, 4/6, 4/7, or 4/8. The complete frame is then sent using one of the SF 7 to 12).

In implicit mode, the header is removed from the packet where the payload size and Coding Rate are fixed or known in advance. Beacons use LoRa radio packet implicit mode for sending time synchronizing information from gateways to the end devices. As a resume, and comparing both, we can say that explicit mode is more flexible and robust with error detection but has additional overhead while implicit mode is more efficient with less overhead but requires fixed parameters.

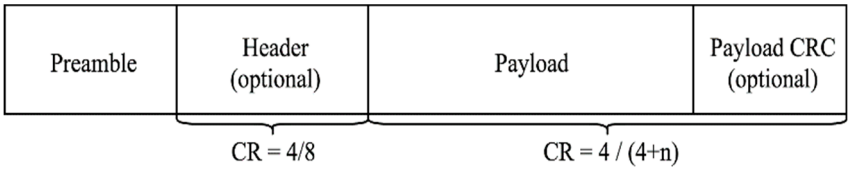

Figure 9. Structure of LoRa packet format with CR n ∈ {1..4} (adapted from [27]).

 doi:10.20944/preprints202411.0254.v1

Duty cycle is the fraction of time a device is busy transmitting data. A higher duty cycle means the signal is "on" for a larger portion of the total period which can result in longer frames. Longer frames take more time to transmit which impacts ToA. The time a packet takes to be transmitted at a given data rate, and this will be impacted by the size of the frames the devices send.

So, the impact of ToA [28] can be seen the following way:

- Data Rate: The data rate in LoRa is determined by the bandwidth, coding rate, and spreading factor. A lower spreading factor provides a higher bit rate for a fixed bandwidth and coding rate. Therefore, for a fixed amount of data (payload), a higher spreading factor (lower data rate) needs a longer ToA.
- Payload Size: The payload size directly affects the ToA. Sending a larger amount of data with a fixed bandwidth and spreading factor requires a longer ToA. This is because the data rate is fixed for a given bandwidth and spreading factor.
- Network Traffic: In a network with high traffic, a longer ToA could increase the risk of packet collisions, leading to packet loss.
- Interference: A longer ToA means the packet is in the air for a longer time, increasing the chance of interference from other signals.

The battery life of an end device is also affected by the ToA. Higher spreading factors result in longer active times for the radio transceivers, which means a longer ToA and consequently, a shorter battery life.

In Wireless Sensor Networks (WSNs), one of the major problems that can arise when using signals that are susceptible to interference is interference between them. This is because, depending on the duty cycle and ToA of each signal, there may be a temporal overlap. This overlap, for two signals susceptible to co-channel interference for example, could have catastrophic consequences for the quality of signal.

As seen for SF, the ToA of signals with high SFs is longer than for low SFs, meaning that it is potentially more susceptible to interference. In addition to the ToA, signals with higher SFs also have a longer time per symbol, which means that even with low duty cycles, the communication time for signals with high SFs will also be high. Bandwidth also affects time-on-air, which decreases with increasing bandwidth. In (7) we see the waiting time of a node, and how this is influenced by the duty cycle, δ.

$$T = ToA\left(\frac{1}{\delta} - 1\right) \tag{7}$$

In addition to the influence on energy efficiency, which is largely affected by the time a node is transmitting, there is also the problem of signal collision. Signal collision can occur at an elementary level for two reasons: temporal or frequency collisions. As you might expect, two (or more) signals being received at the same time (overlap) may lead to collisions and packet loss. However, thanks to the capture effect found in LoRa modulation, a packet received with a higher power level (at least 6 dB stronger) [29], can still be decoded during collision. This means that even if two packets (with the same SF) arrive at the same time, if one has a significantly stronger signal, it can still be successfully received due to this "capture effect", which allows the receiver to "capture" and successfully demodulate the stronger signal, while ignoring the weaker one.

3.2. RSSI and Signal-to-Interference Ratio (SIR)

The channel model of one of our experiments LOS from the end device node to the receiver can be based on the Friis formula (Free Space Path Loss – FSPL). Admitting ideal conditions (no obstacles), and with the antenna of the transmitter and receiver having directivity equal to 1 (isotropic antenna), we can say that:

$$\boldsymbol{FSPL} = \left(\frac{\boldsymbol{4\pi df}}{\boldsymbol{c}}\right)^{\boldsymbol{2}} \tag{8}$$

where d is the distance (meters) f is the frequency (Hz) and c is the speed of light (a constant). Converting this formula to dB:

 doi:10.20944/preprints202411.0254.v1

$$\boldsymbol{FSPL(dB) = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}\left(\frac{4\pi}{c}\right)} \quad (9)$$

A more precise expression can be found considering the gain of the antennas (transmission and reception) by saying that:

$$\boldsymbol{FSPL(dB) = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}\left(\frac{4\pi}{c}\right) - G_{tx} - G_{tr}} \quad (10)$$

Being $\boldsymbol{G_{tx}}$ the gain of the transmitting antenna and $\boldsymbol{G_{tr}}$ the gain of the receiving antenna. If the transmitter is emitting with a power of *Ptx* (expressed in mW), the RSSI will be:

$$\boldsymbol{RSSI = \frac{Ptx}{FSPL}} \quad (11)$$

Which, converted to dBm will result in:

$$\boldsymbol{RSSI(dBm) = Ptx(dBm) - FSPL(dB)} \quad (12)$$

For the scenario of NLOS with vegetation we will need to add to the *FSPL* another factor as vegetation introduces additional loss. A common model for vegetation loss is the ITU-R model [30], which can be approximated as:

$$\boldsymbol{L_v = A.d^B} \quad (13)$$

Being $\boldsymbol{L_v}$ the total loss due to vegetation (dB), *A* an attenuation factor depending on the type and density of vegetation (a constant that represents the specific attenuation rate, dB/m), *d* (m) the depth of the vegetation and *B* a frequency dependent exponent (an exponent that adjusts the relationship between distance and attenuation). Typical (empirical) values for *A* and a cedar with high density of leaves can be considered around 0,2 to 0,3 [30]. For a frequency of 868 MHz, the B factor in the ITU-R vegetation loss model typically ranges around 0.4 to 0.5. This value can vary depending on the specific type and density of vegetation, as well as other environmental factors [31]. The ITU-R model provides a general framework, but empirical measurements are often necessary to obtain precise values for specific vegetation types.

Total path loss would be then:

$$\boldsymbol{PL_{total} = PL_{FS} + PL_{Veg}} \text{ (dB)} \quad (14)$$

The same way for the scenario of NLOS with a concrete wall we would have:

Total path loss:

$$\boldsymbol{PL_{total} = PL_{FS} + PL_{Wall}} \text{ (dB)} \quad (15)$$

Typical values for standard concrete walls vary from 10 to 15 dB (depending on the thickness and material composition of the wall) for an 868 MHz frequency [32].

More accurately and looking for the typical urban scenarios, models like the Rice fading (often a good choice if there is a clear LOS path) can be seen applied in works like [29] [33].

For situations of NLOS we need to include the expected vegetation (can cause path loss due to absorption, reflection, and scattering) and wall loss (create shadowing effects and can significantly reduce signal strength) and this type of scenarios could be seen explored in [33]. Models like Nakagami-m fading [29] (provides flexibility and can be tuned to match the specific conditions if the environment is more complex with significant obstacles) or Log-normal shadowing (accounting for large-scale variations in signal strength due to obstacles) are usually applied. Yet, the application of this model was not the focus of our work.

Another very important variable to understand the reliability of our link and the influence of interference it's the SIR and it can be expressed by the following formula:

$$\boldsymbol{SIR = \frac{RSSI}{I}} \quad (16)$$

where *I* is the aggregate interference (random variable) of the SFs that are interfering over the packets. As was study by Goursaud and Gorce [34] a packet that arrives with higher signal strength than the

 doi:10.20944/preprints202411.0254.v1

lowest limit of the receiver sensibility can still be lost due to interference of other packets either from other end devices or either from the same end device (if packets were sent in the same channel with different SFs and different payload sizes). The tolerance to this interference will depend on the SFs chosen between packets, being one (or more) be considered the interfering packet. The SIR (Table 2) presented can be used to understand if the packet was successfully received or not:

Table 2. SIR Margin for all combinations of SF – for the desired and interferer user (data from [17]).

Interferer SF	7	8	9	10	11	12
Desired SF						
7	-6	16	18	19	19	20
8	24	-6	20	22	22	22
9	27	27	-6	23	25	25
10	30	30	30	-6	26	28
11	33	33	33	33	-6	29
12	36	36	36	36	36	-6

The values of Table 2 can be read this way: Imagining that two packets (packet 1 and packet 2) with the same SF arrive at the same time at the receiver. The receiver will still be able to be demodulated if one (e.g. packet 1) is 6 dB higher than the other. For example:

Packet 1: RSSI= -100 dBm,

Then for the packet 1 can be demodulated the RSSI of the "interfering packet" (packet 2) must not exceed:

-100-6=-106 dBm

For the cases that different SFs were transmitted (our scenario) and imagining a package transmitted with SF=12 (at a longer distance) and received with RSSI=-100 dBm an interfering packet with SF=9 (at a shorter distance and received at the same time) cannot exceed:

-100-(-25) =-75 dBm, for the package with SF=12 be corrected received and demodulated.

This way the implementation of higher SFs for more distant end devices, concerning the noise sensitivity (and RSSI) will allow to overcome the impact of closer devices that are more susceptible of receiving signals with higher signal strength. Yet, the study of [34] are not much clear about in what conditions these values were achieved, and works like of [14], have reduced these values in a very significant terms, leading this quasi-orthogonality to be even more imperfect.

A more precise representation of the channel conditions can be achieved by using the SINR, because SINR will add the noise floor of the channel to the aggregate interference used by SIR. In our case and considering the channel conditions, we will consider SIR≈SINR, considering this way that the noise power is much lower than the signal power and the interference is significantly stronger than the background noise.

4. Collision Management and MAC Protocols in IoT Networks

Operating an IoT system in unlicensed Industrial, Scientific and Medical (ISM) bands, on the one hand, reduces the cost of license fees, on the other hand, we are forced to share the spectrum which causes an inevitable increase in interference as new devices are added and limits the maximum duty cycle which in EU 868 ISM is 1%. This issue has been addressed in some studies, where broadband measurements (200-3000 MHz) were carried out in urban environments in 2016 and it was observed that compared to 2004 data, the average spectral occupancy has increased considerably, which means the emergence of a multitude of new radiation sources.

There is also a problem of possible electromagnetic interference affecting IoT networks that occurs in the access between sensors and access points (AP). When it comes to LoRa, two sources can be identified, LoRa signals and other signals that use the spectrum. In the first case, it occurs during the simultaneous transmission of two or more LoRa devices with the same transmission parameters, a function that defines the chirp signal, bandwidth and spreading factor. In this case, the individual chirp signals would not be mutually orthogonal, making it impossible to differentiate between the

 doi:10.20944/preprints202411.0254.v1

transmissions at the receiver. In the second case, as these signals are from sources outside LoRa, they become even more unpredictable and more difficult to control.

As mentioned earlier, LoRa is based on CSS technology where chirps are used to transmit information. The spreading factor is the variable that controls the chirp rate and in turn the data transmission speed, which varies between SF7 and SF12. Thus, for higher spreading factors, we have higher coverage distances because the processing gain is increased and the data rate decreases, allowing us to receive a signal with fewer errors compared to a lower factor. This factor also affects the ToA, which increases as the SF increases and so does the probability of collisions. Another very important factor that is affected by SF is battery life, which in these types of networks is essential to consider and which, when larger SFs are used, increases transmitter uptime and in turn reduces battery life. By being able to manipulate this factor, we can design a network that can adapt to various end device usage scenarios. Another feature of this factor is traffic control, which is possible due to its orthogonality, allowing modulated signals with different spreading factors that are on the same frequency at the same time not to interfere with each other.

4.1. Collisions and Interference in LoRaWAN

In LoRaWAN, the spreading factor can cause two types of interference: intra-SF interference and inter-SF interference. Detailing:

- **Intra-SF interference** may occur when more than one end-devices transmit with the same SF on the same radio resource (bandwidth and channel frequency) and overlap in time and frequency. A received signal can be demodulated properly if the Capture effect happens [11]**.**
- **Inter-SF interference** may occur when transmissions using different SFs overlap in time and frequency. The signals with a lower SF (higher data rate) can interfere with the signals with a higher SF (lower data rate), leading to packet loss [11].

In LoRaWAN, frames collide due to various factors. A collision can be said to occur when two frames appear at the same time and the receiver is unable to process them or the channel is busy, and a sender sends a frame. Due to the time delay between sending and receiving the frame, a problem is created in accessing the medium in communication networks. When collisions occur in wireless networks, the information sent in these frames will collide and mix resulting in noise, so that it cannot be recovered unless the receiver can filter out the desired information. In cases where this filter doesn't exist, the sender needs to resend the information until it is successfully delivered, which causes a major problem for the network when thinking on a large scale. However, there are various techniques for dealing with this problem, some of which select a random resend time when collisions are detected, others which test the medium to check that the receiver is listening and free before transmitting.

CSS allows packets with different SFs to be transmitted simultaneously on the same channel without interfering with each other, a feature known as orthogonality. However, this orthogonality is not perfect in real-world conditions, and packets with different SFs can interfere with each other under certain circumstances, leading to packet loss.

So, while LoRa technology is designed to minimize packet collisions and loss using different SFs and CSS modulation, it's not immune to these issues.

Also, in LoRaWAN, frame collisions can occur when several packets overlap in time and use the same sending parameters, such as SF, bandwidth, and carrier frequency. When many devices use the same configuration, the probability of a collision is higher. In addition, the selection of SF and transmission power influences the coverage area and, due to signal attenuation and distance, some packets might not collide. The probability of packet collisions is also affected by the periodicity of the transmission size and the size of the data.

Packet loss in LoRaWAN can have several impacts:

- Data Integrity: Packet loss can lead to incomplete or incorrect data being received, which can affect the integrity of the data. This is particularly problematic in applications where accurate data is critical, such as health care applications.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

- Network Efficiency: Packet loss can reduce the efficiency of the network. When packets are lost, they often need to be retransmitted, which uses additional network resources and can lead to congestion.
- Latency: Packet loss can increase latency, as lost packets need to be detected and retransmitted. This can be problematic in applications that require real-time data, such as control systems.
- Application Performance: Depending on the application running on top of the LoRaWAN, packet loss can have varying degrees of impact. For example, in a temperature monitoring application, occasional packet loss might be tolerable, but in a fire alarm system, every packet is critical.

Retransmission of lost packets can also increase energy consumption, which is a significant concern in IoT networks where devices are often battery-powered and expected to operate for long periods without recharging.

To mitigate the impact of packet loss, LoRaWAN often employs various strategies such as error correction codes, packet acknowledgment schemes, and Adaptive Data Rate (ADR) mechanisms. However, it's important to note that no network can eliminate packet loss, and the goal is often to manage it to an acceptable level given the specific requirements of the application and network.

4.2. MAC Protocols

One of the main topics of our project is to study collisions in LoRa communications, so medium access protocols are essential to understanding how they work and in which scenarios they occur. Medium access protocols are protocols that operate at the Medium Access Control (MAC) layer and allow several users to access a shared network, with the aim of optimizing transmission time and minimizing collisions (Figure 10).

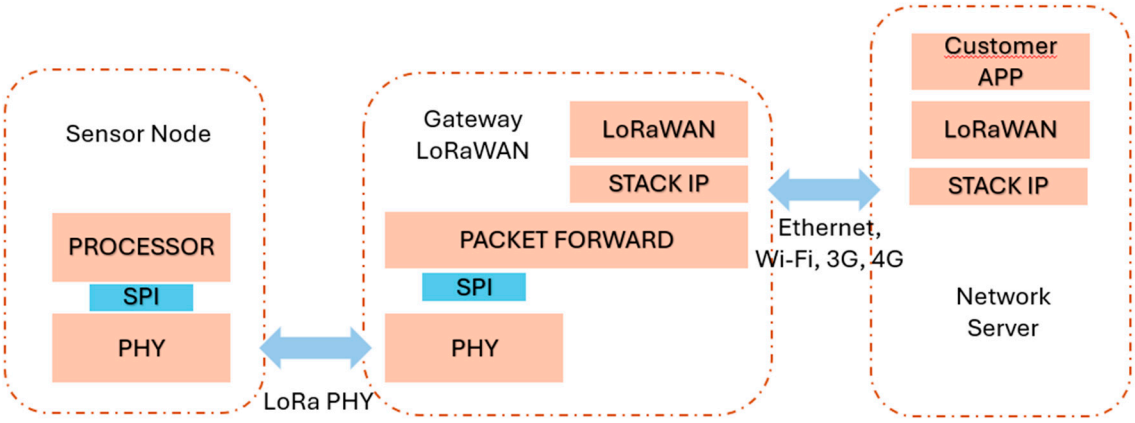

Figure 10. MAC protocol schematic (adapted from [24]).

These protocols can be categorized as random and controlled, and in this experimental study we will study random protocols and specifically Pure ALOHA. Among some of the main characteristics of a randomized protocol are that it does not have a time restriction for sending data (devices can attempt to transmit whenever they have data to send, without waiting for specific time slots) and the number of active stations transmitting data is not fixed. Multiple stations will contend for access to the shared communication channel.

4.2.1. ALOHA Protocol

In this experiment we're going to use an end node device that implements the ALOHA access protocol, using the LMIC libraries. The LMIC library provides a complete LoRaWAN Class A and Class B. This library is intended to be used with plain LoRa transceivers, connecting to them using SPI (Serial Peripheral Interface) protocol. In particular, SX1276 LoRa transceiver.

ALOHA is a random multiple access protocol which, to solve the problem of collisions, implements the logic of transmitting a packet immediately, without any detection of the medium (for

 doi:10.20944/preprints202411.0254.v1

example CSMA), and if no ACK is returned, a retransmission will be made after a random waiting time. There are two variants of this protocol, Pure ALOHA [35] and Slotted ALOHA [36].

The version of the protocol that is now called Pure ALOHA is a simplified version of the original ALOHAnet. This protocol works on the basis that if there is data to be sent, it is sent and if, while transmitting, data is received from another station, a collision has occurred. In this scenario, all the stations will try to retransmit the later one. It should be noted that as this protocol does not detect the availability of the medium, there will be collisions and therefore the need for retransmissions, which means that ALOHA cannot utilise the full capacity of the communication channel. Therefore, the most important aspect of this protocol that determines its quality and efficiency is the backoff scheme chosen.

For this to be efficient, a scheme must be chosen which aims to achieve maximum throughput, which adapts easily to changes in traffic intensity and the number of active stations, and which can be applied to both Pure ALOHA and Slotted ALOHA. Let's see some differences between them:

Pure ALOHA:

- Allows any station to transmit data at any time without synchronization.
- Collisions occur, and colliding frames are destroyed.
- Feedback informs stations if their frames were successfully transmitted.
- Maximum Efficiency: 18.4%

Slotted ALOHA:

- Divides time into discrete intervals called slots, each corresponding to a frame.
- Stations synchronize transmissions and transmit data only at the beginning of each slot.
- This approach reduces collisions and improves overall efficiency compared to unslotted (Pure) Aloha.
- Maximum Efficiency: 36.8%

Resuming, in Pure Aloha, the higher collision probability leads to lower efficiency compared to Slotted Aloha. Slotted Aloha's synchronization reduces collisions and improves overall performance of the network.

LoRaWAN is like Pure ALOHA but allows for variable packet lengths, unlike ALOHA. A key difference is that Pure ALOHA detects collisions after transmission and uses a simple retransmission strategy. In contrast, LoRaWAN employs a spread spectrum technique, which reduces the likelihood of collisions by spreading the signal across a wide frequency range. This leads to greater energy efficiency compared to Pure ALOHA, as fewer retransmissions mean less energy consumption, allowing battery-powered devices to operate for extended periods. The use of spread spectrum in LoRaWAN complements therefore the MAC layer protocols by enhancing signal robustness and reducing interference. Both ALOHA and LoRaWAN detect collisions and use retransmissions, but they operate at different layers and use different techniques to achieve their goals.

5. Results and Discussion

In this section we will describe the specific experimental environment and methods and provide a discussion of the results.

5.1. Hardware Used in This Experimental Study

The hardware used (Figure 11) was: LG02 Dual Channels LoRa Gateway [37], LoRa Bee SX1276 [37] and Arduino UNO REV3 [38].

The LoRa Bee module consists of an SX1276 transceiver, which allows the user to send data. This module enables transmission in multiple modes, working at a frequency of 868 MHz, thus supporting the LoRa networks spread spectrum technology and supporting I/O voltage values of 3.3V. The Sensitivity of this module can be seen in Table 3.

 doi:10.20944/preprints202411.0254.v1

Table 3. RF Sensitivity (dBm) of the SX1276 considering SF and BW [39].

SF	7	8	9	10	11	12
BW						
125 kHz	−123	−126	−129	−132	−133	−136
250 kHz	−120	−123	−125	−128	−130	−133
500 kHz	−116	−119	−122	−125	−128	−130

The LoRa Bee module was working in a class A operational mode (base class for all LoRa devices). Class A devices support bi-directional communication, but the downlink (server to device) communication must follow an uplink (device to server) communication from the device. This means the server can only send data to the device when it's expecting to receive it, which is a short window after it sends data. Some key characteristics of a Class A end device:

- Uplink Transmission: A Class A device can send an uplink message at any time. The uplink slot is scheduled by the end device itself based on its need.
- Downlink Transmission: Once the uplink transmission is completed, the device opens two short receive windows for receiving downlink messages from the network. There is a delay between the end of the uplink transmission and the start of each receive window, known as RX1 Delay and RX2 Delay, respectively.
- Low Power Consumption: Class A end devices have very low power consumption. Therefore, they can operate with battery power. They spend most of their time in sleep mode and usually have long intervals between uplinks.
- High Downlink Latency: Class A devices have high downlink latency, as they require sending an uplink to receive a downlink.

The LoRa Bee module has been connected to the Arduino (SPI connection), enabling long-distance communication, and guaranteeing good connection stability and consistency. It has encryption algorithms that prevent data from being intercepted and compression algorithms that allow small data to be transmitted, making the process faster and more efficient, thus providing good sending reliability.

The LG02 is a two-channel LoRa Gateway. It allows the LoRa network to be connected to Wi-Fi, Ethernet, 3G and 4G. This gateway can support the LoRaWAN protocol and uses the same transceiver module (SX1276) to communicate with the node. The computational design of the LG02 is done using Linux, which allows the LoRa to work in full duplex LoRa mode and increase communication efficiency.

The LG02 gateway can support various modes, such as: LoRa repeater mode, MQTT mode, TCP / IP client mode, TCP / IP server mode. This equipment is often used to extend the signal to other devices on a LoRaWAN or Wi-Fi network.

The LoRa gateway has been registered and configured in the The Things Network (TTN) [40], as has the end device (Arduino with LoRa Bee).

 doi:10.20944/preprints202411.0254.v1

Figure 11. Hardware for experimental experience.

5.2. Experimental Test Scenarios

In our study we have created a scenario of inter-SF interference, transmitting sequentially packets of different sizes and different SFs, (pseudo) randomly. The goal was to create a real scenario of having several devices transmitting different types of information at different distances in a way that packets could overlap, leading to a scenario of high probability of packet losses. Different fading propagation conditions were also created tested in a way that we could study the implication of the signal strength (evaluated by RSSI) in the reliability of our link for this scenario conditions, and the implication of possible SIR reduction when comparing the LOS and in a the NLOS scenarios (leading to an increase in probabilities of inter-SF interference). The impact of the payload size on the choice of the best spreading factor for each of the conditions tested was also analyzed.

We strategically selected positions for both the gateway and the LoRa module to evaluate various factors affecting our communication link. These factors included vegetation, obstacles, building features, distance between the gateway and module, and LOS versus NLOS connections at different distances. Testing with both natural (trees) and man-made (concrete walls) obstructions helped us understanding how different materials and structures impact the communication performance. The GW was installed at the window of a two-story building, 5 meters high, while the ED was positioned on the street at a height of 1.5 meters. The ED was moved to create initial LOS scenarios at distances of 20, 40, and 60 meters. Subsequently, NLOS scenarios were tested: first with a cedar tree obstructing the view, and later by placing the ED behind a concrete wall to introduce this type of obstacle between the devices, specifically for the 60-meter distance.

Our testing approach involved the following:

1. Distance Testing, SFs and Payload Sizes**:**
   - Distances tested: For LOS, 20, 40, and 60 meters. For NLOS only 60 meters.
   - SFs: 7, 9, and 12.
   - Varied payload sizes: 14, 32, and 51 bytes.
2. Scenarios:
   - LOS Scenario:

 doi:10.20944/preprints202411.0254.v1

- Initial test at 20 meters with both devices in line of sight.
- Tested SF7, SF9, and SF12.
- Assessed impact on signal strength and quality.
- Extended Distance (LOS):
- Repeated tests at 40 meters with line of sight.
- Assessed impact on signal strength and quality.
- Further Extension (LOS):
- Increased distance to 60 meters with line of sight.
- Tested SF7, SF9, and SF12.
- Assessed impact on signal strength and quality.
- NLOS Scenarios:
- Vegetation Obstruction:
- Tested at 60 meters without line of sight and vegetation.
- Compared results with LOS scenario.
- Concrete Wall Obstruction:
- Tested at 60 meters with a concrete wall obstructing the signal.
- Assessed impact on signal strength and quality.

By analyzing these scenarios, we aimed to understand how distance, payload size, and interference affect LoRa packet transmission for the several SFs tested. We also compared LOS and NLOS scenarios to assess signal quality and strength.

5.3. LOS Results

In this first scenario, the configurations used are summarized in Table 4.

Table 4. LOS scenario settings.

SF	7,9,12
Distance	20, 40, 60 m
Emitting Power	8 dBm
Frequency	868.2 MHz
Data size	14, 32, 51 bytes
Code Rate	4/5
Bandwidth	125 kHz
Duty Cycle	1%
Time between messages	1 s

We began by studying the influence of the payload size for each SF on the received signal strength (where RSSI indicates the level of the received signal strength), and the relationship of a given chosen SF (with a certain payload size) in ToA. The gain of the antenna of the transceiver SX1276 was 1.5 dBi and for the LG02 the same. Figures 12–14 show the scenarios described in Table 4. GW was positioned at the window of the building at a height of 5 meters, while the ED was placed on the other side of the street, either on the sidewalk at distances of 20 and 40 meters (both at a height of 1.5 meters), or in the parking lot at a height of 1.5 meters and 60 meters.

 doi:10.20944/preprints202411.0254.v1

Figure 12. LOS scenario at 20m (GW at the window of the building and ED at the other side of the street in the sidewalk).

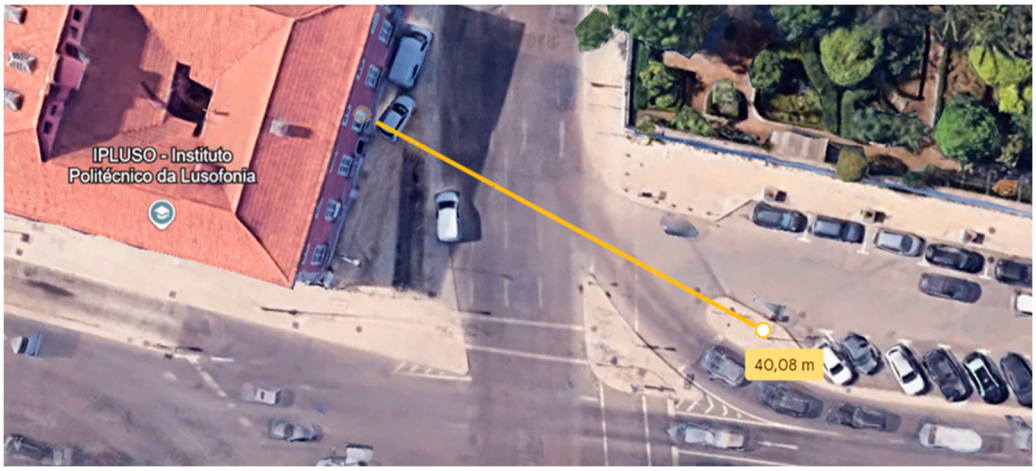

Figure 13. LOS scenario at 40m (GW at the window of the building and ED at the other side of the street in the sidewalk).

Figure 14. LOS scenario at 60m (GW at the window of the building and ED at the other side of the street in the parking lot).

Figures 15–17 show the direct results taken from measurements under these conditions. To note that from the 10 packets sent, some of them had very similar values, that's why some "dots" are not seen.

 doi:10.20944/preprints202411.0254.v1

As expected, the larger the SF used, the greater its ToA (symbol time is directly proportional to SF and the higher the symbol time the higher the ToA).

In terms of RSSI, we can see that, for the same distance, different SFs, and payload sizes we have at:

- **20m**: Highest value for Sf=7 with 14 Bytes (-63 dBm). Lowest for (also) SF=7 and 51 Bytes (-91 dBm).
- **40m**: Highest value for SF=9 with 51 Bytes (-74 dBm). SF=12 with 51 bytes also achieves a good result at this distance (-76 dBm). Lowest for SF=7 with 51 Bytes (-106 dBm). Yet this value it's just for one packet. In all the other 9 the worst value was -89 dBm.
- **60m**: Highest value for SF=7 with 32 Bytes (-82 dBm). Lowest for both SF=9 with 12 and 32 Bytes (-106 dBm).

It's revealing that the payload size has quite an impact on the RSSI. At 20m and for the same spreading factor, SF=7, having a difference of 28 dB (-63-(-91) =28) between the best packet (14 bytes) and the worst (51 bytes) is quite a lot. The best values for SF=7 and 14 Bytes are not so different (-63 dBm) of the best values of SF=7 and 51 Bytes (-74 dBm) but the worst packets of each payload size can be 23 dB (-68-(-91) = 23) down, for the worst case.

Looking for the distance of 20 meters and considering payloads with just 14 bytes, the SF=7 at 20 meters has the best performance, while for 32 and 51 bytes the SF=9 would be the better choice.

In the distance of 40 meters and making the same considerations the SF=7 will have better performance for payloads sizes of 14 bytes while for packets with 32 and 51 bytes, SF=9 perform better.

Looking for the distance of 60 meters we have some mixed results. For 14 bytes SF=7 and 9 are quite similar (with the slightest advantage for SF7), while for 32 and 51 bytes, SF=7 performs better.

Considering just each one of the spreading factors, for the 3 distances tested and for the different payload sizes we achieved the following results:

- **SF7** has the best result of RSSI for 14 bytes at 20 meters (-63 dBm) and the worst for 51 bytes at 60 meters (-95 dBm).
- **SF9** has the best result for 32 bytes at 20 meters (-67 dBm) and the worst for 32 bytes at 60 meters (-106 dBm). Yet this value is just for one packet while the worst of the other 9 packets was -96 dBm.
- **SF12** has the best result for 20 meters (-73 dBm) and payload of 51 bytes and the worst for 14 bytes at 60 meters (-106 dBm). Yet, 8 of the 10 packets were higher than -102 dBm.

From here we can consider that SF7 perform quite well for the shortest distance (20 meters) and for the smallest packet sizes tested (14 bytes), while SF9 at 20 meters and 40 meters and for the packets size of 32 and 51 bytes is the best option. SF12 for the longest distance (60 meters) and for the smallest packet (14 bytes) have the worst performance.

Some more insights: Among the several distances tested, the difference between the highest value (-63 dBm for SF=7 (14 Bytes) at 20 meters) and the lowest (-106 dBm for SF=12 (14 bytes) at 60 meters) is of 40dB, which reveals quite a big difference between this two different SFs (7 and 12) and makes us consider the right choice of the SF for this conditions critical (e.g. the SF7 for 60m have the his highest value=-82 dBm (at 32 bytes) and the lowest -95 dBm (at 51 bytes) . And in this case, we have a difference of 13 dB.

On other hand and considering that at different distances, different SFs might be sending packets received by the gateway, inter-SF interference must be considered. If we consider that for 20 meters an SF7 will be the logical choice, signals with an RSSI between -63 and -68 dBm would be arriving at the gateway. If a more distant node with SF9 is sending packets to the same gateway, in our case we would have values of RSSI between -77 dBm and -83 dBm for 40 meters or -86 to -96 dBm in the case of the same SF9 to 60 meters. Observing the values in Table 2, if a desired packet with SF9 is arriving at the same time as a packet with SF7, for the SF9 packet to be demodulated successfully, a separation of at least 27 dB would need to be guaranteed between the RSSI signals from the two different FS. And it's far from that. Thus, we are facing a scenario of probable inter-SF interference and packet loss.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

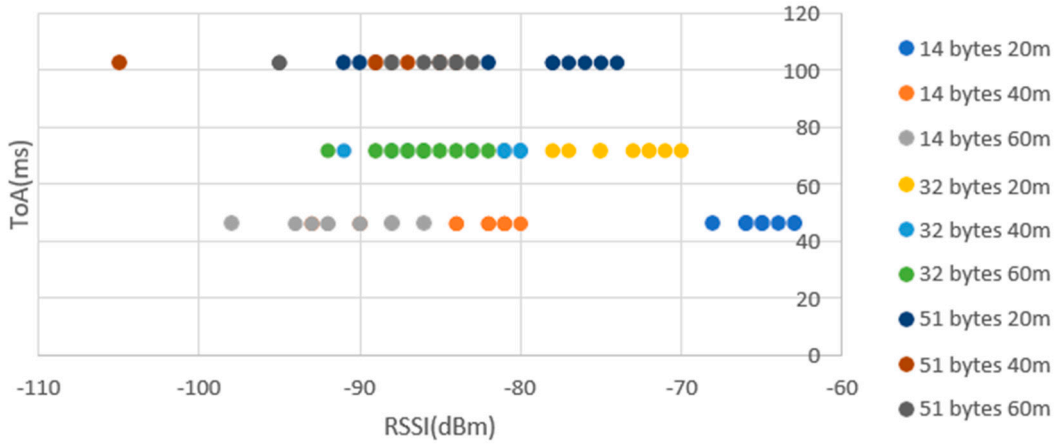

Figure 15. Influence of the payload size (for SF7) on ToA and on the RSSI (aggregated by payload size).

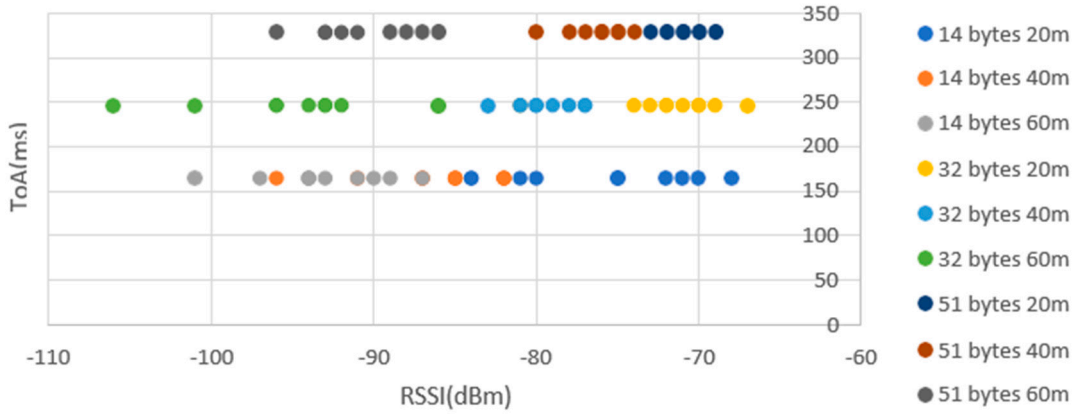

Figure 16. Influence of the payload size (for SF9) on ToA and on the RSSI (aggregated by payload size).

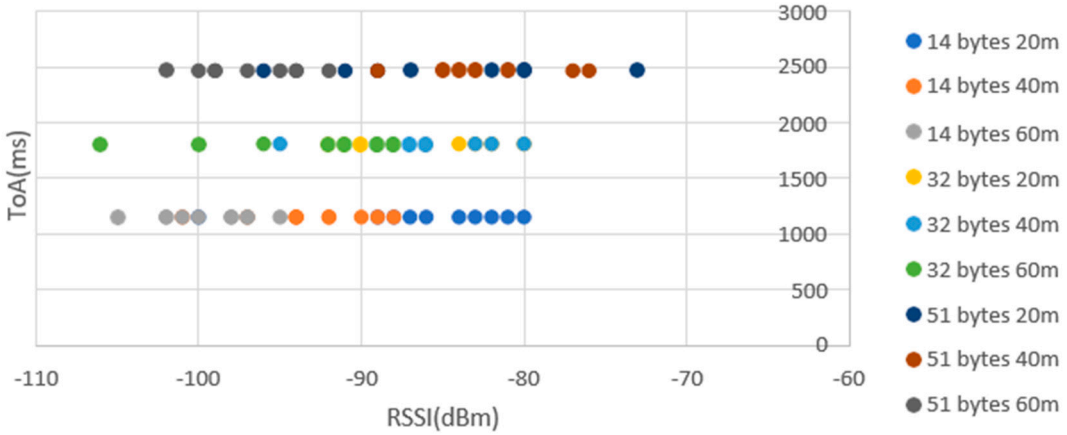

Figure 17. Influence of the payload size (for SF12) on ToA and on the RSSI (aggregated by payload size).

Next, we have studied, more, the impact of the choice of SF for different file sizes on their ToA. The results obtained were in line with the expectations, and with increasing SF, ToA increases considerably. In relation to the impact of file size, ToA is also greater and grows proportionally, as

 doi:10.20944/preprints202411.0254.v1

can be seen in Figure 18. A very important factor in the choice of SF is the fact that the larger the SF used, the greater the ToA, (which can lead to more collisions as the channel is occupied for longer).

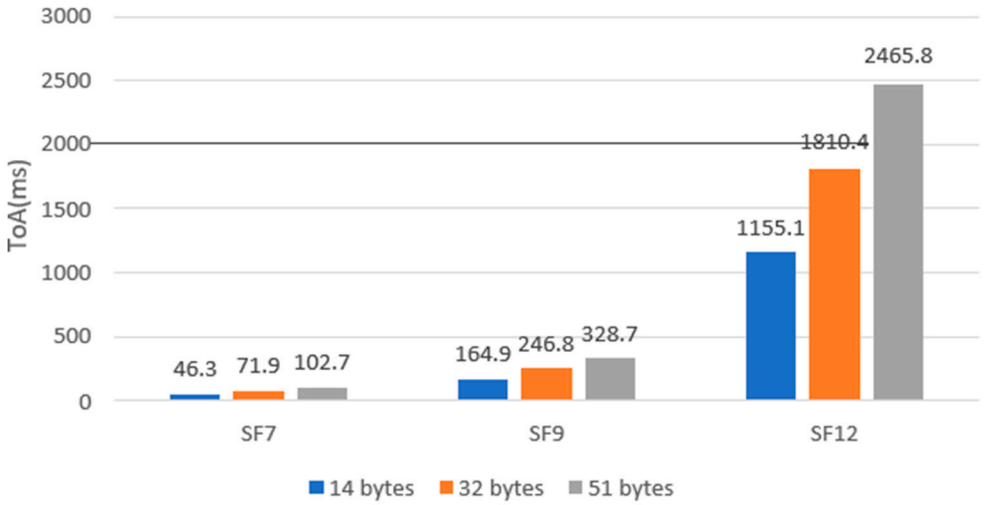

Figure 18. ToA according to SFs and data size.

Figures 19–21 make a graphical resume of what has been said about the values of RSSI for different SFs, payload sizes and distances. RSSI according to different data size and different distances for SF7/9/12.

In the case of SF7 (Figure 19), we can see that for the 20 meters, as the file size increases, the quality of the connection decreases, since the power received is lower. For the 40 and 60-meters cases, the connection quality is lower than for 20 meters, but the values of RSSI are more stable.

In SF9 (Figure 20), we obtained the more balanced results for the three scenarios tested since the quality of the connection is very stable. This could be a viable solution for a scenario where you want to send packets of various sizes, and you need signal stability.

For SF12 (Figure 21), at distances of 20 and 40 meters, the quality of the connection improves as the file size increases and its value converges at 51 bytes, while at 60 meters the value oscillates between -98 and -90 dBm.

Thus, and reaffirming what was said before, given that for medium-distance connections (40 meters), the use of SF9 is ideal and with the variation in file size there is only an oscillation of at least. In the case of the SF7 measurement, the impact of varying the file size is noteworthy, even if for larger files (and distances) the quality of the connection doesn't vary much, which can lead to very interesting optimizations. SF12 is also quite stable for the two bigger file sizes tested. We were also able to conclude that larger SFs can handle larger files.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

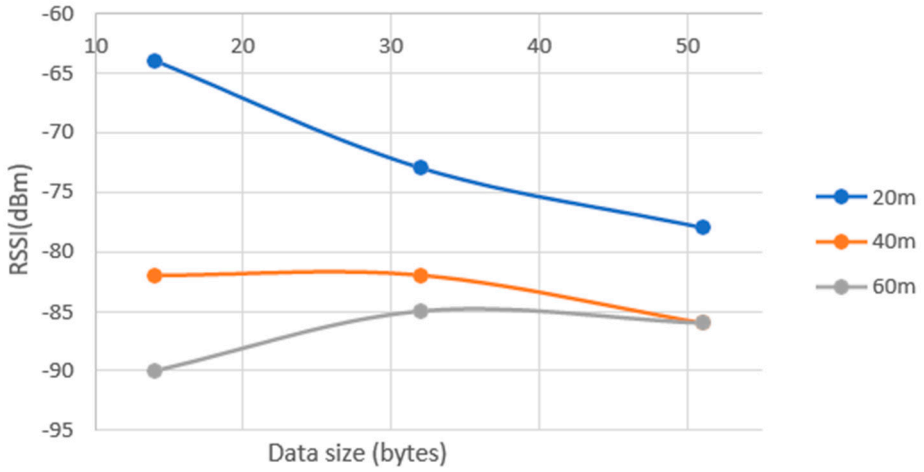

Figure 19. Average RSSI according with payload lengths and different distances for SF7.

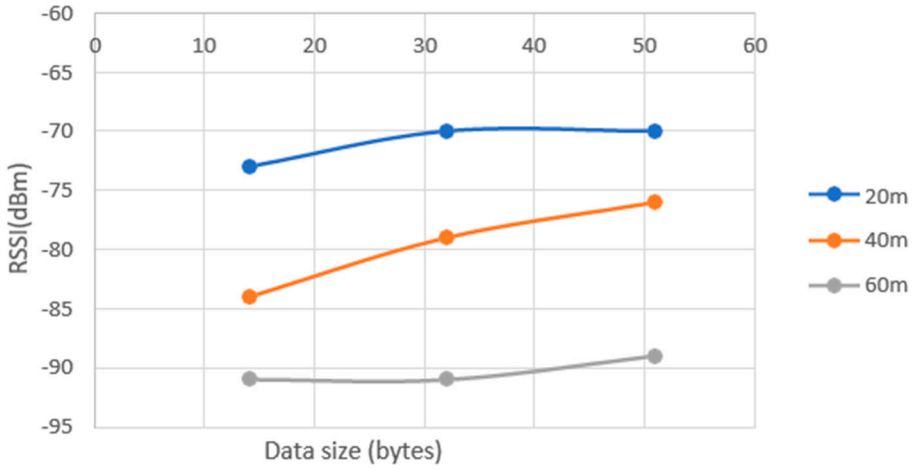

Figure 20. Average RSSI according with payload lengths and different distances for SF9.

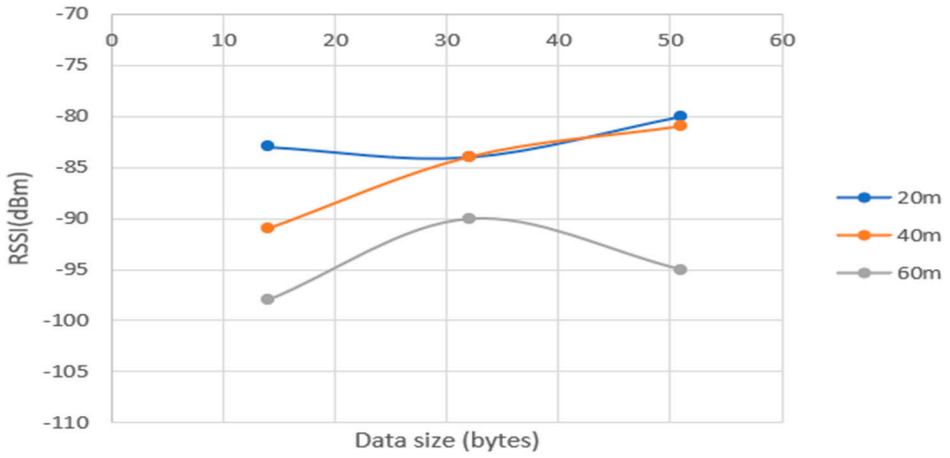

Figure 21. Average RSSI according with payload lengths and different distances for SF12.

Then, we investigated the possibility of packet loss for various values of SF, payload sizes, and distances. Even in a LOS scenario at 60 meters, with SF=12 and a payload of 51 bytes, we observed packet loss due to the conditions described at the beginning of Section 5.2. Under these conditions,

 doi:10.20944/preprints202411.0254.v1

we lost one packet out of every ten sent. This test was repeated five times, consistently yielding the same result. All tests for SF=12 and the three different payload sizes were repeated five times, resulting in a total of 50 packets sent for each data size. Ultimately, we observed that for SF=12 and 51 bytes at 60 meters, we lost one packet out of ten, resulting in a PDR of 90%. This expected packet loss can be attributed to the extended ToA (nearly 2500ms), which increases the likelihood of collisions and interference, leading to connection degradation and packet loss for transmissions with these characteristics. In Table 6 we can see a resume of the PDR for this scenario and the next.

5.4. NLOS Results

After carrying out the measurements for the previous scenario and stablishing a pattern we have now checked the impact of obstacles in the quality of our link and the possibility of also having some number of packets lost for the same SFs and payload sizes. The distance tested will only be one (60 meters) of the previous three. To do this, we visualized two types of scenarios: sparse vegetation and a concrete wall between the module and the gateway. The configurations of Table 5 resume the settings.

Table 5. NLOS scenario settings.

SF	7,9,12
Distance	60 m
Emitting Power	8 dBm
Frequency	868.2 MHz
Data size	14, 32, 51 bytes
Code Rate	4/5
Bandwidth	125 kHz
Duty Cycle	1%
Time between messages	1 s

In Figure 22, we can see the scenario with sparse vegetation, including a cedar tree. The GW was positioned in the building at a height of 5 meters, while the ED was placed behind the cedar tree at a height of 3 meters.

Figure 22. NLOS scenario at 60m (GW at the window of the building and ED at the other side of the street behind a cedar tree).

 doi:10.20944/preprints202411.0254.v1

In Figure 23, we can see the scenario with a concrete wall. GW was positioned in the building at a height of 5 meters, while the ED was placed behind the wall at a height of 2 meters (in this point the wall as 4m high).

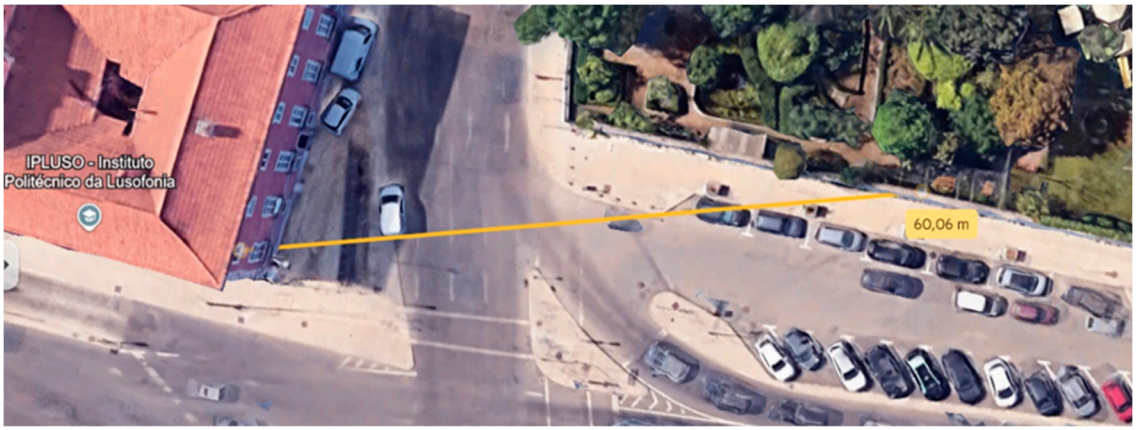

Figure 23. NLOS scenario at 60m (GW at the window of the building and ED at the other side of the street behind a concrete wall).

As in the previous scenario (LOS), we began by studying the influence of ToA on the RSSI of the payload size for each SF on the received signal strength of the connection, considering the size of the files sent and the relationship of a given chosen SF in ToA

Comparing Figures 24 and 25 with the previous figures (15, 16, 17), we can see that the fact that there is no line of sight does not alter the ToA values of the connection. ToA according to SFs and data size in LOS and NLOS scenarios are nearly identical. This indicates that there is no significant impact on the RSSI. The distances involved are relatively short, and the propagation delay introduced by obstacles such as walls or vegetation is minimal compared to the overall distance. For instance, even with a wall, vegetation or some additional distance (by the order of dozens of meters), the delay would be in the order of nanoseconds (speed of light is 3.3 ns/m), which is negligible when considering the overall ToA for the tried packets. The ToA for a 14-byte packet (the lowest is 46.3ms for SF7), or any other packet in this experiment, is primarily determined by the data rate (determined by the SF and BW), modulation scheme (determined by SF, BW, CR, and frequency), as well as the payload length, preamble, and header used in LoRaWAN, rather than minor propagation delays. As far as RSSI is concerned, the values obtained in the case of the NLOS with vegetation, the best performance at this distance and for the three packets sizes it's the SF7, with the highest value being -76 dBm for 32 bytes and the worst -91 dBm for the case of the 51 bytes. This values, are all better than the ones recorded previously, for the same distance at 60 meters in LOS, and for the three different packets sizes (with SF7).

However, the concrete wall will introduce a greater decay in the quality of the connection than all the previous situations study until now.

 doi:10.20944/preprints202411.0254.v1

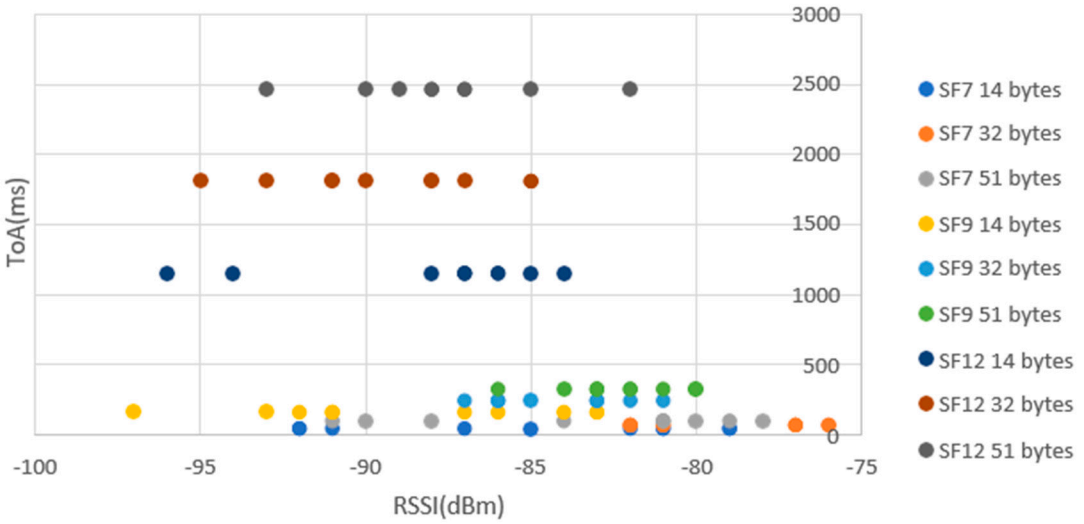

Figure 24. Influence of the payload size (for the three SFs) on ToA and on the RSSI (with vegetation).

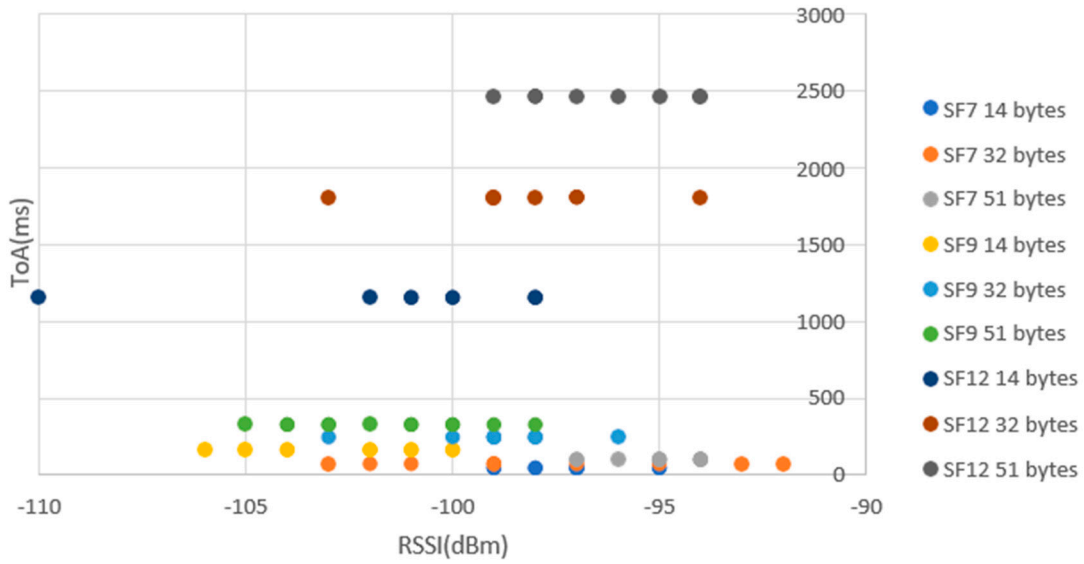

Figure 25. Influence of the payload size (for the three SFs) on ToA and on the RSSI (with concrete wall).

And analyzing the results for the case of the concrete wall, we can see that for the three packet sizes, both the transmission with SF7 and the transmission with SF12 have very similar values, but with SF12 having the smallest variance between the highest values and the lows for the three packet size situations. And choosing the SF12 spreading factor could be the best option in these cases. For SF12, the highest value is -94 dBm (51 bytes) and the lowest is -102 dBm (14 bytes), thus showing very robust behavior under these conditions. For SF7, the highest value is -92 dBm (for the 32 byte packet) while the worst is -103 dBm (also for 32 bytes). This stability of SF12 values is also an advantage, if we think about the possibility of inter-SF interference, because a connection with the latter's characteristics is less likely to have inter-SF interference (arising from communications with different SF), than one with more dispersed values, thus resulting in an advantage for the designer.

Next, we looked, more, at the effect of SF on ToA for various file sizes. As previously mentioned, the ToA primarily depends on the data rate, which is determined by the SF and BW, as well as the modulation scheme, which is influenced by the SF, BW, CR, and frequency. However, in our

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

experiment, the frequency, BW, and CR were fixed. Given the Non-Line-of-Sight (NLOS) scenarios tested and the short distances involved, the propagation delays are negligible (in the nanosecond range) compared to the ToA values, which are in the millisecond range. Therefore, we considered that there was no variation in ToA values (Figure 26) compared to the Line-of-Sight (LOS) scenario.

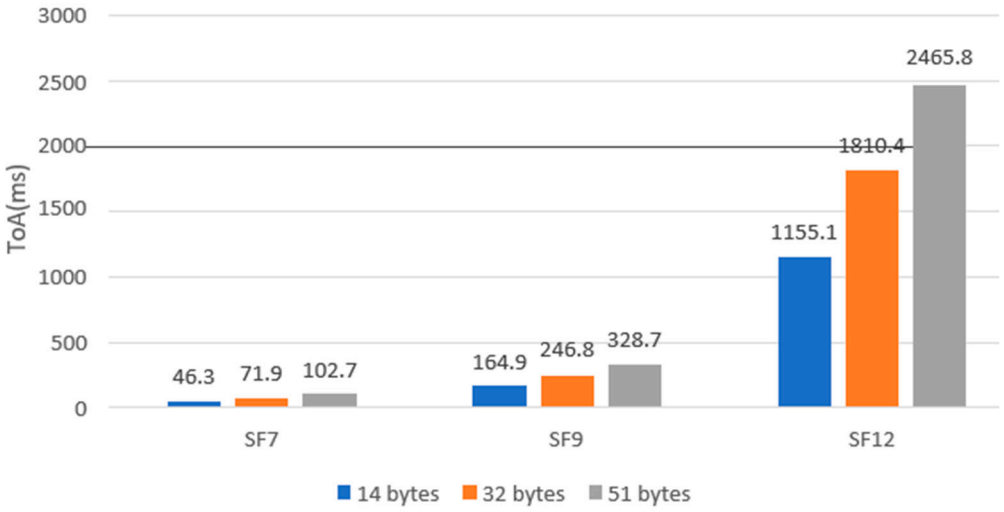

Figure 26. ToA according to SFs and data size in NLOS scenario.

As in the previous scenario, Figure 27 (vegetation as an obstacle) and Figure 28 (concrete wall as an obstacle) make a graphical resume of what has been said about the values of RSSI for different SFs and payload sizes at 60 meters. It compares the impact on connection quality of varying file sizes at this distance, using the average value of the 10 packages sent. It is important to emphasize that in the case of the wall as an obstacle, SF9 performed worse than SF12.

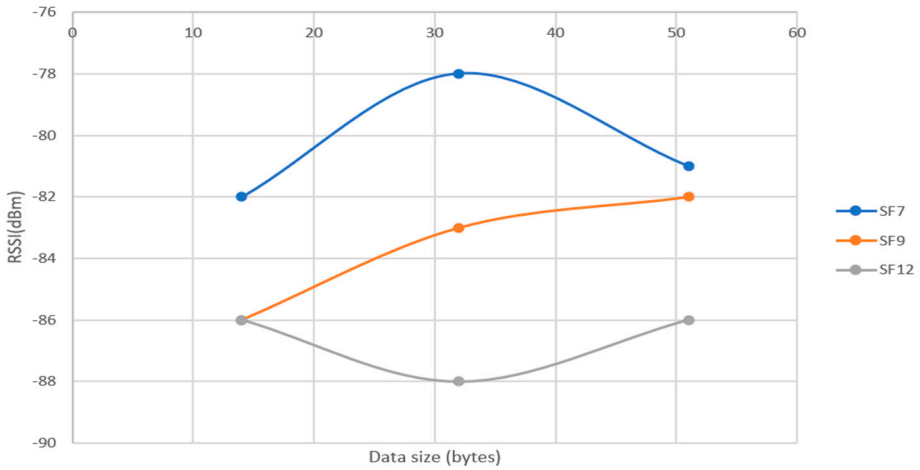

Figure 27. Average RSSI according with payload lengths for different SFs, including vegetation.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 November 2024 doi:10.20944/preprints202411.0254.v1

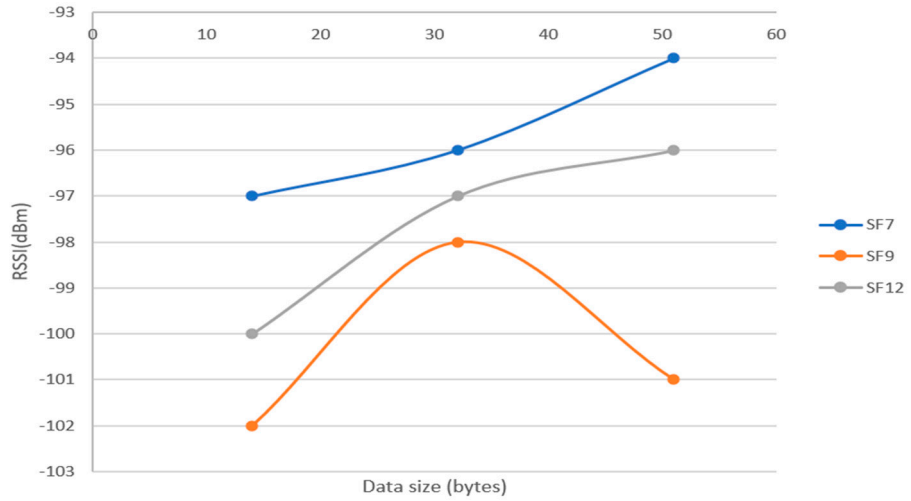

Figure 28. Average RSSI according with payload lengths for different SF, including a concrete wall.

Finally, the number of packets sent and received in both obstacle scenarios was analyzed. In the case of the vegetation obstacle there was only the loss of one packet out of 10 sent, at SF12 for a 51 byte file. To resolve any doubts, the test was repeated 5 times, with a total of 50 packets sent. And the result was always the same.

With the concrete wall of the field serving as an obstacle, there was also the loss of one packet, out of 10 sent, for SF12 and, this time, for all file sizes (14, 32, 51 byte). As in the LOS situation and the previous one, we decided to send more (5 times) packets, for a total of 50, and the result was the same. In Table 6 we can see a resume of the PDR for all scenarios tested.

Table 6. PDR Results for Various Scenarios, Distances, SF, and Payloads.

Scenario	Distance	SF	Payload (bytes)	Packets Sent	Packets Received	PDR (%)
LOS	60m	12	51	10	9	90
NLOS (Vegetation)	60m	12	51	10	9	90
NLOS (Concrete Wall)	60m	12	14	10	9	90
NLOS (Concrete Wall)	60m	12	32	10	9	90
NLOS (Concrete Wall)	60m	12	51	10	9	90

So, if by one hand the stability of values could be an advantage for the SF12 choice, on the other hand we had lost packets we experienced packet loss, and in situations that it's important not to lose packets (e.g. Surveillance systems, Energy monitoring and management - smart grids, Autonomous vehicles, Monitoring of electrical signals) the option for the SF7 will be the correct one. Considering the problem of inter-SF interference, we see that, for the three SFs tested and, in a case, where a gateway may be receiving communications packets from different SFs with different packet sizes (at the same distance), the RSSI values are much closer together than in the case of the LOS scenario, making this case the worst for the SIR (lowest).

Packet loss in the case of the NLOS (concrete wall) scenario of SF12 and 51 bytes was expected. Considering that previously for the case of payload with 51 bytes and SF12, in the LOS and NLOS (with vegetation) scenarios, it had already been verified, the loss of a packet in this case of the concrete wall also happened. The long ToA led to this.

Furthermore, in this latter scenario, signals must penetrate, diffract, or reflect around obstacles (such as concrete walls or objects), which can cause multipath propagation (in addition to normal attenuation). Signals will reflect off surfaces and arrive at the receiver at different times. If we think that in addition, we have a long ToA (which for the case of SF12 and the three data sizes, varies from 1155 ms (14 bytes) to 2465ms (51 bytes)) we will most likely cause destructive interference to the

 doi:10.20944/preprints202411.0254.v1

signals and increase thus the probability of collisions and packet loss for the case of SF12 and the other two data sizes (14 and 32 bytes), thus leading to a result in the PDR, for each one, of 90%.

6. Conclusions

This study aimed to investigate the effects of collisions and interference in short-range urban LoRaWAN networks, focusing on SFs and payload sizes influence signal transmission quality. We used performance indicators such as RSSI, ToA and PDR to assess the reliability of LoRaWAN links in real-world scenarios. Additionally, we validated the effectiveness of these performance indicators in ensuring good signal quality.

Initially, we established a reference by determining the values of RSSI, ToA, and PDR in a LOS scenario for various SFs, payload sizes, and distances. Subsequently, we conducted experiments at a distance of 60 meters in a NLOS environment with vegetation and a concrete wall.

PDR provided a more realistic assessment of link reliability. Although RSSI consistently indicated good or at least acceptable signal strength, we observed packet losses due to specific conditions: inter-SF interference, fading, shadowing, multi-path effects, and extended ToA (especially for SF12 with varying packet sizes). Our experimental results indicate that the choice of SFs and packet lengths critically influences ToA, RSSI, and PDR.

In an inter-SF interference environment, packet payload length and the choice of SFs impact ToA, leading to packet loss in NLOS scenarios. For both LOS and NLOS scenarios (with vegetation) at a distance of 60 meters, using SF12 and a payload of 51 bytes, 10 packets were sent and 9 were received, resulting in a PDR of 90%. However, in the NLOS scenario with a concrete wall, the worst results were obtained. For all payloads (14, 32, 51 bytes), 10 packets were sent at a distance of 60 meters with SF12, resulting in a PDR of 90%. When dealing with multiple devices located near the gateways, the combination of different SFs and varying packet lengths will lead to increased latency and longer ToA. As a result, the risk of packet loss becomes more significant, especially if the Signal-to-Interference Ratio (SIR) is low.

Observing the NLOS conditions, such as the concrete wall at 60 meters, a PDR of 90% underscores the robustness of LoRaWAN for most non-critical applications, even in challenging environments. However, ToA varied significantly due to the payload lengths, ranging from 46ms to 2500ms, highlighting the potential for increased latency and packet loss in situations of inter-SF interference. In our short-distance scenario, close-range RSSI values also revealed a high probability of interference and collisions due to inter-SF interference. This limitation will affect scalability for end nodes positioned very close to gateways, as they interfere with more distant nodes.

These findings are essential for optimizing LoRaWAN deployments in smart cities. By carefully selecting SFs and managing packet lengths, network designers can mitigate the adverse effects of interference, thereby enhancing the reliability and efficiency of urban IoT systems. These experiments also underscore that selecting an appropriate SF for a given link is not straightforward, and designers should conduct field tests to validate their choices and optimize their networks.

For networks with devices far from gateways, addressing higher ToA values (e.g., SF12) also poses a significant risk of packet loss due to latency. This limitation, whether for short or long distances, will affect scalability, especially in NLOS scenarios, such as those in smart cities involving buildings. Therefore, a balance between emitted and received power will be critical in a large network, especially at the two “extreme” points. This balance is important because Adaptive Data Rate (ADR) does not solve everything. Ensuring this balance helps prevent the nearest nodes from suffering from inter-SF and intra-SF interference caused by the farthest nodes, and vice-versa. This balance also mitigates the issues of latency and poor signal strength experienced by the farthest nodes. The performance of LoRaWAN signals in scenarios of inter-SF interference is critically important, as these networks are expanding exponentially.

While some studies have explored inter-SF interference to understand how different spreading factors interact with payload lengths and affect network performance, these studies often focus on theoretical models and simulations. Only a few include field measurements, and the extent and comprehensiveness of these measurements can vary. The field is quite dynamic, so continuous study,

 doi:10.20944/preprints202411.0254.v1

especially with comprehensive field measurements, is essential to address new challenges and applications.

In our next study, we intend to increase the distances and expand the number of devices in the network. Extending these scenarios, as already proposed, will lead to further validation of these metrics in various conditions. This will also allow us to test the scalability of a network with several end nodes and different SFs at greater distances, and to examine aspects like collisions and interference in the performance of these networks. This is a promising direction for future work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Andri Rahmadhani and Fernando Kuipers (Del. University of Technology), "Understanding collisions on LoRaWAN", Conference: the 12th International Workshop, pag.1, 2018.
2. Oracle - "What is IoT?". Available online: https://www.oracle.com/internet-of-things/what-is-iot/ (accessed on 21/03/2024).
3. Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar and Adel Elmaghraby, "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges", Smart Cities 2021, 4(2), 429-475.
4. Malik, Hassaan; Anees, Tayyaba; Faheem, Muhammad; Chaudhry, Muhammad Umar; Ali, Aatka; Asghar, Muhammad Nabeel, "Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions", October 2023. Available online, https://core.ac.uk/reader/589149010, (accessed on 19/07/2024).
5. Leeban Moses, Perarasi Sambantham, Muhammad Faheem, Shoukath Ali, Arfat Ahmad Khan, "Joint delay and energy aware dragonfly optimization-based uplink resource allocation scheme for LTE-A networks in a cross-layer environment", January 2024. Available online, The Journal of Engineering 2024(2):12353, (accessed on 19/07/2024).
6. Rajkumar Buyya, Satish N. Srirama, Redowan Mahmud, Mohammad Goudarzi, Leila Ismail, and Vassilis Kostakos, "Quality of Service (QoS)-driven Edge Computing and Smart Hospitals: A Vision, Architectural Elements, and Future Directions", 2021. Available online, https://arxiv.org/pdf/2303.06896v1, (accessed on 19/07/2024).
7. Semtech Corporation, "LoRa® and LoRaWAN®: A Technical Overview", December 2019 (accessed 17/05/2024).
8. Davide Magrin, Martina Capuzzo, Andrea Zanella, "A Thorough Study of LoRaWAN Performance Under Different Parameter Settings", IEEE Internet of Things Journal, Vol: 7, Issue: 1, January 2020. Available online, https://ieeexplore.ieee.org/document/8863372, (accessed 20/05/2024).
9. Eugen Harinda, Andrew J. Wixted, Ayyaz-UI-Haq Qureshi, Hadi Larijani, and Ryan M. Gibson, "Performance of a Live Multi-Gateway LoRaWAN and Interference Measurement across Indoor and Outdoor Localities", Computers 2022, 11(2), 25. Available online, https://www.mdpi.com/2073-431X/11/2/25, (accessed 25/05/2024).
10. Prachi V. Wadatkar; Bharat S. Chaudhari; Marco Zennaro, "Impact of Interference on LoRaWAN Link Performance", IEEE Xplore, 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), September 2019. Available online, https://ieeexplore.ieee.org/abstract/document/9128417, (accessed 25/05/2024).
11. Poonam Maurya, Aatmjeet Singh and Arzad Alam Kherani "A review: spreading factor allocation schemes for LoRaWAN", May 2022, available online, https://link.springer.com/article/10.1007/s11235-022-00903-4, (accessed on 17/05/2024).
12. Aamir Mahmood, Emiliano Sisinni, Lakshmikanth Guntupalli, Raúl Rondón, Syed Ali Hassan, Mikael Gidlund, "Scalability analysis of a LoRa network under imperfect orthogonality", August 2018, IEEE Transactions on Industrial Informatics, vol. 15, issue 3, p. 1425-1436. Available online, https://ieeexplore.ieee.org/abstract/document/8430542, (accessed on 18/05/2024).
13. Antoine Waret, Megumi Kaneko, Alexandre Guitton, Nancy El Rachkidy, "LoRa Throughput Analysis with Imperfect Spreading Factor Orthogonality", March 2018. Available online, https://arxiv.org/pdf/1803.06534, (accessed on 16/05/2024).
14. Daniele Croce, Michele Gucciardo, Stefano Mangione, Giuseppe Santaromita, Ilenia Tinnirello, "Impact of LoRa Imperfect Orthogonality: Analysis of Link-level Performance". Available online: https://www.researchgate.net/publiction/319486965_Impact_of_Spreading_Factor_Imperfect_Orthogonality_in_LoRa_Communications, (accessed 17/05/2024).
15. Jetmir Haxhibeqiri, Floris Van den Abeele, Ingrid Moerman and Jeroen Hoebeke, "LoRa Scalability: A Simulation Model Based on Interference Measurements", Sensors 2017, 17(6), 1193.

16. Bor, M.C.; Roedig, U.; Voigt, T.; Alonso, J.M.; "Do LoRa low-power wide-area networks scale?", In Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation ofWireless and Mobile Systems, Valletta, Malta, 13–17 November 2016; pp. 59–67.
17. Lavric, A.; Petrariu, A.I.; Coca, E.; Popa, V.; "LoRa traffic generator based on software defined radio technology for LoRa modulation orthogonality analysis: Empirical and experimental evaluation". Sensors 2020, 20, 4123.
18. Sokratis Kartakis, Babu D. Choudhary, Alexander D. Gluhak, Lambros Lambrinos, Julie A. McCann, "Demystifying Low-Power Wide-Area Communications for City IoT Applications", WiNTECH '16: Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization, October 2016.
19. Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios", IEEE Wireless Communications, 23(5), October 2015.
20. Sanchez-Iborra, R.; Sanchez-Gomez, J.; Ballesta-Viñas, J.; Cano, M.-D.; Skarmeta, A.F. , "Performance evaluation of LoRa considering scenario conditions". Sensors 2018, 18, 772.
21. Brecht Reynders, Sofie Pollin, "Chirp Spread Spectrum as a Modulation Technique for Long Range Communication", IEEE Symposium on Communications and Vehicular Technology (SCVT), November 2016. Available online, https://ieeexplore.ieee.org/document/7797659, (accessed on 19/07/2024).
22. Qingjie Guo, Fengxu Yang and Jianming Wei, "Experimental Evaluation of the Packet Reception Performance of LoRa", Sensors 2021, 21(4), 1071.
23. Semtech Corporation, "AN1200.22 LoRa™ Modulation Basics", May 2015.
24. LoRa Alliance. Available online: https://lora-alliance.org/wp-content/uploads/2020/11/what-is-lorawan.pdf, (accessed 9/4/2024).
25. T. Elshabrawy e J. Robert, "Evaluation of the BER Performance of LoRa Communication using BICM Decoding", 2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin), p.162-167, 2019.
26. LoRa. Available online: https://lora.readthedocs.io/en/latest/, (accessed 18/5/2024).
27. The Things Network. Available online: LoRa Physical Layer Packet Format | The Things Network, (accessed 17/5/2024).
28. The Things Network. Available online: https://www.thethingsnetwork.org/docs/lorawan/spreading-factors/, (accessed 17/5/2024).
29. Courjault, J.; Vrigenau, B.; Berder, O.; Bhatnagar, M. A Computable Form for LoRa Performance Estimation: Application to Ricean and Nakagami Fading. *IEEE Access* **2021**, *9*, 81601–81611.
30. ITU-R. Available online: https://www.itu.int/rec/R-REC-P.833-10-202109-I/en, (accessed on 18/5/2024).
31. Alexis Barrios-Ulloa, Paola Patricia Ariza-Colpas, Hernando Sánchez-Moreno, Alejandra Paola Quintero-Linero and Emiro De la Hoz-Franco, "Modeling RadioWave Propagation for Wireless Sensor Networks in Vegetated Environments: A Systematic Literature Review", Available online: https://www.mdpi.com/1424-8220/22/14/5285.
32. ITU-R. Available online: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.2040-2-202109-S!!PDF-E.pdf, (accessed on 18/05/2024).
33. Dias, C.F.; Lima, E.R.D.; Fraidenraich, G. Bit error rate closed-form expressions for LoRa systems under Nakagami and Rice fading channels. *Sensors* **2019**, *19*, 4412.
34. Claire Goursaud, Jean-Marie Gorce, "Dedicated networks for IoT : PHY / MAC state of the art and challenges". Available online: https://hal.science/hal-01231221, (accessed 18/05/2024).
35. N. Abramson and F.F. Kuo, Eds., Computer-Communication Networks, Englewood Cliffs, NJ: Prentice-Hall, Chapter 13, 1973.
36. R. Metcalfe, Steady state analysis of a slotted and controlled ALOHA system with blocking, *Proc. 6th Hawaii Int. Conf. Sys. Sci.*, January 1973.
37. Dragino. Available online: https://www.dragino.com/ (accessed on 9/4/2024).
38. Arduino. Available online: https://www.arduino.cc/ (accessed on 11/3/2024).
39. Semtech Corporation. Available online: https://www.semtech.com/products/wireless-rf/lora-connect/sx1276#features, (accessed 09/04/2024).
40. The Things Network. Available online: https://www.thethingsnetwork.org/, (accessed on 23/2/2024).