UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

# ON THE PERFORMANCE OF IEEE 802.15.4 UNDER JAMMING ATTACKS

TESIS PARA OPTAR AL GRADO DE MAGISTER EN CIENCIAS DE LA INGENIERÍA, MENCIÓN ELÉCTRICA

NICOLÁS ALBERTO LÓPEZ VILOS

PROFESOR GUÍA:
CESAR AZURDIA MEZA

PROFESOR CO-GUÍA:
SAMUEL MONTEJO SÁNCHEZ

MIEMBROS DE LA COMISIÓN:
NESTOR BECERRA
SAMUEL BARALDI MAFRA

Este trabajo ha sido parcialmente financiado por Proyecto FONDECYT Iniciación 11160517, ANID FONDECYT Iniciación 11200659 y Vicerrectoría de Investigación y Desarrollo (VID) de la Universidad de Chile, Proyecto ENL 01/20

SANTIAGO DE CHILE
2021

RESUMEN DE LA MEMORIA PARA OPTAR AL TÍTULO DE
MAGISTER EN CIENCIAS DE LA INGENIERÍA,
MENCIÓN ELÉCTRICA
POR: NICOLÁS ALBERTO LÓPEZ VILOS
FECHA: 2021
PROF. GUÍA: CESAR AZURDIA MEZA
PROF. CO-GUÍA: SAMUEL MONTEJO SÁNCHEZ

# ON THE PERFORMANCE OF IEEE 802.15.4 UNDER JAMMING ATTACKS

Las ampliamente utilizadas redes de sensores, se encuentran expuestas a una serie de problemáticas en términos de seguridad. Los jamming attacks son un tipo de ataque enfocado en la capa física y que merma la seguridad e integridad de la red. Además, su detección y análisis en ambientes indoor no ha sido ampliamente estudiado desde un enfoque experimental, por lo que es imperioso su estudio en estas condiciones.

Mediante la proposición y uso de un testbed experimental, los jamming attacks son analizados en una red IEEE 802.15.4 mediante métricas de desempeño. Para la validación de los datos experimentales, se efectúa una completa caracterización del sistema de canal mediante modelos de regresión y de las métricas de desempeño con un modelo probabilístico.

Los resultados muestran una alta correlación entre los datos experimentales y teóricos. Específicamente, para un atacante en las comunicaciones, se obtiene que para un SINR $\geq 3.1$ dB al menos la mitad de los paquetes enviados, considerando hasta 4 transmisores, es posible. Para el caso de dos interferentes, se determina que se debe asegurar un threshold de al menos 3d$Bm$ entre los nodos transmisores e interferentes para tener alguna recepción de paquetes en el nodo receptor.

SUMMARY OF THE THESIS TO OBTAIN
THE MASTER'S DEGREE IN ENGINEERING SCIENCE,
MENTION IN ELECTRICAL ENGINEERING
BY: NICOLÁS ALBERTO LÓPEZ VILOS
DATE: 2021
ADVISOR: CESAR AZURDIA MEZA
CO-ADVISOR: SAMUEL MONTEJO SÁNCHEZ

## ON THE PERFORMANCE OF IEEE 802.15.4 UNDER JAMMING ATTACKS

The extensively used wireless sensor networks are exposed to several threats in security terms. The jamming attacks are a type of attack that aims the physical layer to diminish the security and integrity of the network. Moreover, the detection and the analysis of the attacks in an indoor environment has not been deeply studied from an experimental approach. For this reason, their study is imperious.

By the proposition and use of an experimental testbed, the jamming attacks are analyzed in an IEEE 802.15.4 network using performance metrics. A complete characterization of the channel system by the use of regression models and for the performance metrics by the use of a probabilistic model is made to validate the collected experimental data.

The results show a good correlation between the experimental and theoretical values. Specifically, for an SINR $\geq$ 3.1dB, half of the total transmitted packets considering a maximum of 4 transmitters is possible. Meanwhile, for two interferers, a 3 dBm threshold is necessary between the transmitters and interferers to guarantee the reception of packets in the sink node.

*“La realidad está ahí y nosotros en ella,*
*entendiéndola a nuestra manera,*
*pero en ella.”*
*Julio Cortázar*

# Agradecimientos

Este trabajo es el fruto de una serie de eventos, situaciones y sentimientos, que podrían ser englobados en un esfuerzo conjunto entre mi querida familia y amigos, que estuvieron presente en estos tiempos de incertidumbre, de mis profesores y colegas que estuvieron guíandome por este arduo camino de la investigación y de los deseos de contribuir con un grano de arena, en el interminable camino del conocimiento.

A todos ustedes, gracias.

*"La vida de cada hombre es un camino hacia sí mismo,*
*el intento de un camino,*
*el esbozo de un sendero."*
Hermann Hesse

# Contents

# List of Tables

# List of Figures

# Acronyms

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **ASK** | Amplitude Shift Keying |
| **BPSK** | Binary Phase Shift Keying |
| **BE** | Backoff Exponent |
| **BER** | Bit Error Rate |
| **CA** | Collision Avoidance |
| **CE** | Capture Effect |
| **CA** | CCA Threshold |
| **CCA** | Clear Channel Assesment |
| **COAP** | Constrained Application Protocol |
| **CSMA** | Carrier-sense multiple access |
| **CTS** | Clear To Send |
| **DC** | Direct Current |
| **DSSS** | Direct-Sequence Spread Spectrum |
| **DOS** | Denial Of Service |
| **DTMC** | Discrete Time Markov Chain |
| **ED** | Energy Detection |
| **FFD** | Full-Function Device |
| **HART** | Highway Addressable Remote Transducer Protocol |
| **IOT** | Internet Of Things |

| | |
|---|---|
| **Ipv6** | Internet Protocol Version Six |
| **ISM** | Industrial Scientific and Medical |
| **LLN** | Low Power and Lossy Networks |
| **LR-WPAN** | Low Rate-Wireles Personal Area Network |
| **LQI** | Link Quality Indicator |
| **MAC** | Medium Access Control |
| **QoS** | Quality of Service |
| **O-QPSK** | Offest Quadrature Phase Shift Keying |
| **P2P** | Peer-to-Peer |
| **PCA** | Priorized Contention Access |
| **PDR** | Packet Data Rate |
| **PHR** | PHY Header |
| **PHY** | Physical |
| **PN** | Pseudo-random Noise |
| **PSK** | Phase Shift Keying |
| **PPDU** | Presentation Protocol Packet Data Unit |
| **PSDU** | PHY service data unit |
| **QPSK** | Quadrature Phase Shift Keying |
| **RFD** | Reduced-Function Device |
| **RPL** | Routing Protocol for Low power and Lossy Networks |
| **RSS** | Received Signal Strength |
| **RSSI** | Received Signal Strength Indicator |
| **RTS** | Request To Send |
| **SER** | Symbol Error Rate |
| **SHR** | Synchronization Header |
| **SFD** | Start Frame Delimiter |

**SDR** Software Defined Radio

**SINR** Signal Interference-plus-Noise Ratio

**SNR** Signal to Noise Ratio

**TDMA** Time Division Multiple Access

**TSCH** Time Slotted Channel Hopping

**WLAN** Wireless Local Area Network

**WPAN** Wireles Personal Area Network

**WSN** Wireless Sensor Network

# Chapter 1

# Introduction

## 1.1 Motivation

The massive deployment of Low-Power and Lossy Networks (LLN) to obtain data from different environments has caught the attention of the scientific and industrial communities. The LLN uses a series of nodes to acquire data from the environments where there are placed or to communicate actuators that allow the automatization of tasks. The communication between the nodes is performed by the use of communication protocols that specifies the requirements in the Medium Access Control (MAC) and Physical Layer (PHY). The standard IEEE 802.15.4 [4] details the requirements of the MAC and PHY layers in numerous LLNs.

The standard IEEE 802.15.4 specifies the technical requirements in the PHY and MAC layers that allow the communication of the constrained nodes. Different requirements are detailed in the standard to cope with the particular considerations of diverse environments of application. In particular, the use of different frequency bands, modulation techniques, and MAC protocols are detailed. The 2.4 GHz frequency band with an Offset Quadrature Phase Shift Keying (O-QPSK) modulation is the specified configuration in the PHY layer for indoor applications. This PHY layer configuration allows the use of different MAC protocols as Time Division Multiple Access (TDMA), Time Slotted Channel Hopping (TSCH), and Carrier-Sense Multiple Access (CSMA). The use of the mentioned protocols and configurations enables communications in several environments as industrial, medical, and vehicular in controlled scenarios [5].

The networks using the IEEE 802.15.4 network are exposed to several security issues owing to the broadcast nature of the wireless medium used for the communication process [6]. The denial of service (DoS) attacks could be performed in several layers of the communications systems to disrupt the normal behavior of the network. The jamming attacks are a type of DoS attack that targets the PHY layer in a network by the generation of interference signals to block the communications or a type of packet in particular. Using different strategies, the attacker can optimize the performance of the attack to achieve a more stealthiness and energy-efficient jammer [7]. The different strategies that the attacker could use bring notable challenges in the security and performance of the LLN using the standard IEEE 802.15.4.

Several models are proposed to analyze the LLN using the standard IEEE 802.15.4 in terms of security and performance [8–22]. Through the use of game theory and Markov chain models, the different events in a network can be completely characterized. In particular, the Discrete-Time Markov Chain (DTMC) is being used to model the LLN using the standard IEEE 802.15.4 to analyze the performance in terms of performance metrics as Packet Data Rate (PDR), goodput, latency, and energy consumption generally. The use of the mentioned performance metrics could predict the behavior of the networks under different assumptions and scenarios. However, few works analyze the performance and security of an LLN using IEEE 802.15.4 under scenarios with the existence of jamming attacks. Additionally, the ability to correctly receive packets despite the presence of jamming attacks or interferences, known as Capture Effect (CE), is not included in the analysis of the networks.

## 1.2 Problem Statement and Hypothesis

### 1.2.1 Problem Statement

Many studies of single-hop and multi-hop models with homogeneous and heterogeneous traffic have been studied in the literature [9–14, 17–31] . However, few works, models and analyze the impact of an attack or interference on the networks [10, 26–31] or assume channel models [11, 18, 25]. In [12], the authors proposed a model for the MAC layer for single-hop and multi-hop networks using unslotted IEEE 802.15.4. By Markov chains, the network using CSMA/CA algorithm is generated and evaluated through metrics as reliability, delay, and energy consumption. Although, considerations of the PHY layer are not considered for the CSMA/CA as stated in [18] . Consequently, the errors in the transmission due to channel conditions are stated as probabilities and no specific for a real scenario. Moreover, the attacks performed in the PHY layer as jamming attacks, can not be studied. However, in [11], the error in the transmission and the use of the Capture Effect (CE) are considered to increase the reception of the packets due to collisions. Also, the model is generated using HMM for the MAC layer, and they validate the model using the Cooja simulator and the implementation of the Contiki OS in Sky motes. Although the PHY layer is not considered for the HMM model, only the measurement of the Capture Effect empirically can represent the behavior of the PHY layer in the model. Moreover, the analyzed MAC mechanism correspond to TSCH.

Other works model the different types of jamming in Wireless Networks [26, 28, 29] and present the countermeasures to the assumptions presented in this works. In [26], the authors focus on the analysis of the wireless networks using BPSK and QPSK modulations in terms of outage probability and error probability metrics. The principal contributions state that the number of jammers required to achieve a specific outage probability is dependent on the signal power of the victim. The model inferences are validated through simulations. However, experimental results are not performed, and the analysis of the interaction with MAC layers is not considered. Similarly in [29], the cross-layer interactions and the validation with experimental data are not present.

In [28] the modeling, and detection of jamming attacks are realized in time-critical applications. The jamming strategy analyzed is constant and reactive mode using a gambling-based model. Also, they validate the theoretical analysis by an experimental setup using the standard IEC 61850. Using the results obtained for the theoretical and experimental setup, they design an algorithm to detect attacks called jamming attack detection based on estimation (JADE). Despite, considerations about the channel model is not analyzed. Moreover, the analyzed network is a single-hop model with homogeneous traffic.

Although, in [31] the authors focus on the analysis of a communication system using Direct Sequence Spread Spectrum (DSSS) against reactive jamming to the Start Frame Delimiter (SFD) of the messages. Using the metrics of Packet Delivery Ratio (PDR), Chipe Error Rate (CER), and Received Signal Strength (RSS) the proposed detection algorithm is generated. The standard IEEE 802.15.4 with three nodes; sender, receiver, and jammer is implemented with a single-hop and homogeneous traffic. However, the modeling of the network and the channel model are not performed.

In [30], the authors analyze the performance of IEEE 802.11 MAC in the presence of various types of jammers. Using theoretical analysis, simulations, and experimental results, the authors build a Discrete Markov Model with the considerations of attackers in the network. Using a testbed with one transmitter and receiver using the IEEE 802.11 and a jammer device implemented in an SDR, they analyze the performance of the network, in terms of throughput due to the network size, packet size, and jamming rate. The conclusions state that the periodic, reactive, and omniscient jammer have a high impact on the throughput on the network.

Our work has a similar methodology to the presented in this work [30], and the differences are: our work considers the IEEE 802.15.4 standard, a greater number of devices in the conformation of the network, a characterization of the channel, and different jamming strategies. Also, we use the SDR as a sniffer to analyze the activity of the network, and the jammer is implemented following a QPSK modulation and a random noise generated by a Voltage Controlled Oscillator. Additionally, in order to analyze the models of the MAC layer, we choose the works [19, 25] due to their considerations of the capture effect and interferers in the network.

### 1.2.2 Hypothesis

We establish the hypothesis of the work as follows:

- The jamming attacks undermine the performance of IEEE 802.15.4 networks using CSMA-CA, and the impacts of these attacks depend on the scheduling strategy, the type of attack, and the scenario where the network is deployed.

## 1.3 Objectives

The objectives of the work are summarized as follows:

- **General objective:** To evaluate, analytically and experimentally, the performance of an IEEE 802.15.4 network using CSMA-CA in the presence of jamming attacks in different scenarios.

- **Specific objectives:**
    - To study and analyze MAC and PHY layer models of IEEE 802.15.4 networks with probabilistic models and different models of jamming attacks.
    - To study and determine different performance metrics to evaluate the network under different jamming attacks strategies.
    - To design and implement an experimental testbed to evaluate the network against jamming attacks.
    - To calculate the state probabilities of the probabilistic model and obtain the performance metrics in the experimental and simulated scenarios.
    - To analyze the performance metrics of the model and their correlation with experimental data in the different scenarios.
    - To evaluate the correlation of the performance metrics with different number of interferer and jamming strategies.

## 1.4 Methodology

In order to achieve the objective to evaluate analytically and experimentally the performance of an IEEE 802.15.4 network with the presence of jamming attacks, we use the following methodology. First, we extensively research the probabilistic models proposed for the IEEE 802.15.4 and their considerations. Specifically, due to the nature of this research work, we focus on models that consider the cross-layer interaction between the PHY and MAC layers, and if they analyze the signal interference in the communication link. Next, we correlate the performance metrics used by the model with the used for the evaluation of the performance when attackers are considered. Then, we propose an experimental testbed to evaluate the performance metrics of the models in a real scenario and their correlation with scenarios under jamming attacks. Additionally, we use two jamming strategies to evaluate the impact of each strategy on the chosen performance metrics. Finally, we evaluate the correlation of the acquired data in the experimental testbed with the probabilistic model to extend the model with the presence of jamming attacks.

## 1.5 Thesis Structure

The rest of this thesis is structured as follows. In Chapter 2, we briefly review some concepts related to Wireless Sensor Networks (WSN), the IEEE 802.15.4 standard, and the some of the main challenges in these networks. In Chapter 3, we analyze the analytical model of the standard IEEE 802.15.4 used in this work. In subsequent Chapters, we present the model of the attackers and the integration to the analytical model of the standard IEEE 802.15.4 to analyze the performance metrics.

# Chapter 2

# Background

In this chapter, we present definitions for the Wireless Sensor Networks (WSNs) and an overview of their functions and challenges in their deployment in the security area. We also explain the different standards that govern the WSN, in particular the standard IEEE 802.15.4. Finally, a review of the attacks performed in the PHY layer of the communications as the jamming attacks are analyzed.

## 2.1 Wireless Sensor Networks (WSNs)

The use of sensors to acquire data from different types of applications, as military, industrial, agriculture, and marine has been extensively used [32]. These sensors are deployed to collect and transmit the data of interest for each application as the monitoring of changes in the environment to help in the prevention of failures. The deployment of the WSN has been promoted owing to the miniaturization of the electronic devices that facilitates their integration to diverse areas.

A WSN is a type of wireless network where the sensors are interconnected to collect data of the surrounding environment as shown in Figure 2.1 The sensors are defined as constrained nodes due to their physical limitations in terms of computational power, access to energy, and restricted size [33]. The constrained nodes have defined roles inside the network that generally consists of assuming the coordinator, router, or end device function. The roles of the nodes, the topology it can adopt, and all the specifications of the communications will depend on the standard that governs the nodes.

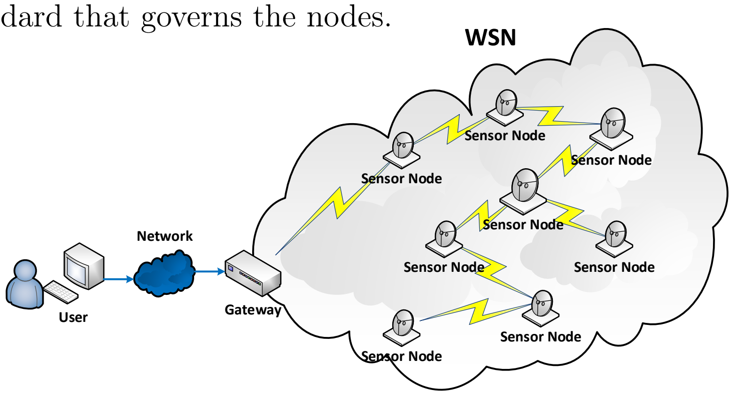


Figure 2.1: Example of a typical WSN composed of several end devices like sensor nodes, the gateway device that bridge the communications between the network and cloud services that the user can use to process and manipulate the acquired data.

In general, the principal characteristics of these types of networks, despite the standard used are:

- Low energy consumption that permits the use of battery or energy harvesting techniques.
- Ability to cope with failures of the nodes expressed as the resilience of the network.
- The network can be easily incorporate more nodes.
- The network can be used in hostile's environments.
- Present a cross-layer interaction.

The nodes in a WSN can be configured by adopting different configurations or functions, according to the programmer. The main roles of the nodes in the network according to the standard [4] are:

- End Device: Generally, correspond to the sensors nodes that acquire the data from the application environment.
- Router: It redirects the transmitted data from several end devices to other nodes in the network.
- Coordinator: It is the master device that conforms and governs the network.

According to the number of nodes deployed and the functions of them, different topologies can be created. However, the basic rules to conform the network despite the topology are:

- The end devices need to be connected to a router or coordinator device.
- The routers can establish connections between them and with the coordinator.
- The routers and coordinators do not have sleep times because they store the communication data in the buffers.
- The end devices can have sleep times.

However, new mechanisms in the MAC layer improves the sleep times of the devices to permit some nodes with the router or coordinator function, to perform sleep functions [34]. Although, it strongly depends on each application.

### 2.1.1 Standarization

The principal works tasks that standardized the WSN are the Institute of Electrical and Electronics Engineers (IEEE), the Engineering Task Force (IETF), and the HART communication foundations. Notable standards and specifications are:

- **IEEE 802.15.4** [4] standard specifies the requirements of the MAC and PHY layer in the Wireless Personal Area Networks (WPAN) for low rate transmissions. It is the most used standard for different motes and platforms as Zigbee [35], WirelessHART [36], and Digi [1] that extend the functionality of the standard in the upper layers to enhance the capabilities of the network.

  - Transmission rates of 250 kbps, 40 kbps, and 20 kbps that depends on the frequency band configured.
  - Sixteen channels in the 2.4 GHz ISM band, ten channels in the 915 MHz ISM band, and one channel in the 868 MHz band.
  - Incorporates the CSMA/CA algorithm to channel access.
  - Addressing modes of 64-bit and 16-bit.
  - Algorithms that optimize energy consumption with the use of sleep times.
  - The coordinator of the network is capable of the establishment of a network automatically.

- **Zigbee** [35] is a specification of the standard IEEE 802.15.4 that adds upper layers to the existent MAC and PHY layers. It is developed by a consortium of industry players under the name of Zigbee Alliance that focus on the domotic, process automatization, and healthcare monitoring areas. The principal characteristics of this specification are:

  - Multiple network topologies can be configured; point-to-point, point-to-multipoint, and mesh networks.
  - Low duty cycle to improve energy efficiency.
  - Low latency.
  - Up to 65000 nodes per network.
  - ZigBee can automatically establish its network.

- **WirelessHART** [36] is an open-access communications protocol of the mesh type that cope with the requirements of the application that involves the automatization of process. The PHY layer uses the band ISM 2.4 GHz with Direct-Sequence Spread Spectrum (DSSS), and the MAC layer uses (TDMA). To ensure the confidentiality of the data, AES-128 with symmetric keys are used.

- **6LoWPAN** [37] is the name of the task force of the IETF that incorporates the use of IPv6 in Low Power Wireless Personal Area Networks. Consequently, the working group defines the encapsulation and compression mechanisms of the packets to be transported across the network that use the standard IEEE 802.15.4.

In this work, the experimental setup consists of several constrained nodes named XBee S1, developed by Digi. The XBee nodes could be configured to use the different standards and specifications detailed. However, the use of the standard IEEE 802.15.4 without extended functionalities is configured in the nodes.

### 2.1.2 Challenges of WSN

The intrinsic characteristics of the WSN have enabled the growth of the concepts of Smart Cities and the Internet of Things (IoT). The development of the technologies that IoT encompasses has contributed to initiate the fourth industrial revolution [38]. However, with the benefits that the technologies as IoT, artificial intelligence, nanotechnology, robotic, quantum computing, and biotechnology, also it has several issues. In particular, the growth of IoT has brought serious concerns in terms of privacy and security [5]. Consequently, the WSN has gained a lot of attention from the industrial, governmental, and scientific community to address these concerns.

The deployment of the WSN deals with multiple challenges given the broadcast nature and the requirements to enable the communications of the system. The principal challenges that the scientific community is focused could be grouped under the following concepts:

1. **Reliability:** The data transmitted across the network by the different nodes have to be decoded correctly in the receiver side. The probability of success is usually used to model the correct reception of packets on the receiver side and is one of the most critical parameters in the communications systems. Generally, the tradeoff is to use more transmission power and lowering energy efficiency to ensure a high probability of success in the transmission of the packets.

2. **Delay:** The time between the transmission and the reception of the packet is one of the metrics that the Quality of Service (QoS) integrates and is critical to ensure that the packets are still valid to be decoded.

3. **Energy Efficiency:** The energy consumption related to the energy capacity of the network determines the lifetime of a WSN. The energy efficiency englobes this concept that permits the correct design of the network using nodes with limited energy availability.

4. **Security:** The integrity of the data and the network are the most important and critical factor given the massive use of the WSN in different areas. The possibility that malicious users corrupt the transmitted data, shutdown networks, or take control over the network is a big challenge.

Malicious users use different strategies to maximize the damage to the WSN in the mentioned concepts. The analysis of the WSN under the attacker assumption is critical to gain insight to predict the behavior of the communications system and to address these difficult challenges. Consequently, this work emphasizes the analysis of the WSN under attacker's assumptions with different strategies.

## 2.2 PHY Layer Attacks

The natural broadcast nature of the WSN makes them exposed to several inconveniences in the transmission channel. The effect of the path loss, shadowing, multipath, and noise are some of the principal factors that affect the wireless communication link. In particular, the interferences could be inherent in the medium channel or can be generated by a malicious attacker. The attacks that target the PHY layer of the system could be categorized as eavesdropping and jamming attacks [5]. These attacks are difficult to detect owing to the data over the air can be intercepted by every device in the range of transmissions.

### 2.2.1 Eavesdropping

The objective of eavesdropping attacks is the interception of the legitimate data of the legitimate nodes by a malicious node. The interception can only occur if the malicious node is in the range of the legitimate transmissions and can decode the data. Additionally, the attacker optimizes the stealthiness of the attack to intercept a lot of data on the transmissions. As a consequence, the attacker makes a log of the intercepted transmissions that leads to decode the data or gain insights about the communications protocols.

The jammer device is used as a sniffer of the communications of the network to capture the data of the transmissions. These solutions are offered in commerce to different communication protocols, making easy the access to malicious users to compromise the security of the networks. Also, the existent sniffer software can be used in conjunction with the sniffer to dissect the data and improve the analysis of the intercepted data. Moreover, the SDR can be programmed to work as a sniffer of different communications protocols simultaneously with a lot of capabilities to decode several critical information.

The attacker can decode information as node identification number, routing updates, and application sensitive data. Therefore, the information can be used to compromise the integrity of the nodes in the network, disrupt the routing process, or mesmerize the performance of the network. However, exist different techniques to overcome the problem of eavesdropping attacks.

The principal countermeasure against this type of interception is the use of cryptography techniques to encrypt the data. There are three main categories of cryptographic algorithms used to improve the security on the communication systems: symmetric key cryptography, asymmetric key cryptography and hash functions. However, due to their limited computing power, sensors cannot efficiently process the standard cryptographic keys that are used in typical wired networks.

### 2.2.2 Jamming Attacks

The radio interference attacks or jamming attacks are implemented by a jammer device that generates interference signals that affect the legitimate signal used in the communication link of the nodes, represented in Figure 2.2. The attacker aims to cause the Denial of Service (DoS) in the communications links by the degradation of the Signal to Noise (SNR) ratio. This degradation can be performed using different strategies and pulses width to undermine the reception of the data.

The denial of the reception of the data can be accomplished using the following width pulses:

- Wide Band Denial: In these types of attacks, the interference signal has great power and encloses the entire spectrum of the frequencies used by the nodes. Therefore, the mechanisms of Channel Hopping are not capable of overcoming the attack.

- Pulse Band Denial: Conversely, the pulse band interference aims only at specific channels of the communications or to only one channel. With this, the attacker can prevent

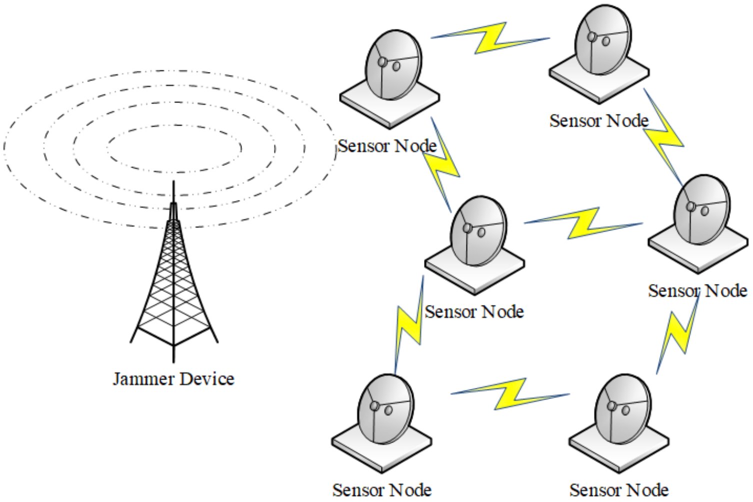


Figure 2.2: The jammer device can perpetrate an attack if only is in the range of transmission of the nodes present in the network.

the use of certain channels by the legitimate nodes, deceiving the Energy Detection (ED) algorithm to blacklist the channel.

Then, the attacker combines the width pulses with different rates of the jamming signal to generate the DoS in the network. The principal rates that categorize the jamming attacks are:

1. Constant : The interference signal is generated every time, without intervals of silence.
2. Intermittent: The interference signal is generated at certain intervals of times configured by the attacker. Usually, the interference follows a distribution (exponential, Gaussian) in the implementation.
3. Reactive: When the jammer device detects activity in the communication link (channel), the device initiates the interference signal.
4. Intelligent: When the jammer device detects the transmission of a specific data type, configured by the attacker, the device initiates the interference signal.

The jammer device can hear the transmissions in reactive and intelligent strategies. Therefore, the attacker could extend the acknowledgment of the network by the log of the data and the events in the transmission. Consequently, the communication protocol used in the MAC layer could be completely discovered [39].

In order to analyze the impact of the jamming attacks in the network, we use the performance metrics used in various works [26, 28, 29, 31, 31, 40]. These works use the reactive and non-reactive strategies to analyze the performance differences between the absence of attackers and with the presence of them. Following a theoretical and experimental methodology, the metrics of SINR, PDR, and SIR are analyzed in these works. Despite the differences in the methodology and the assumptions for the system model, the results show that the jamming attacks debilitates the performance metrics drastically. For these reasons, we use the performance metrics of SINR, PDR, goodput, energy consumption, and the analysis of the RSSI values to completely analyze the attackers.

Additionally, to provide a complete analysis of the jamming strategies, we analyze the strengths and weaknesses of each approach from the attackers' view. Extensive research and categorization of the attacks, with their respective characteristic, is made in several works [5, 6, 41, 42]. These works shows that the different attack strategies have different impact, energy consumption, implementation complexity, and stealthiness on the network.

Therefore, to analyze the implemented attacks in our experimental testbed, we use the criteria proposed in the previously mentioned works:

- Implementation Complexity : The attack complexity depends on variables as the knowledge, and understanding of the communication protocols by the attacker and the complexity to implement the algorithms of the strategy. Also, some strategies require specifical hardware to achieve the implementation.

- Energy consumption: The attacker and the constrained nodes in the networks aim to consume the minimum power possible to perform the attack. With lower energy consumption, the attacker can make the attack more efficient with the same impact on the network.

- Impact: The impact of the attack is determined by the extension of the network that is compromised by the effect of the attack. Also, the percentage of blockage of the messages is considered.

- Stealthiness: If the attack does not provoke the initialization of the countermeasures integrated into the nodes, the attack will be undetected by the system. This behavior is possible if the attack is well performed.

Then, to compare the strengths and weakness of each jammer strategy, we tabulate the used criteria in Table 5.1 to clarify their respective performance on each of them. These strategies were chosen owing to the impact on the networks and the differences on the implementation complexity, the energy efficiency, and the stealthiness between the constant and reactive approach.

Table 2.1: Comparative analysis of the different jamming models according to the chosen criteria with the implemented jamming in our work.

| **Jamming Model** | **Implementation Complexity** | **Energy Efficiency** | **Stealthiness** | **Impact** |
|---|---|---|---|---|
| Constant | Low | Low | Low | High |
| Wide Band Denial | Low | Low | Low | High |
| Reactive | High | High | Medium | High |

Several works of jamming attacks were reviewed to be used in our study. Therefore, in Table 2.2 we provide the principal works chosen to analyze and guide our work with their principal contributions.

Table 2.2: An Overview of the works on the use of jamming attacks used in our work.

| **Authors** | **Year** | **Contributions and Concepts** |
|---|---|---|
| Amuru et al. [26] | 2017 | The study uses the outage probability metric in a Base Station (BS) to Access Point (AP) link under a different number of jammers to observe the behavior of the communication link. Specifically, it is seen that with only 1 jammer per BS/AP, the outage probability of the wireless network can be increased from 1% (in the non-jamming case) to 80 % and when retransmissions are used, the effective network activity factor (interference among the BSs) can be doubled. Furthermore, they also analyzed the error probability of the victim receiver, both from a simulation and a theoretical perspective, to show that the exact error probability expressions can be evaluated for binary modulations. |
| Bayraktaroglu et al. [30] | 2008 | The study comprises a theoretical analysis of the saturation throughput of 802.11 under jamming, an extensive simulation study, and a testbed to conduct real-world experimentation of jamming IEEE 802.11 using GNU Radio and the USRP platform. The author uses a discrete-time Markov chain analysis to derive formulae for the saturation throughput of IEEE 802.11 under memoryless, reactive, and omniscient jamming. |
| Cheng et al. [39] | 2019 | The study shows that an attacker can reverse engineer the channel hopping sequences by silently observing the channel activities and put the network in danger of selective jamming attacks, bringing severe threats into WSANs by the presentation of two case studies using publicly accessible TSCH implementations. The paper provides a series of insights gathered from their analysis and case studies to secure the TSCH channel hopping by increasing the cracking difficulty. |
| Li et al. [7] | 2010 | The work-study the idealized case of perfect knowledge by both the jammer and the network about the strategy of each other and the case where the jammer and the network lack this knowledge. The latter is captured by formulating and solving optimization problems where the attacker and the network respond optimally to the worst-case or the average-case strategies of the other party. Their results provide insights into the structure of the jamming problem and associated defense mechanisms and demonstrate the impact of knowledge as well as the adoption of sophisticated strategies on achieving desirable performance. |
| Lopez et al. [15] | 2019 | The authors simulate the presence of an attacker in an LLN with IPv6 over the Time-slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e and the most recent Orchestra mode. The results show remarkable variations, in terms of Packet Data Rate (PDR) and energy efficiency, in the simulated scenarios when a malicious node is present, despite the Medium Access Control (MAC) mode used. Specifically, the PDR shows a variation of 20% and the energy consumption 20% in the jamming scenario. |
| Lopez et al. [16] | 2020 | The authors evaluate the impact of the capture effect inan IEEE 802.15.4 WSN based on unslotted-CSMA/CA in the presence of an attacker, considering different values of back-off. Additonally, the capture effect for multiple values of SINR and back-off in terms of Packet Reception Rate (PRR) and goodput is analyzed . The results shows that the PRR-to-SINR and the goodput show that for SINR values higher than 4.5dB , the PRR is almost 0.99, and the goodput 3048.38 bps, despite the backoff exponent (BE) used value. |
| Lu et al. [28] | 2014 | The works provide an in-depth study on the impact of jamming attacks against time-critical smart grid applications by theoretical modeling and system experiments by the introduced metric of message invalidation ratio to quantify the impact of jamming attacks. It is showed that via both analytical analysis and real-time experiments that there exist phase transition phenomena in time-critical applications under a variety of jamming attacks. Therefore, the authors designed the JADE system to achieve efficient and robust jamming detection for power networks. |
| Proano and Lazos [43] | 2010 | The work shows the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol, showing that such attacks can be launched by performing real-time packet classification at the physical layer. Also, the authors examine the combination of cryptographic primitives with physical-layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attacker. |
| Spuhler et al. [31] | 2014 | The authors show that the chip error rate-based metric is superior to metrics used in the literature, offering an accurate and reactive indicator of the true PDR. To validate this, they design and evaluate a detection technique relying on this metric to detect reactive jammers by building a software-defined radio testbed and show that their technique enables the error-free detection of reactive jammers that jam all packets on links with a PDR above 0.3. |
| Wilhelm et al. [40] | 2011 | The authors of this work propose a prototype of real-time reactive jamming implemented on an SDR USRP2. Using this prototype, the authors provide insights into the causes for loss and offered guidelines for successful reactive jamming against WSNs with an experimental study on physical layer effects in a system using MICAz motes. In summary, the work demonstrates that reactive jamming should be considered a serial threat to wireless networks. Thus research in jamming countermeasures becomes an even more important and delicate research issue in the future. |

Finally, with the performance metrics and criteria selected, we focus on the characterization of the system model. This model will be implemented using the IEEE 802.15.4 standard in a proposed experimental testbed to acquire the performance metrics. Therefore, in the next chapter, we review the PHY and MAC layer of the standard with the theoretical model. Then, to validate this study, the acquired experimental data will be correlated with the analytical values obtained from the theoretical model.

# Chapter 3

# IEEE 802.15.4 System Description

In this chapter, we review the main concepts associated with the WSN that uses the standard IEEE 802.15.4 and the principal requirements in the implementation. We also present the theoretical model that characterizes the system model to be correlated with the proposed experimental testbed.

## 3.1 General Description

The standard IEEE 802.15.4 is a Low-Rate Wireless Personal Area Network (LR-WPAN) standard aimed at providing simple, low-cost communication networks. LR-WPANs are intended for short-range operation and involve little or no infrastructure. In this context, the WSN is one of the most used LR-WPAN to acquire data from different environments with limited power, low-cost, and reliable data transfer. The mentioned characteristics are the main objectives that the standard pursuits to cope with the wide range of devices that operates using the standard. However, the networks can be developed based directly on the IEEE 802.15.4 or based on another protocol which is itself built on IEEE 802.15.4 (for example, the mentioned specifications ZigBee and WirelessHART).

## 3.2 Components and Topologies

The composition of an IEEE 802.15.4 network may use different devices with singular functions and capabilities. The devices are divided into two classes: Full-Function Device (FFD) and Reducted-Function Device. The FFD devices communicate between devices of their similar or different class; on the contrary, the RFD devices only communicate with a similar class. As a consequence, only the FFD devices could assume the coordinator function in a network, and always at least one of these types of the device needs to be present in the conformation of a network. However, exist FFD that are programmed with the function of an end device as RFD in some applications.

Some application scenarios require different topologies of the network to fulfill the requirements of the designer. The star and point-to-point (P2P) topologies are the defined arrangement of devices defined in the standard, as presented in Figure 3.1. In a P2P topology, the devices only communicate with other devices in the range of communications. On the contrary, the star topology admits the communications between the coordinator and the end devices that are not necessarily in the transmission range of the coordinator by the use of router nodes .

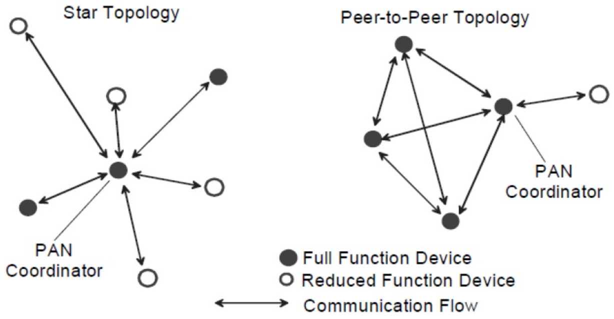


Figure 3.1: Topologies and nodes specified in standard IEEE 802.15.4

## 3.3 PHY Layer

The standard IEEE 802.15.4 defines two physical layers (PHY) to enable the communications of the nodes in different applications. The ISM band 2.4 GHz and the band 868/915- MHz are specified in the standard. The election of the band of frequency to use in communication depends on local regulations and user preference. However, only the unlicensed 2.4 GHz band is considered in this work to be analyzed under the jamming attacks. A total of 16 channels are available in the 2.4 GHz band, numbered 11 to 26, each with a bandwidth of 2 MHz and a channel separation of 5 MHz. Additionally, the output power of the nodes are around 0 dBm and typically operates within a $50 - 100$m range.

### 3.3.1 DSSS transmission

The Direct Sequence Spread Spectrum (DSSS) transmit scheme used in 802.15.4 is designed to promote co-existence. The basic idea is to use more bandwidth than is strictly required, thus spreading the signal over a wider frequency band. This is achieved by mapping the incoming bit-pattern into a higher data-rate bit sequence using a “chipping” code. Since the signal is spread over a larger bandwidth, narrow-band interferers block a smaller overall percentage of the signal, allowing the receiver to recover the signal.

Depending on the communication mode employed by the nodes, the PHY layer could be divided into

- 868/915 MHz direct-sequence spread spectrum (DSSS) PHY employingbinary phase-shift keying (BPSK) modulation.
- 868/915 MHz DSSS PHY employing offset quadrature phase-shift keying(O-QPSK) modulation.
- 868/915$MHz$ parallel sequence spread spectrum (PSSS) PHY employing BPSK and amplitude shift keying (ASK) modulation.
- 2450 MHz DSSS PHY employing O-QPSK modulation.

IEEE 802.15.4 uses one of 16 nearly orthogonal 32-chip long PN sequences to represent one of 16 symbols . In all these systems, multiple repetitions of known symbol sequences in the preamble provide the receiver with sufficient processing gain for a more reliable decision about the presence of a signal. Non-coherent energy detection on the other hand does not take advantage of this processing gain and hence suffers from a poor signal-to-noise ratio leading to unreliable channel state decisions.

The functions carried out by the PHY layer consists in:

- Activation and deactivation of the devices.
- Perform the process of Energy Detection (ED) and Link Quality Indicator (LQI).
- Execute the sensing process of the Clear Channel Assessment (CCA) for the CSMA/CA algorithm.
- Transmission and reception of the data units.

### 3.3.2 Clear Channel Assesment (CCA)

The process for the ED and the obtention of the LQI parameter varies between the different devices according to the five modes that the CCA support.

1. CCA Mode 1: Energy above threshold. CCA shall report a busy medium upon detecting any energy above the ED threshold. In the XBee devices, this is configured using the CA parameter.

2. CCA Mode 2: Carrier sense only. CCA shall report a busy medium only upon the detection of a DSSS signal. This signal may be above or below the CA threshold configured by the user.

3. CCA Mode 3: Carrier sense with energy above threshold. CCA shall report a busy medium upon the detection of a DSSS signal with energy above the ED threshold.

4. CCA Mode 4: CCA Mode 4: Carrier sense with timer. CCA shall start a timer whith a configured duration in ms and report a busy medium only upon the detection of a High Rate PHY signal. CCA shall report an idle medium after the timer expires and no High Rate PHY signal is detected.

5. CCA Mode 5: A combination of carrier sense and energy above threshold. CCA shall report busy at least while a High Rate PPDU with energy above the ED threshold is being received at the antenna.

According to the detailed in the datasheet of the device [1], the XBee is configured in CCA Mode 5 with the existence of a delay configured by the backoff exponent (BE) between the sensing and the transmission.

### 3.3.3 PPDU Format

The PHY protocol data unit (PPDU) packet structure consists of the encapsulation of various fields. The fields that the PPDU encapsulates are the following:

- The SHR field , which integrates the preamble field that has a length of 8 symbols for the O-QPSK modulation, and the SFD field that indicates the end of the SHR and the start of the packet data.

- The PHR field, which encapsulates the frame length field that specifies the total number of octets contained in the PHY payload, and the PSDU field corresponds to the payload.

### 3.3.4 Encoding

Four bits of the 250 kbps input data of the PPDU are mapped into a symbols. The symbol is then used to select one of 16-ary orthogonal PN sequences which are to be transmitted and results in 2 Mchips/s , which is used to convert a narrow band signal into wide band signal. It also provides resistance to intended or unintended jamming and achieves reduced signal/background-noise level which hampers interception. Since the time average of modulated chip sequence is zero, there is no DC component in the modulated signal .This spread signal is half sine pulse shaped using the signal given by

$$\begin{cases} p(t) = sin(\frac{\pi t}{2T_c}) & 0 \leq t \leq 2T_c \\ 0 & \text{otherwhise.} \end{cases}$$

This pulse shaped signal is modulated using O-QPSK modulation at the frequency of 2.4 GHz and transmitted. The different process for the PPDU to be finally transmitted is represented in Figure 3.2

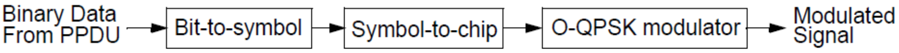


Figure 3.2: Modulation and spreading functions for the O-QPSK PHYs

### 3.3.5 Capture Effect

Capture Effect (CE) is the ability of wireless devices to capture a packet despite interference or collisions during transmission. The CE probability will depend on the power ratio between the signals that collide. Therefore, the power ratio between the carrier signal $RSS_c$ and the sum of the interfering signal $RSS_\text{i}$ as SINR is used. Later, the CE is analyzed for different values of SINR to found the probability to capture packets despite collisions.

To evaluate the number of transmissions that could be decoded at reception, the analysis of the PRR-to-SINR ratio is used. The relationship between both metrics has been studied in the scientific literature, to evaluate SINR intervals that allow guaranteeing the correct reception of a certain number of packets. Depending on the modulation of the signal used and the implementation scenario, there are different proposed regression models. In this work, the PRR-to-SINR is analyzed for OQPSK modulation with jamming-type attacks to verify in the future a model that coincides with the experimental results.

In order to obtain the signal strengths, devices using the IEEE 802.15.4 [4] standard use an Energy Detection (ED) mechanism for over 8 symbol periods (128$\mu$S) to grant a Received

Signal Strength Indicator (RSSI) value. This RSSI value is used to obtain the values to be used in the SINR equation and we denote them as $RSS_C$ for the legitimate transmitter and $RSS_I$ for the interferers.

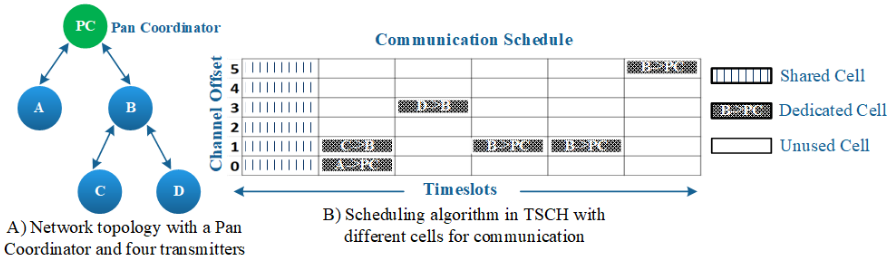
## 3.4 MAC layer

Multiple algorithms are defined in the MAC layer for the standard IEEE 802.15.4 that can be implemented in different scenarios. The methods CSMA/CA, TSCH with CCA, CSMA with Prioritized Contention Access (PCA), and ALOHA with PCA is the random access methods defined in the standard. The CSMA/CA and TSCH methods are analyzed in our work because they are implemented in multiple scenarios.

### 3.4.1 Time Slotted Channel Hopping

TSCH was designed to allow IEEE 802.15.4 devices to support a wide range of applications. This support is possible through the use of time synchronization to specify different time slots for distinct traffic. Also, channel hopping mechanisms can be configured to achieve high reliability. The accuracy of the synchronization is critical to guarantee the lowest power consumption possible. However, the TSCH algorithm does not amend the PHY layer, and it can operate in any hardware that is compliant with IEEE 802.15.4. Moreover, it can be used in conjunction with IPv6-enable protocol stack for LLNs as RFC6550, Constrained Application Protocol (CoAP) RFC7252.

The standard IEEE 802.15.4e only defines the mechanisms for a TSCH node to communicate, but it does not define the policies to build and maintain the communication schedule, adapt the resources allocated between neighbor nodes to the data traffic flows, and others. Summarizing the TSCH is designed to allow optimizations by the simplification in the integration with another protocol stacks based on IPv6, 6LoWPAN, and RPL.



A) Network topology with a Pan Coordinator and four transmitters

B) Scheduling algorithm in TSCH with different cells for communication

Figure 3.3: Example of a network composed of one coordinator and four transmitters using the TSCH algorithm.

#### Orchestra

The last improvement to the TSCH mode is called Orchestra [44]. Orchestra mode combines the mechanisms of different channels and times with the addition of autonomous scheduling of communications as represented in Figure 3.4. This communication scheduling achieves a better performance of the nodes in terms of Packet Data Rate (PDR) and energy efficiency by the calendarization of the different traffic in the communications

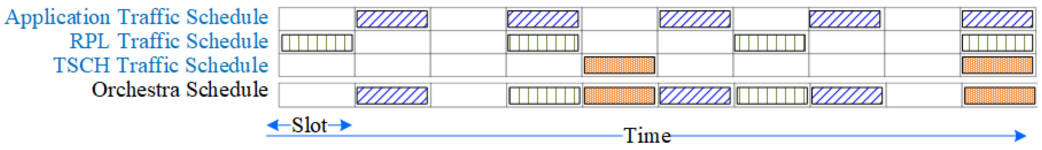


Figure 3.4: Different types of scheduling that the Orchestra mode uses to communicate the data.

### 3.4.2 CSMA

The devices that use the IEEE 802.15.4 standard with the CSMA/CA algorithm, before transmitting a packet, choose a random integer value between $[0, 2]$. The backoff exponent (BE) value within this range is initialized by the configuration of the macMinBE parameter. Then, each time that the sense mechanism asses the channel busy, the BE value will be incremented by one. The maximum value that the BE can grow is determined by the macMaxBE parameter. If the algorithm CSMA/CA reaches the macMaxBE value and also the maximum number of retransmissions macMaxFrameRetries then the packet is discarded. Consequently, retransmission is initialized with the default values of macMinBE and macCSMABackoffs. For networks using acknowledgment frames (ACK) in the transmission, the value of BE is set to macMinBE after the reception of the ACK.

Multiple reasons lead to the retransmission of the packets in the networks using CCA with interference. If the sensing process asses the channel as busy in one of the two scans, it means that the noise in the channel is over the CCA Threshold. Therefore, a backoff time can ensure to find the channel free the next time. However, the presence of high noise, simultaneous transmissions, the coexistence with other networks, and other variables in the medium channel reduces the probability to initiate a transmission, and also the probability of collisions. Consequently, the retransmission of the packet will occur. Although, the retransmissions can experiment collisions or losses, that the sense mechanisms can not solve.

#### Unslotted Mode

The CSMA/CA algorithm can be programmed to use beacons in the transmission for the Contention Access Period (CAP) that is namely slotted mode. Also, the algorithm can work without beacons in the CAP, which is known as the unslotted mode as shown in Figure 3.5. In both cases, the algorithm is implemented using units of time called backoff periods, where one backoff period shall be equal to aUnitBackoffPeriod. In slotted CSMA-CA, the backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries defined by the coordinator of the PAN . Also, the MAC sublayer shall ensure that the PHY commences all of its transmissions on the boundary of a backoff period. On the contrary, in unslotted CSMA-CA, the backoff periods of one device are not related in time to the backoff periods of any other device in the PAN.

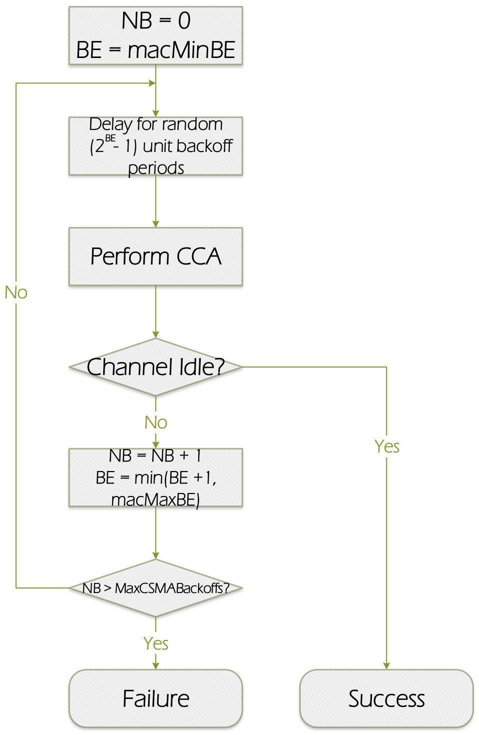


Figure 3.5: IEEE 802.15.4 CSMA/CA Algorithm Unslotted Mode

Each device shall maintain three variables for each transmission attempt: NB, CW, and BE. NB is the number of times the CSMA-CA algorithm was required to back off while attempting the current transmission. In the used devices the firmware allows more retransmissions controlled by the RR parameter. CW is the contention window length, defining the number of backoff periods that need to be clear of channel activity before the transmission can commence. The value of shall $CW_0$ be initialized to two before each transmission attempt and reset to CW= 0 each time the channel is assessed to be busy. The CW variable is only used for slotted CSMA-CA. BE is the backoff exponent, which is related to how many backoff periods a device shall wait before attempting to assess a channel. For the used devices, the RN parameter permits the control of the macminBe.

### 3.4.3 Analytical model

Multiple works focus on model the MAC and PHY layer of the standard IEEE 802.15.4 using different analytical models. Inspired by the work realized by Bianchi [23], various authors used the Markov Chains approach to model the IEEE 802.15.4 states and transitions. In [19], the authors used the Discrete-Time Markov Chains (DTMC) to provide an analytical model for the description of the transition between node states of the CSMA/CA 802.15.4 MAC protocol. The proposed MAC model is built as a state-transition diagram that analyzes and derives the probabilities that a node succeeds in the access to the channel, in the transmission of its packet, and the probability that the sink receives a packet coming from any node.

The unslotted CSMA/CA is used in this work and illustrated to the process presented in Figure 3.5, starting from when the node has data to be transmitted. The states that the node can be in the CSMA/CA process are backoff, sensing, transmission, or idle and are modeled as a bidimensional process $Q(t)$. The variables $BO_C(t)$ and $BO_S(t)$ represent the backoff time counter and the backoff stage (i) that corresponds to time-discrete stochastic processes. As a consequence, the process constitutes a chain, but given that the $BOC(t)$ is not a memoryless process, it can not be modeled as a Markovian chain. The initial value of $BO_C(0)$ is uniformly distributed in the range $[0, W_{NB} - 1]$, where $W_{NB} = 2^{BE}$ is the dimension of the contention window. The value of BE depends on the second process characterizing the state $BO_s(t)$. In Table 3.1 the different backoff stages with the correspondent $W_{NB}$ values are shown.

Table 3.1: The different values of BOS,NB,BE and WNB.

| **BO$_S$** | **NB** | **BE** | **W$_{NB}$** |
|---|---|---|---|
| 0 | 0 | 3 | 8 |
| 1 | 1 | 4 | 16 |
| 2 | 2 | 5 | 32 |
| 3 | 3 | 5 | 32 |
| 4 | 4 | 5 | 32 |

Then, the transition diagram is built from the initial values NB= 0 and BE= 3. Next, each time the channel is sensed busy, NB and BE are increased by 1. When BE reaches its maximum value, there is no more increase. The case BO$_s$ = 4 is the last case because here, NB reaches its maximum value, and it cannot be increased any further. Following the detailed methodology, the transition diagram is modeled for each BO$_s$ = 0, 1, 2, 3, 4 and Figure 3.6 represents the station diagram that represents the first of the five backoff stage that characterizes the complete process.

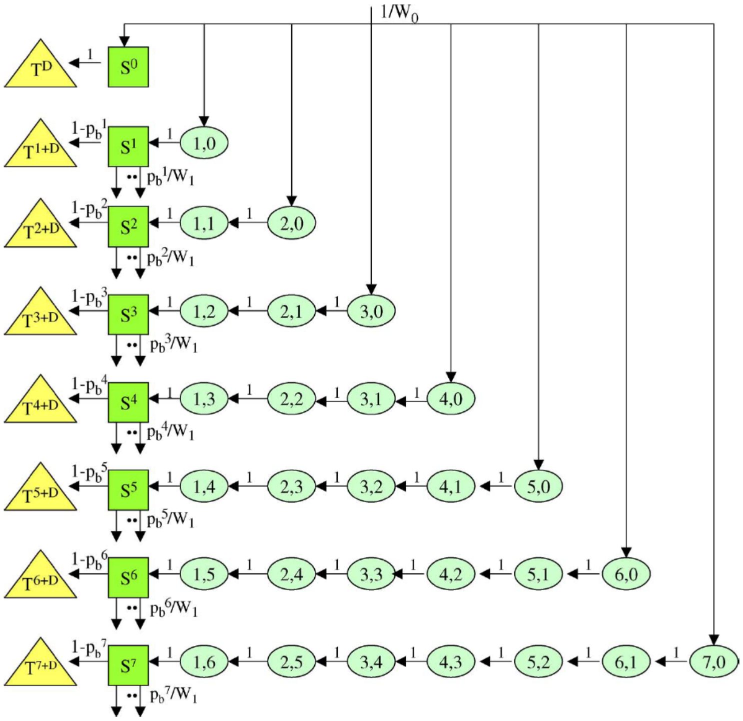


Figure 3.6: State-transition diagram related to the first backoff stage. The others transition diagram are obtained with a similar approach.

The first step to obtaining the different states and transition probabilities is to determine the sensing probabilities $P\{S_{\mathrm{i}}^{j}\}$. To obtain the values of the five sensing states, a single node behavior is used to describe the relationship between all the possible states in which a node can be. Then, the calculated values are used to obtain the probabilities for different slots, backoff stage, and numbers of nodes.

Denoting as $P\{\mathrm{BO}_c = c_1, \mathrm{BO}_s = \mathrm{i}_1, t = j_1 | \mathrm{BO}_c = c_0, \mathrm{BO}_s = \mathrm{i}_0, t = j_0\} = P\{c_1, \mathrm{i}_1, j_1 | c_0, \mathrm{i}_0, j_0\}$ the transition probability from state $\{c_0, \mathrm{i}_0, j_0\}$ to state $\{c_1, \mathrm{i}_1, j_1\}$ the transition probabilities between backoff states are given by

$$P\{c, 0, j+1 | c+1, 0, j\} = 1. \tag{3.1}$$

This equation denotes that at the beginning of each time slot, the backoff time counter is decreased by 1 until it reaches the zero value with probability 1. This transition probability between the backoff states, is equal for all the backoff stages $i$ that characterizes the IEEE 802.15.4 unslotted mode.

With the transition probabilities acquired, the sensing probabilities $\mathrm{P}\{S_{\mathrm{i}}^{j}\}$ are obtained for each backoff state. This probability depends on the values of $\mathrm{W}_{NB}$, $p_b^j$, and it is calculated iteratively with the initial values given by

$$P\{S_0^j\} = \begin{cases} \frac{1}{W_0}, & \text{for } j \in [0, W_0 - 1] \\ 0, & \text{for } j > W_0 - 1 \end{cases}. \tag{3.2}$$

Then, depending on the slot value and the length of the window of the backoff time, the sensing probabilities are determined for different ranges by

$$P\{C^j\} = \begin{cases} P\{S_0^0\}, & \text{for } j = 0 \\ P\{S_0^1\}, & \text{for } j = 1 \\ \sum_{\mathrm{i}=0}^{j-1} P\{S_{\mathrm{i}}^j\}, & \text{for } j = (2, ..., 4) \\ \sum_{\mathrm{i}=0}^{NB_{max}} P\{S_{\mathrm{i}}^j\}, & \text{for } j = (5, ..., W_0 - 1) \\ \sum_{\mathrm{i}=1}^{NB_{max}} P\{S_{\mathrm{i}}^j\}, & \text{for } j = (W_0, ..., W_{0,1} - 1) \\ \sum_{\mathrm{i}=2}^{NB_{max}} P\{S_{\mathrm{i}}^j\}, & \text{for } j = (W_{0,1}, ..., W_{0,1,2} - 1) \\ \sum_{\mathrm{i}=3}^{NB_{max}} P\{S_{\mathrm{i}}^j\}, & \text{for } j = (W_{0,1,2}, ..., W_{0,1,2,3} - 1) \\ P\{S_4^j\}, & \text{for } j = (W_{0,1,2,3}, ..., W_{0,1,2,3,4} - 1) \end{cases}, \tag{3.3}$$

where $NB_{max}$ indicates that the maximum number of admitted retransmissions has been reached. The sensing states can be initialized in differents window lengths that are determined by the actual number of the NB value and is represented as $W_{NB}$ depending on the backoff state of the chain.

These and the following formulas are present in the three works presented by Buratti, and to be applied to this work, we perform correlations of the concepts with the different formulas to correctly obtain the state and transition probabilities of the state transition diagram. The model assumptions that are correlated to this work are presented in [19, 20, 25] and here concisely present.

- All nodes start the backoff algorithm at the same time.
- We assume that each node only has one packet per round to be transmitted
- In the model, the resolution time (hereafter denoted as slot) is set equal to $\mathrm{d}_b$, which corresponds to the duration of the backoff period, of the sensing phase, and of the packet transmission time when $D = 1$.
- Ideal channel conditions are assumed: All the nodes can "hear" each other, and therefore, no hidden terminal problem is accounted for.
- Collisions between nodes may occur in case two or more nodes perform channel sensing at the same time, find the channel free, and simultaneously transmit their packets.
- No acknowledge and retransmission mechanism is implemented; therefore, when a packet collides, it is definitely lost in that round.

For clearness , the list of variables used in this work, is presented in Table 3.2.

Table 3.2: Definition of variables used in the description of the analytical model.

| **Variable** | **Description** |
|---|---|
| BE | Backoff Exponent |
| $\mathrm{BO}_C$(t) | Backoff counter at slot t |
| $\mathrm{BO}_S$(t) | Backoff stage at slot t |
| D | Length of the packet expressed in backoff period time |
| $\mathrm{d}_b$ | Backoff Period with duration equal to 320$\mu$s |
| $\mathrm{f}^j$ | Probability to find the channel free in slots j-1 and j |
| j | Correspond to the slot related to the time slot from jdb to j+1 db |
| NB | Number of times that the CSMA/CA algorithm was required to backoff |
| $\mathrm{p}_b^j$ | Probability that in the jth slot the channel is found to be busy after sensing |
| $\mathrm{p}_s$ | Probability that a node succeeds in transmitting its packet in a round whatever the slot. |
| $\mathrm{P}\{\mathrm{C}^j\}$ | Probability of being in a sensing state at the jth slot |
| $\mathrm{P}\{\mathrm{R}^j\}$ | Probability that the sink receives the packet tail, coming from whatever node in a given slot |
| $\mathrm{P}\{\mathrm{S}_\mathrm{i}^j\}$ | Probability of being in a sensing state at the jth slot and at the ith backoff stage |
| $\mathrm{P}\{\mathrm{T}^j\}$ | Probability that a node ends the transmission of its packet in a given slot |
| $\mathrm{P}\{\mathrm{Z}^j\}$ | Probability that a successful transmission ends in slot j |
| Q(t) | Node state modeled as bidimensional process that depends on $\mathrm{BO}_C$ and $\mathrm{BO}_S$. |
| t | Integer value that represents the time slot |
| $\mathrm{T}_s$ | Symbol time equal to 16$\mu$s |
| $\mathrm{W}_{NB}$ | Length of the contention window for each backoff stage |
| $\alpha$ | Protection ratio from each enviroment acquired from the experimental methodology in [25] |
| $\beta$ | Propagation constant |

### Peformance Metrics

With the probability of sensing determined, it is important to know the probability to found the channel busy after the sensing was performed. The channel is busy if a transmission is detected in the channel conditioned on the fact that the channel in the previous slot was free or busy, depending on the case. Therefore, the derivation to found the channel busy using the probability that the channel in certain slot is free as $p_f^j$ we have

$$p_f^j = \begin{cases} (1-p_b^{j-1}) \prod_{\mathrm{i}=0}^{NB_{max}} (1-P\{S_{\mathrm{i}}^{j-1}\})^{N_c^{j-1}-1} + p_b^{j-1}, & \text{for } D=1 \\ (1-p_b^{j-1}) \prod_{\mathrm{i}=0}^{NB_{max}} (1-P\{S_{\mathrm{i}}^{j-1}\})^{N_c^{j-1}-1} & , \\ +(1-p_b^{j-D-1} \cdot [1-\prod_{k=0}^{NB_{max}} (1-P\{S_{\mathrm{i}}^{j-D-1}\})^{N_c^{j-D-1}-1}, & \text{for } D>1 \end{cases} \tag{3.4}$$

Therefore, the channel is free if the other nodes $N_c$ are not sensing or transmitting in the same slot j. Consequently, the probability of founding the channel busy is

$$p_b^j = 1 - p_f^j. \tag{3.5}$$

With the probabilities of sensing, found the channel free, and found the channel busy, the probability in which a transmission terminates can be calculated by

$$P\{T^j\} = P\{C^{j-D}\}(1-p_b^{j-D}), \tag{3.6}$$

that evaluates the probability that a generic node ends its packet transmission in slot $j$. Additionally, the probability is null for all $j < D$.

However, the probability of $P\{T\}$ does not account for successful transmissions of a generic packet. Using the law of total probability with the Equations (3.3),(3.5) we have

$$P\{Z^j\} = (1-p_b^{j-D})P\{C^{j-D}\} \prod_{\mathrm{i}=0}^{NB_{max}} (1-P\{S_{\mathrm{i}}^{j-D}\})^{(N_c^{j-D-1})}, \tag{3.7}$$

where $P\{Z^j\}$ is the probability that a successful transmission ends in slot j, which means that one and only one transmission starts in the slot j-D+1. Assuming that all nodes can hear each other, if in slot j- D+1 only one node starts its transmission, then the sink will correctly receive (i.e., without collisions) the end of the packet in j. Therefore, the probability to correctly receive the tail of the packet is calculated

$$P\{R^j\} = N_c^j \cdot P\{Z^j\}. \tag{3.8}$$

When the capture effect is taken into account, the probability to correctly receive a packet $P\{Z^j\}$ needs to be extended [25]. Due to the capture effect owe to the signal strength of the signals, a protection ratio is added. Also, the ability to capture effect takes into account the existence of nodes that interferes with communication. Therefore, the nodes that provoke the collision as interferences ($N_{\mathrm{i}}$) can be a random number of nodes in the network that is model as a binomial coefficient. Consequently, a protection ratio is included ($p_{c,N_{\mathrm{i}}}$) to model the probability that a packet is captured when the $N_{\mathrm{i}}$ interfering nodes are present.

$$P\{Z^j\}_{CE} = f^{j-D} \cdot P\{C^{j-D}\} \cdot p_{c,N_{\mathrm{i}}} \cdot \binom{N_c - 1}{N_{\mathrm{i}}} \cdot P\{C^{j-D}\}^{N_{\mathrm{i}}} \prod_{\mathrm{i}=0}^{NB_{max}} (1-P\{S_{\mathrm{i}}^{j-D}\})^{(N_c - N_{\mathrm{i}} - 1)}. \tag{3.9}$$

We remark that the probability $P\{Z^j\}$ accounted for the capture effect is obtained using the slotted mode of the CSMA/CA algorithm. Consequently, the probabilities inside of the

Equation (3.9) needs to be correlated with the unslotted mode. The variations between the two models of the slotted and unslotted CSMA/CA and their correlations are the following:

- The probability $P\{C^j\}$ indicates the probability of being in the second sensing phase for all the backoff stages in the slotted mode. Conversely, for the unslotted mode, this probability accounts for all the sensing phases.
- The probability that the remaining nodes do not sense the channel in the slot j-D obtained by $\prod_{\mathrm{i}=0}^{NB_{max}}(1-P\{S_{\mathrm{i}}^{j-D}\})^{(N_c-N_{\mathrm{i}}-1)}$ is calculated considering only the second sensing phase. However, for the unslotted mode, this can happen in all sensing phases. Therefore we calculate the probability $P\{Z^j\}_{CE}$ for all the (i) range.
- For the joint probability to find the channel free in slot j $f^j$, we take into account the same assumption of the probability of the sensing phases for the $P\{Z^j\}_{CE}$.

Consequently, we correlate the concept of founding the channel free in the given slot, making $p_f^j = f^j$ to be used in the calculation of the probability $P\{Z^j\}$. Finally, the probability that a generic packet is successfully transmitted on the channel is given by

$$p_s = \sum_{j=0}^{t_{max}+D-1} P\{Z^j\}, \tag{3.10}$$

where the probability that a successful transmission ends can be used when the capture is taken into account or not. Figure 3.7 shows the probability $p_s$ for different packet sizes without the capture effect. The results show that for higher values of D, the probability of success tends to be lower. This behavior accounts for the fact that an increment of N or D produces a larger delay to each node accessing the channel. Additionally, this represents a high offered load of the traffic for the network.

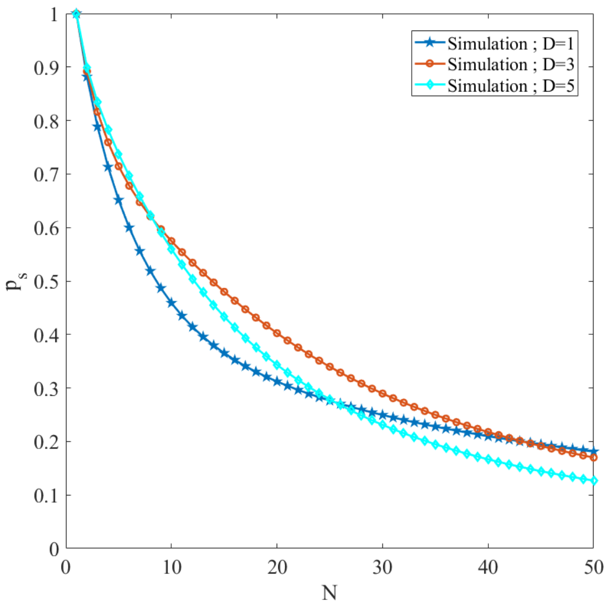


Figure 3.7: Probability of success for different length of the packets when the capture effect is not considered. The $p_s$ monotonically decreases by increasing N for all the length of packets analyzed. Additionally, the curves show that exists an optimum value of D that maximizes the $p_s$ depending on N.

Finally, to show how the capture effect varies, depending on the parameters $\alpha$ and $\beta$, we plot three cases in Figure 3.8, that corresponds to the curves with the colors green, purple, and yellow as stated in the legend of the figure. We remark that all plotted curves are acquired using a fixed length of packet $D = 2$. We also adjust the limit of axes to the presented in the original works [25].

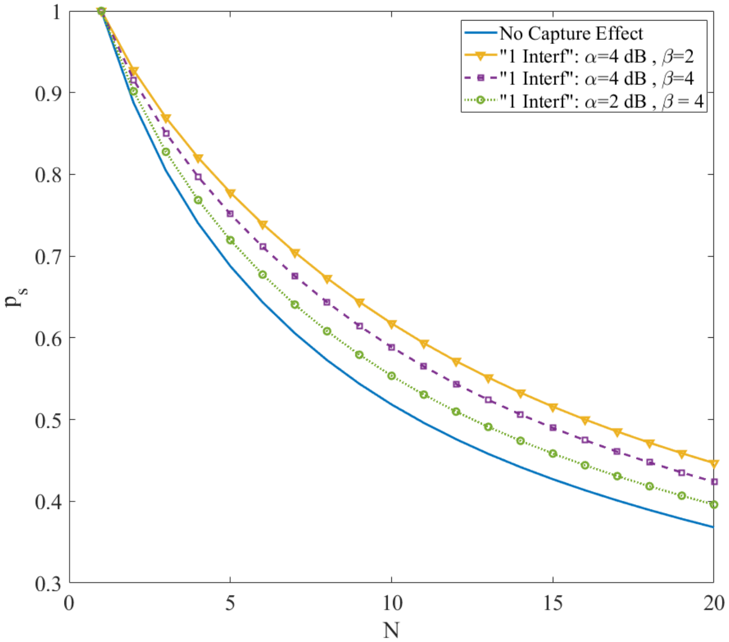


Figure 3.8: $p_s$ as a function of N when capture effect is considered and not for the unslotted mode and with a length of the packet $D = 2$. We use different values of $\alpha$ and $\beta$ to show the behavior of the capture effect that depends on these parameters. The capture effect is higher when $\alpha$ increase and $\beta$ decrease.

## 3.5 Jamming Attacks

The jamming attacks and their impact on the networks can be model considering the parameters of the incidence rate of the signal interference ($r_j$), the probability to interfere with the communication ($q_{\mathrm{i}}$), the synchronization between the signals ($\phi$), and the difference between the power of the interference signal and the power of the legitimate signal (SINR).

The rate of the jammer signal $r_j$ will be different for the different strategies and scenarios. The rate will vary depending on the length of the packet or the width of the pulse and the generation of the signal. Therefore, the different jamming strategies can be analyzed in terms of rate and their correlation with the impact and the energy consumption.

The level differences between the signals are usually treated as Signal-Interference plus Noise Ratio (SINR) or similar formulas than incorporates the effects of the attacker with a different approach. In this work, we add the power of the signal created by the attacker in the parameter of interference of the SINR.

$$\text{SINR}_{\text{d}B} = 10log_{10}\left(\frac{10^{RSS_c/10}}{\sum_{I=0}^{N_\text{i}} 10^{RSS_I/10} + 10^{N/10}}\right). \tag{3.11}$$

The mentioned parameters characterize the different jamming strategies that the attacker could adopt when decides to initiate a DoS in the WSN. However, to correctly differentiate the impact of the strategies, a parameter that correlates the attacker and the MAC model is mandatory. According to the works [45], the time when the signals collide permits to divide the analysis in different cases. In particular, the affectation of some fields of the packet is more critical than others when the reception of the packet is required.

To correctly differentiate the impact of the jamming strategies, a parameter that correlates the attacker and the MAC model is mandatory. According to the works the time when the signals collide permits to divide the analysis into different cases [27,40,45]. These cases will be divided according to the field of the frames that are involved in the collision.

The sync bytes and the header field are the most critical fields when the probability of receiving a packet is analyzed. Consequently, the time over the air of the different fields of the packet is essential in the analysis of the attacker. Here, we refer, and we differentiate the analysis of the attacker considering the preamble, sync bytes , and the headers of the packets as reference. Therefore, we determine the synchronization of the interference signal with the first fields of the packet as

$$\phi = \frac{t_a - t_b}{t_{pr} + t_{sc} + t_{h\text{d}}}, \tag{3.12}$$

where $t_a$ is the time when the legitimate packet initiates it transmissions, $t_b$ the time when the signal interference is generated, and $t_{total}$ the sum of the time that takes to transmit the first fields of the packet denoted as $t_{pr}$ $t_{sc}$ and $t_{h\text{d}}$ respectively. Later, the synchronization is transformed from time to slots to analyze each case.

Depending on the timing and the power of the signals in the communication, collision detection is possible in certain scenarios. This behavior is described as stronger-first and stronger-last scenarios where the legit user signal is analyzed with one interfere packet on the receiver side, Figure 3.9 presents a simplification of the realized experiments [45].Summarizing, when two packets arrive at the receiver, the collision detection will depend on the power of the signals and the time difference between the packets. Therefore, when interference is present in the communications, the analysis is divided into: the users can be identified or the users can not be identified. This identification process will depend on the range of values that the parameter $\phi$ can assume. When $0 \leq \phi < 1$ the users can not be identified, and when $\phi \geq 1$ the users can be identified.

Summarizing, if the preamble, sync, or headers bytes collides with the interferer packet, the receiver can not synchronize with the legitimate transmitter, or it can not capture the packet. Therefore, this transmission will be completed loss, and the identification of the users can not be achieved. We remark that this behavior is conditioned to the power of the signals that need to be determined for each application scenario.

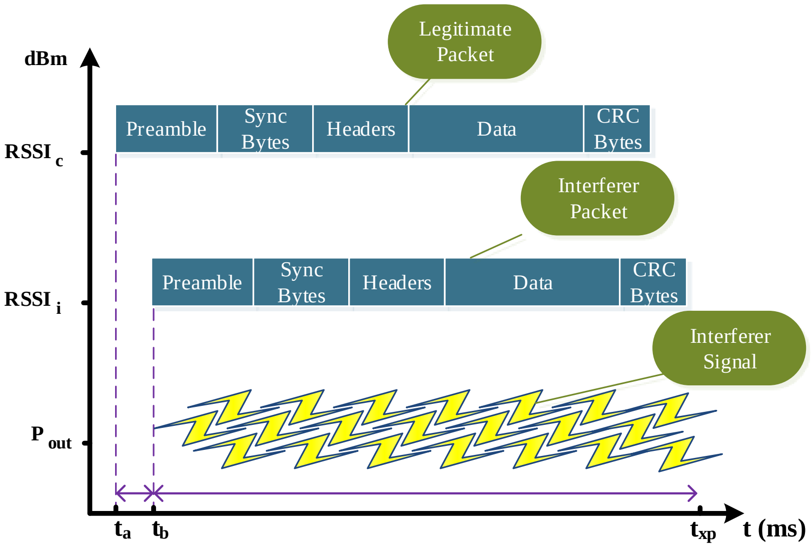


Figure 3.9: Description of the collision scenario for the different experiments. The difference between $t_a$ and $t_b$ divides the analysis of the collision and help to understand the behavior of the transmission under jamming attacks. We also show that the jamming strategy can be carried out using a data frame or noise injection.

The jamming attacks and their impact on the networks can be model considering the parameters of the incidence rate of the signal interference ($r_j$), the probability to interfere with the communication ($q_{\text{i}}$), the synchronization between the signals ($\phi$), and the difference between the power of the interference signal and the power of the legitimate signal (SINR).

The rate of the jammer signal $r_j$ will be different for the different strategies and scenarios. The rate will vary depending on the length of the packet, the width of the pulse, the generation of the signal, or the activity time in the experiments. Therefore, the different jamming strategies can be analyzed in terms of the total time in transmission state for each experiment.

Following the analytical model presented, we have to analyze the probability of the packets collides by the effect of the jamming strategy considering a different number of nodes. For a network composed by $N$ nodes, we have that $N_c$ contends for the channel in a given slot, and $N_{\text{i}}$ interferes nodes are present in the communications. When the interferes nodes are present, they can provoke constructive interference that can be analyzed under the capture effect concept. On the contrary, if the interfere nodes do not improve the reception of the packets, it means that destructive interference is present. Therefore, the interfere node can be interpreted as a jamming device in the network.

Considering $N_{\text{i}} = 1$ interferes with a destructive interference $\phi < 1$, the reception of the packet is analyzed using the SINR parameter. Therefore, the complement of the linear regression model that correlates the PRR to the SINR values, gives the probability of jamming

$$p_j = 1 - (\text{PRR-to-SINR}_{model}). \tag{3.13}$$

Then, the probability that a packet in the transmission collides with the jamming signal is equal to

$$p_j = 1 - ((1 - \frac{1}{2}\text{exp}(-\beta_0/2))^{8\beta_1 f}, \tag{3.14}$$

where $f$ is the frame size in bytes, $\beta_0$ the SINR obtained by experimental measurements, and $\beta_1$ corresponds to noise Bandwidth.

Expression (3.14) is valid only for $N_{\text{i}} = 1$ despite the numbers of $N_c$ nodes present in the network. If more interferes are present in the scenario, then is important to know the relative distance of the interferes to characterize the behavior of the PRR-to-SINR curve, the synchronization $\phi$ , and the number of interfere nodes in the communication channel regard the legitimates nodes.The regression model is accounted for OQPSK modulation in the 2.4 GHz frequency band, 250 Kbps of data rate with NRZ encoding [46].

The rate of constant jamming is $r_j = 1$, given that the interfere signal is always present in the communication channel. As a consequence, we could establish that the timing differences between the packets are equal to zero, and therefore the synchronization is total.

With a $\phi = 0$, we have that the collision of the packets can not be detected at all, and we assume that is by the effect of the jammer device. Therefore, we have that the jamming signal is generated independently of the communication process in the network, and we can calculate the probability to jam $p_{s_{jam}}$ as

$$p_{s_{jam}} = p_s \cdot p_j. \tag{3.15}$$

Therefore, $p_j$ will depend on the PRR for the different ranges of SINR according to the regression model.

The reactive strategy generates interference for some packets or activity in the network. To guarantee the collision, we assume that the jammer knows the time when the transmission is generated in the nodes. The times can be easily decoded by the attackers [39] for different MAC protocols. Therefore, the probability of jamming for the reactive strategy is the same as the constant strategy with different jamming rates that can be configured for the different scenarios.

The success probability for the existence of jamming strategies is calculated for a total number of nodes $N \geq 2$ due to is considered an interfering node. We plot the proposed model in Figure 3.10 for SINR values equal to 3.1 dB and 4 dB to show the behavior of the curve. The curves that consider the jammer show that for higher values of SINR, the probability of reception grows as we expected.

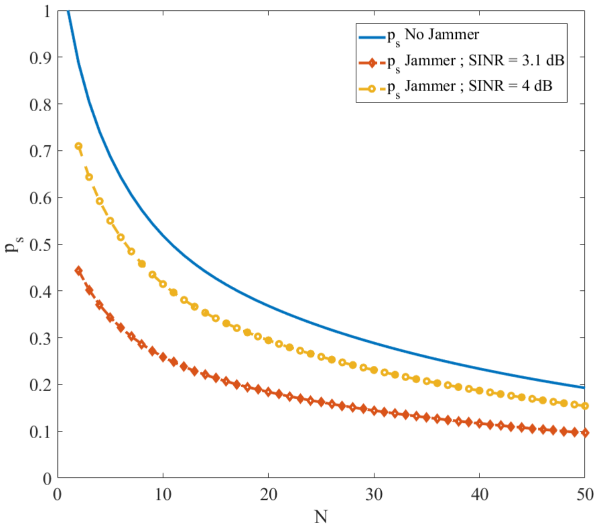


Figure 3.10: Probability of reception comparison between scenarios with the jammer ($N_{\mathrm{i}} = 1$) and not, with different probabilities to jam according to the regression model. We plot the probability of reception for two different values of SINR with the jammer to show that for higher values of SINR, the probability of reception grows.

Finally, we compare the capture effect with the proposed model of jamming to show the difference between them. Here, we assume a PRR of 0.5 to show the different plots in Figure (3.11). As we remark previously, all the curves plotted considers the length of the packets D = 2 to make a fair comparison between them and for the capture effect, we use the protection ratio $\alpha = 3.1$ dB that ensures a PRR= 0.5.

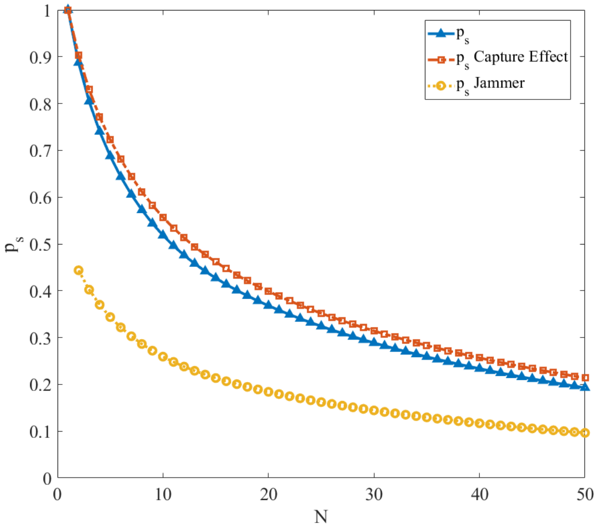


Figure 3.11: Probability of reception comparison between scenarios with the jammer, and the capture effect assuming a PRR of 0.5 for both curves. Also, the original model is shown. The used $\alpha = 3.1$ dB corresponds to protection ratio in concordance with assumption of an PRR = 0.5.

The extended proposed probabilistic model that includes the presence of jamming attacks exhibit a good correlation with the original assumptions. Specifically, for higher values of SINR, as shown in Figure 3.10, the impact of the jammer is negligible. Therefore, to validate the theoretical results, we propose a novel experimental testbed capable of acquiring metrics in the presence of jamming attacks.

# Chapter 4

# Experimental Testbed

In this chapter, we present a novel experimental testbed for WSN using the IEEE 802.15.4 standard to acquire performance metrics under jamming attacks. The devices used in the testbed consist of typical transceivers used in diverse applications with the presence of a sniffer that does not interfere with the conformed network. Additionally, the synchronization of the devices is guaranteed despite the presence of jamming attacks. Therefore, the proposed testbed can be used to correlate several probabilistic models with the presence or absence of jammer devices.

The proposed experimental testbed is composed of multiple nodes using the IEEE 802.15.4 standard with CSMA/CA is implemented to analyze the capture effect under jamming attacks. The Freescale MC1321x transceivers [3] perform the communication of the data in the network using the 2.4$GHz$ frequency band with OQPSK modulation. A single coordinator receives the data from the "N" transmitters to analyze the performance of the communications in a star topology. Additionally, a sniffer implemented in an SDR using the code in [47] is deployed in the same location as the coordinator to analyze the collisions. The code is modified to ensure that the SDR does not communicate with the other nodes, but can listen and record all the transmissions. In Figure 4.1 the different devices and instruments used for the experiments are shown.

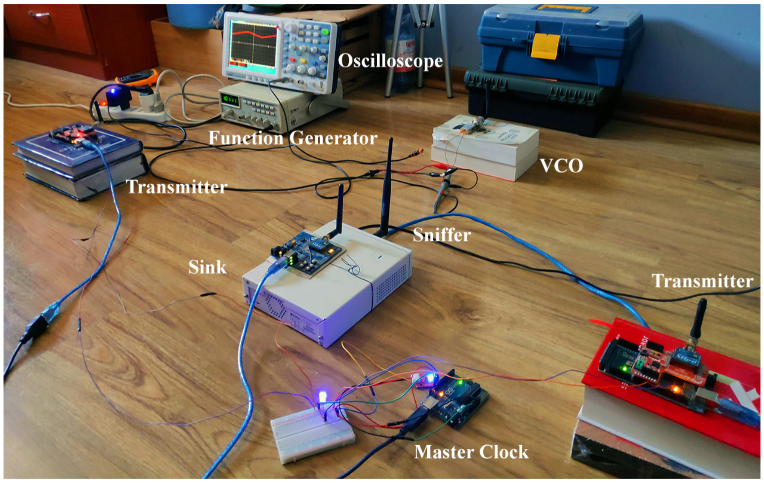


Figure 4.1: Network devices and instruments are used to obtain experimental data in the indoor environment that consists of a typical bedroom.

## 4.1 Hardware

The hardware used in the implementation of the WSN consists of XBee S1 devices [1] as the constrained nodes. The principal characteristics are the following :

- Incorporates the MC1312x transceiver by NXP Semiconductors [3].
- Point-to-multipoint network topology.
- Low-power sleep modes.
- 2.4 GHz for communications with O-QPSK modulation.

The MC1312x transceiver is similar in characteristics to the CC2420 [48] transceiver implemented in the Tmote Sky, Zolertia Z1, and other motes widely used in the research of the WSN. However, only the fabricant firmware can be uploaded to the XBee devices.

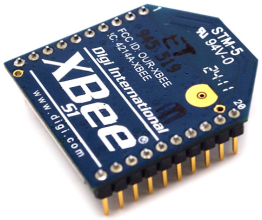


Figure 4.2: XBee S1 device used to conform the WSN

Each XBee device is connected to a chip ATMega2560 [49] using a Shield device that allows an easy connection. The ATMega2560 are used to extend the functionality of the transceivers and to acquire more relevant data in the implemented scenarios. In particular, an experimental testbed is proposed to analyze the networks under jamming attacks by the use of this interconnection between the MC1312x and the ATMega2560.

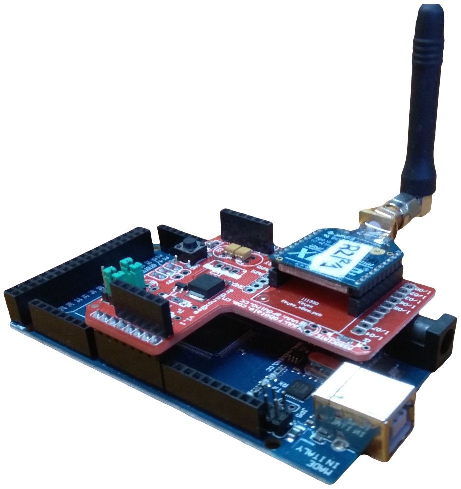


Figure 4.3: Transceiver with the XBee incorporated to the Arduino by the use of a Shield.

Given that the impact of the jammer in the communication processes is not always clear, the network incorporates a sniffer device that can hear all the transmissions. For example, the Software Defined Radio (SDR) N-210 shown in Figure 4.4, is used as a sniffer [2].

Figure 4.4: SDR used as sniffer of the communications

We choose the Wide Band Constant Jamming strategy to cause great damage to the network. Therefore, to implement the jammer device with a wide pulse, we need to use the following circuit. Using a Voltage Controlled Oscillator, we can generate an interference signal with a wideband to interfere with several channels of communications. The problem is that the VCO is generally used to produce the output of a single frequency due to the voltage tune. For this reason, we use a frequency generator with the generation of a triangle wave. With the triangle wave, we can sweep the voltage in the desired tuning voltage. Then, to power up the VCO, we use a simple DC supply. Finally, the implemented circuit is presented in Figure 4.5.

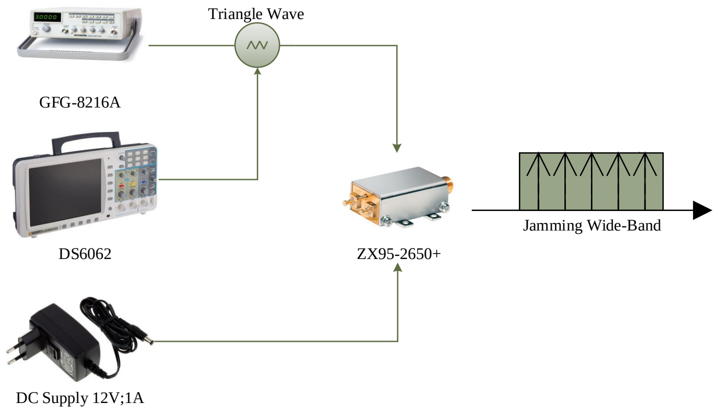


Figure 4.5: Block diagrams of the jammer circuit used to produce the Wide Band Denial Jamming strategy.

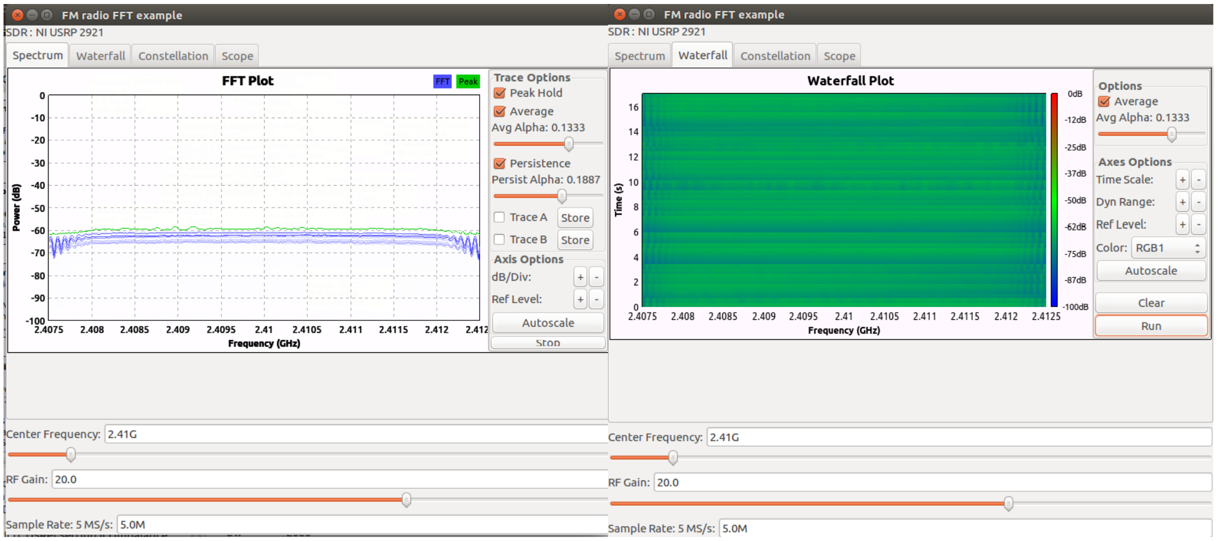
Several experiments have been carried out to found the optimal parameters that produce a Wide-Band Denial Jamming. Using a triangle wave with the parameters show in Table 4.1 the desired output is achieved.

To control the triangle wave and to measure the different times of the processes in the transceivers, we use an Oscilloscope DS6062 EV. Also, to see the correct function of the

Table 4.1: Parameters of the function generator to produce the tune voltage for the VCO

| Device | Function Generator | Frequency | $V_{peak-to-peak}$ | $V_{minimum}$ | $V_{maximum}$ | $V_{offset}$ |
|---|---|---|---|---|---|---|
| GFG-8216A | Triangle Wave | 1 kHz | 4 V | 8 V | 12 V | 10 V |

VCO, we change the configuration of the SDR to a spectrum analyzer and we obtain the FFT and Waterfall plot as shown in Figure 4.6.


SDR: NI USRP 2921

Avg Alpha: 0.1333

Persist Alpha: 0.1887

Center Frequency: 2.41G

RF Gain: 20.0

Sample Rate: 5 MS/s: 5.0M

Figure 4.6: FFT and Waterfall plot showing the incidence of the constant jamming in the communication channel

Finally, the parameters of the circuit for the VCO that produces the Wide-Band Denial in the network are tabulated in Table 4.2

Table 4.2: Parameters of the VCO used to produce the Wide Band Signal.

| Device | Output Power | Output Frequency | Antenna Gain | $I_{max}$ | $V_{cc}$ |
|---|---|---|---|---|---|
| ZX95-2650+ | 4.76 dBm | 2358.3 to 2526.8 MHz | 3 dBi | 27 mA | 12 V |

### 4.1.1 Synchronization

The synchronization between the different devices used in the experimental testbed is critical to ensure the analysis of the different jamming strategies. In this section, we review the methods used in the literature with their pros and cons to show the ideal methodology to our work. We highlight that the energization of the transceivers was made using USB 3.0 ports that we manually connect in the different rounds of experiments to ensure the correct behavior of the devices.

#### Code synchronization

The XBee devices incorporate a python library named Digi-XBee that allows the use of Python to communicate with the devices using the SPI port. The possibility to use Python to control the XBee devices it is a great solution considering the easy use of the language and the notable libraries to control process and multi-threading. However, the transceiver MC1312 of the XBee is directly connected to the ATMega2560 chip with the use of a shield that uses the UART port to perform the communications. As a consequence, the connection between the PC and the MC1312 through the SPI port is not possible that leads to an important disadvantage. An example of this methodology is show in Figure 4.7.

The principal problem when Python is used to control the communication process of the MC1312 transceiver is the complexity to control the interrupts produced in the UART and SPI port when the different handlers are functions are called. In particular, we saw that the aperture of the SPI port produces a reset in the association process of the devices that interferes with the correct log of the data. Additionally, the energization of the devices produces the initialization of the association process in differents instants of times that provokes inconsistences in the syncronization.

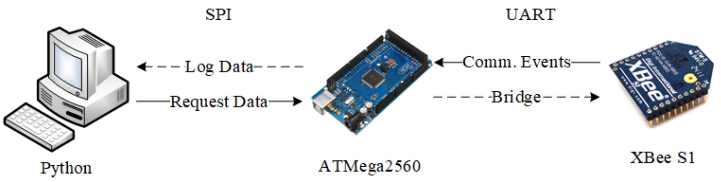


Figure 4.7: Representation of the code synchronization technique.

### MCU syncronization

To overcome the problems of the anterior methodology in the interrupts generated by the code, we upload the neccesary codes to the ATMega2560 MCU that directly communicates with the MC1312 transceiver chipset. Also, we use a USB HUB to energize the devices at the same instant of time to guarantee the same time of initialization of the association process. The execution of the codes in the devices waits for an instruction in the SPI port connected to the PC by the use of delay times. The methodology is represented in Figure 4.8.

Despite the energization at the same time and the execution of the codes by a common signal generated in the principal PC, we saw that the association process differs between the devices. The delay only ensures the association times at the same time but not the same time of execution of the codes in the devices.

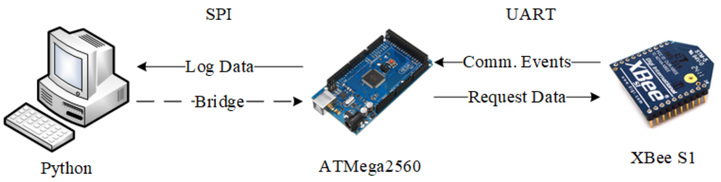


Figure 4.8: Representation of the MCU synchronization technique

### Master clock configuration

In order to ensure a collision for our scenario, a Master-Slave configuration is used (4.9). In this configuration, a Master clock implemented in an ATMega 2560 chip is programmed to generate signals at precise times to the transmitting and interfering devices on the network. Using this configuration, the execution times of the streaming processes have a maximum delay of $80\mu s$. The devices are connected between them using wires to ensure that the jammer device is not capable to interfere with synchronization process as shown in Figure 4.9.

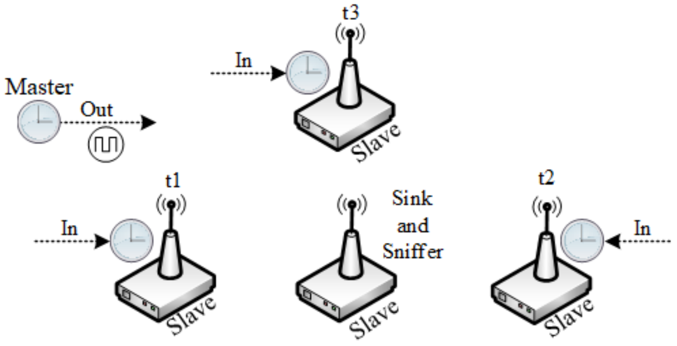


Figure 4.9: The master clock synchronizes all the transmitter's devices in the network.

The experiments show that the Master clock configuration fulfill the requirements to analyze the jamming attacks in the implemented network.

## 4.1.2 Energy Consumption

To obtain the energy consumption associated with the transmission of the packets and the different processes involved in the communications, we adequate the formula used in [15] to the used transceiver. Moreover, the data is corroborated with experimental measures. To obtain the energy consumption measured in Joules $E_{\mathrm{d}}$, we need to know the current consumption for the different modes of each MCU and the operation voltage. Consequently, we can obtain the energy consumption for each device as

$$E_{\mathrm{d}} = (t_{at}\mathrm{i}_{tat} + t_{\mathrm{id}}\mathrm{i}_{\mathrm{id}} + t_s\mathrm{i}_s)\ v_{cc}\ , \tag{4.1}$$

where each $t$ is the time in milliseconds that the MCU is in that state with their corresponding current consumption. Specifically, $t_{at}$ is the time of the duty cycle where the device is active, $t_{\mathrm{id}}$ is the idle portion of the device in this state, and finally $t_s$ are the sleep or low consumption state of the device. Additionally, we use the same time of the length of the experiments $t_{xp}$ to compare the energy consumption in the different scenarios and devices.

### XBee

Using the formulas provided by the manufacturer of the XBee devices, we correlate the different times of the communication process with the times present in the formulas of each device [1]. Additionally, by the use of an oscilloscope, the process is analyzed to link with the presented formulas. According to the analyzed pulses in the oscilloscope, we assume that the transmission and the CCA process use almost the same amount of current. On other hand, the ACK and reception process is similar.

In our experiments, we use 64-bit addressing, $32\mu s$ of byte time and a unicast transmission in a ideal conditions. We also know that the CCA have a fixed value of $0.128ms$ and the ACK $0.864ms$ when is activated. Finally, when the random delay is configured by the use of the backoff exponent, this value is calculated according to the minMacBE and maxMacBE as $t_{Random\ Delay} = 2^{(BE-1)} \cdot 0.032$ ms

### ATMega2560

For the ATMega2560, we have the following process running that makes the transition of the processor in different states.

- The generation of the transmissions and the data packets to be uploaded to the MC1312x MCU.
- The processor continually senses the digital input for the incoming pulse from the master clock to initiate the transmission.
- The reception of the data from the MC1312x MCU and the redirects of the data through the UART port.

Therefore, the ATMega2560 continually changes from the idle to the active states without entering sleep mode. With these processes running in the processor, we can correlate the time active and idle with each of them [3]. As a consequence, the generation of transmission and the reception of the data is the active part $t_{at} = t_{tx} + t_{rx}$. Consequently, the sense of digital input corresponds to idle time $t_{\text{id}} = t_{sense}$. Besides, we consider that the baud rate configured in the code corresponds to 38400 Bd to estimate the time active for the transmission and reception of the data packets printed to the UART and serial port.

### ZX95-2650

The VCO ZX95-2650+ is used to generate the Wide Band Denial jammer as a constant jammer rate [50]. Therefore, the device is always on in the experiments, and the power consumption will be constant through the experiment $t_{at} = t_{xp}$. However, we highlight that the energy consumption is calculated considering only the VCO and not the tuning circuit.

Finally, Table 4.3 presents the different current consumption and the respective operation voltage of each device for the calculation of the power.

Table 4.3: Current consumption for each state and operation voltage for each device used in the experimental testbed [1–3]. The consumption of the devices used for the synchronization and the tuning circuit are not considered for the comparison analysis.

| **Device** | **Current Consumption** | | | **Voltage** |
|---|---|---|---|---|
| | **Transmission** | **Idle** | **Sleep** | |
| XBee | 45 mA | 50 mA | 10 uA | 3.3 V |
| ATMega2560 | 4 mA | 13 mA | 15 uA | 5 V |
| ZX95-2560+ | 27 mA | - | - | 12 V |

## 4.2 Software

The open-source GNURadio software is used to program and to acquire the data of the sniffer implemented in the SDR N-210 [2]. The implemented code is a variation of [47] to acquire the transmitted packets in our implemented scenarios. The code is divided into two flow graphs: the physical layer and MAC layer implementation. In the PHY flow graph, the modulation, demodulation, synchronization, pulse shaping, and process of the data are performed as specified by the standard. Finally, the PHY flow graph is encapsulated in a hierarchical block to improve the clearness of the complete code as shown in Figure 4.10.

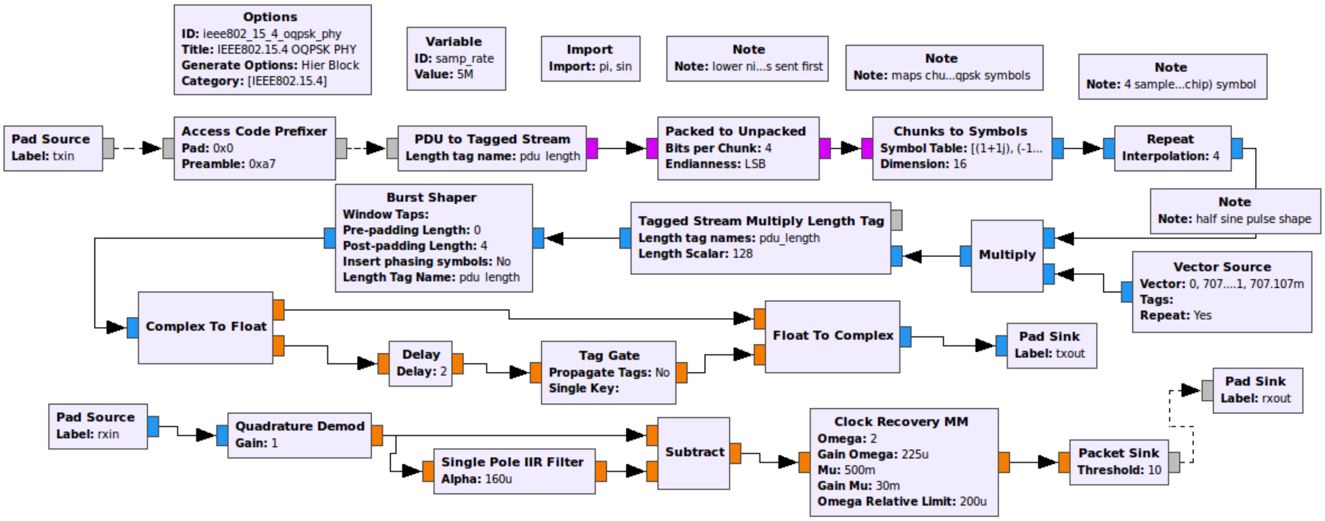
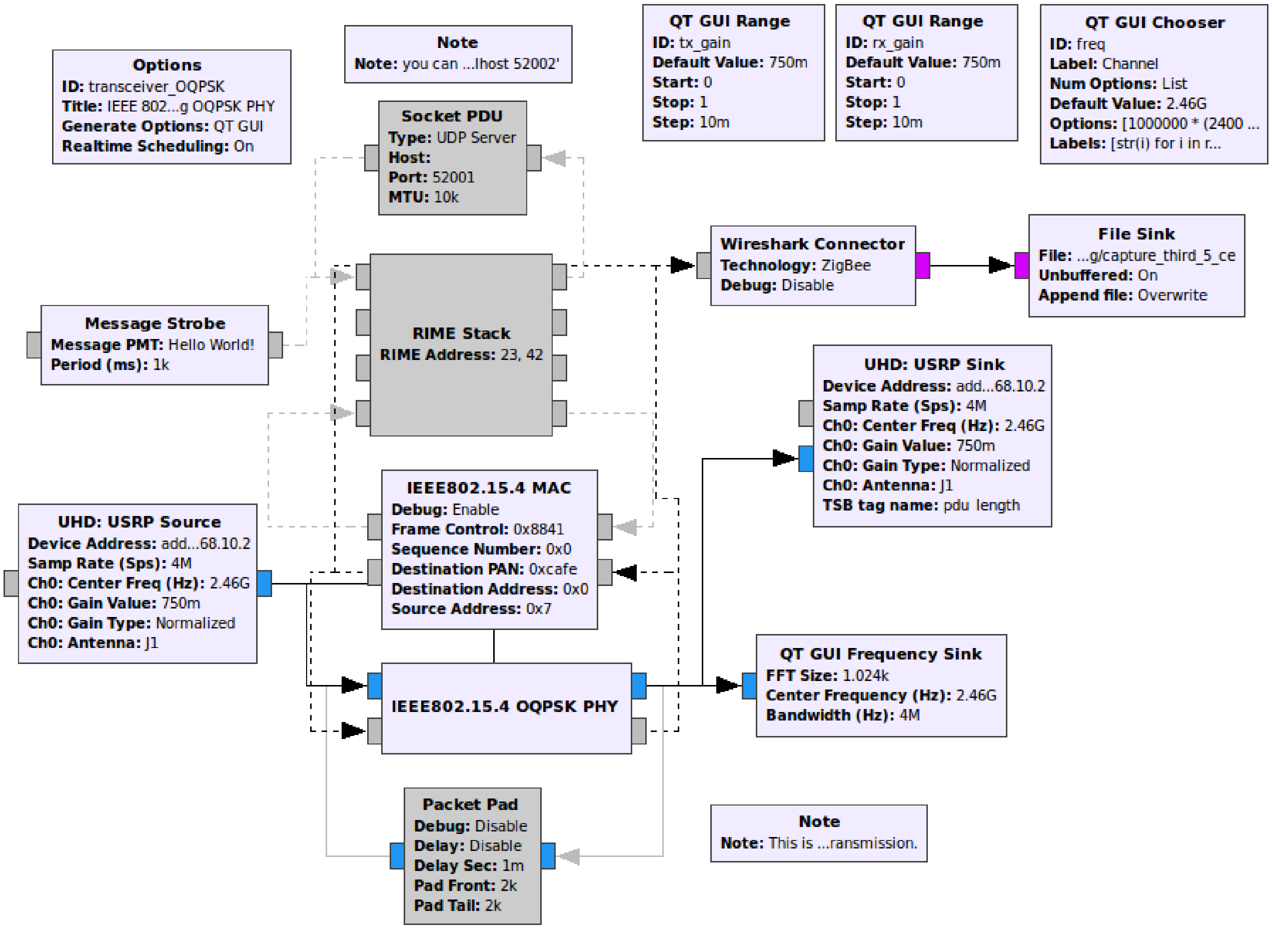


Figure 4.10: Flow graphs of PHY layer implemented in GNURadio

In the MAC flow graph, the different blocks that allow the obtention and transmission of the data are present. The RIME stack is implemented as a block to communicate with the IEEE 802.15.4 motes in the network. Additionally, a block with the MAC parameters itself is implemented to interact with the RIME block and the encapsulated PHY flow graph. The data acquired by the SDR is stored in a way that can be analyzed using the Wireshark software.

For our proposed testbed, the transceiver code needs to be modified to not intervene in the communication process in the network and behave like a sniffer. As a consequence, some blocks of the MAC layer was suppressed, and only we preserve the blocks that permit the capture of the data. Also, the blocks of the USRP were modified to ensure the match of the frequency, bandwidth, and gain with the implemented network as presented in Figure 4.11.



**Options**
**ID:** transceiver_OQPSK
**Title:** IEEE 802...g OQPSK PHY
**Generate Options:** QT GUI
**Realtime Scheduling:** On

**Note**
**Note:** you can ...lhost 52002'

**QT GUI Range**
**ID:** tx_gain
**Default Value:** 750m
**Start:** 0
**Stop:** 1
**Step:** 10m

**QT GUI Range**
**ID:** rx_gain
**Default Value:** 750m
**Start:** 0
**Stop:** 1
**Step:** 10m

**QT GUI Chooser**
**ID:** freq
**Label:** Channel
**Num Options:** List
**Default Value:** 2.46G
**Options:** [1000000 * (2400 ...
**Labels:** [str(i) for i in r...

**Socket PDU**
**Type:** UDP Server
**Host:**
**Port:** 52001
**MTU:** 10k

**Wireshark Connector**
**Technology:** ZigBee
**Debug:** Disable

**File Sink**
**File:** ...g/capture_third_5_ce
**Unbuffered:** On
**Append file:** Overwrite

**Message Strobe**
**Message PMT:** Hello World!
**Period (ms):** 1k

**RIME Stack**
**RIME Address:** 23, 42

**UHD: USRP Sink**
**Device Address:** add...68.10.2
**Samp Rate (Sps):** 4M
**Ch0: Center Freq (Hz):** 2.46G
**Ch0: Gain Value:** 750m
**Ch0: Gain Type:** Normalized
**Ch0: Antenna:** J1
**TSB tag name:** pdu length

**IEEE802.15.4 MAC**
**Debug:** Enable
**Frame Control:** 0x8841
**Sequence Number:** 0x0
**Destination PAN:** 0xcafe
**Destination Address:** 0x0
**Source Address:** 0x7

**UHD: USRP Source**
**Device Address:** add...68.10.2
**Samp Rate (Sps):** 4M
**Ch0: Center Freq (Hz):** 2.46G
**Ch0: Gain Value:** 750m
**Ch0: Gain Type:** Normalized
**Ch0: Antenna:** J1

**IEEE802.15.4 OQPSK PHY**

**QT GUI Frequency Sink**
**FFT Size:** 1.024k
**Center Frequency (Hz):** 2.46G
**Bandwidth (Hz):** 4M

**Packet Pad**
**Debug:** Disable
**Delay:** Disable
**Delay Sec:** 1m
**Pad Front:** 2k
**Pad Tail:** 2k

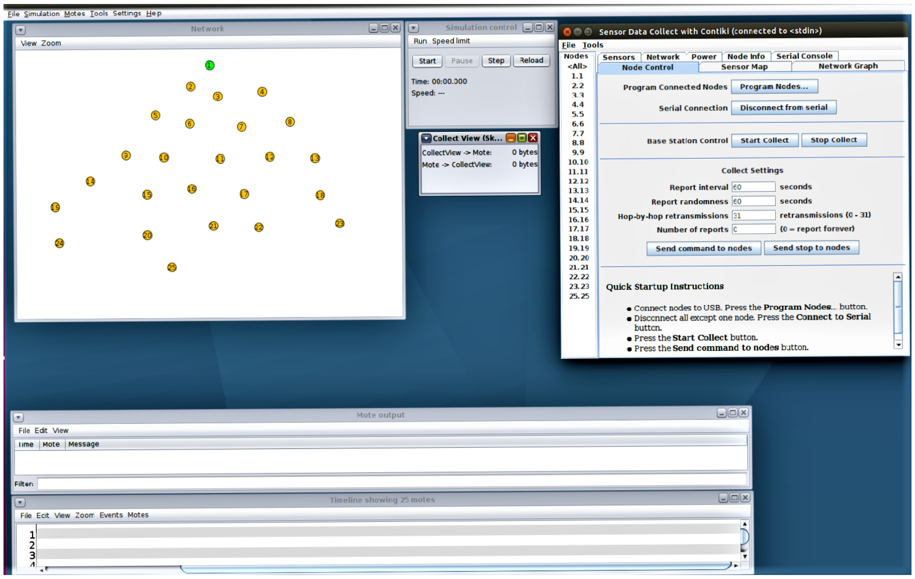
**Note**
**Note:** This is ...ransmission.

Figure 4.11: Flow graphs of MAC layer implemented in GNURadio

The data captured by the sniffer needs to be analyzed to correlate with the parameters used in this work. The Wireshark software is used in the sniffer side to analyze the data acquired in the different experiments, using the provided filters for the IEEE 802.15.4 standard. Later, the data is tabulated in an excel sheet with the data obtained in the transmitters and sink side.

In the sink and the transmitter side, composed by the XBee devices, we use python libraries to manipulate and log the data. For the transmitter side, we use the uploaded code to the ATMega2560 in conjunction with the software ExtraPutty to log the data. The code in the ATMega2560 has the instructions to send data through the UART port of the communication process. Then, for each transmitter, an instance of ExtraPutty is initialized to log the data with their corresponding timestamp of the event. For the sink side, we use the terminal provided by the manufacturer Digi that permits an easy way to configure the devices Over The Air (OTA) and log the data.

Simulations were carried out to compare the analytical and experimental results of the different scenarios. The Cooja simulator incorporated in the Contiki OS was used to realize the simulations of the experimental scenarios under jamming attacks. The simulator emulates the physical devices (motes) with their particular characteristic as show in Figure 4.12. Also, the simulated code could be uploaded to the mote if the device admits the upload of open-source firmware. Moreover, several MAC protocols and networking stacks can be configured.



Time: 00:00.000
Speed: ---

CollectView -> Mote: 0 bytes
Mote -> CollectView: 0 bytes

Report interval 60 seconds
Report randomness 60 seconds
Hop-by-hop retransmissions 31 retransmissions (0 - 31)
Number of reports 0 (0 = report forever)

Quick Startup Instructions

- Connect nodes to USB. Press the **Program Nodes...** button.
- Disconnect all except one node. Press the **Connect to Serial** button.
- Press the **Start Collect** button.
- Press the **Send command to nodes** button.

Figure 4.12: Graphical interface of a simulation in the Cooja simulator

The Cooja simulator also integrates four types of model channel. We use the Unit Disk Graph(UDGM) Radio Medium for the simulations implemented. The range of transmission of the transmitter is abstract as a circle with two ranging parameters: one for transmissions and one for interfering with other radios and transmissions.

Finally, the analytical results, the experimental results, and the model were implemented in Matlab to obtain the different probabilities and values of the performance metrics.

# Chapter 5

# Results and Discussion

With the novel experimental testbed implemented, we proceed to acquire the performance metrics in different scenarios. Next, we perform the correlation of the experimental data with the obtained theoretical results from the previous chapter. Consequently, several conclusions arise from the analysis of the results in the jamming scenarios from the analyzed performance metrics.

## 5.1 TSCH & Orchestra

We conducted extensive experiments using the Cooja simulator to evaluate the performance of the simulated network in the presence of a jamming node. We evaluated the TSCH and Orchestra algorithms on two simulated scenarios generated in the Cooja simulator. Once we have simulated the network, we test the network to verify a correct operation. Then, we acquire the performance metrics. Next, we add a jammer device into the network to generate the second scenario. Finally, we establish a comparison between the simulated scenarios.

Due to the limitations in terms of memory available on the emulated nodes, the algorithms of the application layer are not implemented to guarantee the correct behavior of the MAC and routing layer. The routing protocol used in the experiments is Contiki RPL, which is supported for the Zolertia Z1 motes (MSP430, 8KB RAM, 92KB Flash, and CC2420 transceiver) [51].

Figure 5.1 shows the ideal scenario with five constrained nodes (1 root, 4 senders), transmitting packets related to the MAC and RPL non-storing mode. The nodes are uniformly distributed in a 10 times 10 m$^2$ square network area. The distance between each node is equal to 10m with a communication range of 50m, without variations in the experiments. Also, the distribution order of the nodes in the deployment is the same, shown in the Figure 5.1. During the experiments, we do not consider mobility of the nodes. The radio model simulated is a Zolertia Z1 with a data rate of 250kbps in the 2.4 GHz band.

In the experiments, the ideal scenario is used to establish a comparison. We employ this scenario to acquire performance metrics without an attacker. After that, the scheduling algorithms are implemented in the nodes to achieve Orchestra mode and later acquire the same performance metrics.

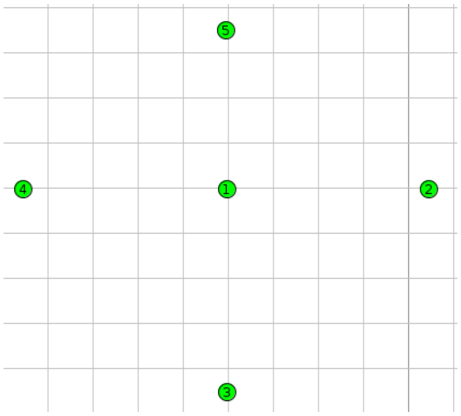


Figure 5.1: The first scenario for the simulations consists in the ideal scenario with the presence of four transmitters and one sink node in the absence of jamming attacks.

Subsequently we put a disrupt node in the simulated network, that will be the jammer device performing a DoS attack. The jammer generates a interference signal when a transmission of any legitime nodes is performed. We select two fixed places to put the jammer. These places allow the jammer to impact various nodes at the same time. The interference signal power and the transmission range is the same as the sender nodes. Also, we obtain the performance metrics for each node. Later, we compare and analyze the results obtained of the both scenarios.

Using the defined metrics, we evaluated the performance of TSCH and Orchestra mode. In the scenario with the presence of an attacker, the disrupted node (jammer) is deployed in two different places as showed in Figure 5.2 with the following considerations: interferes one transmitter node, interferes two transmitters and neighbors node, interferes two transmitters, neighbors and coordinator nodes. These variations are performed to analyze the behavior of the network and also, acquire the metrics of PDR and energy consumption. Also, we perform a third scenario where the jammer interrupts two transmitter nodes and the coordinator of the network. When the coordinator is affected, the scheduling algorithm is lost in the transmitter nodes but not in the coordinator. Consequently, the results of the PDR and duty cycle are not relevant as the other two scenarios. For this reason, the results obtained are not considered in the analysis.

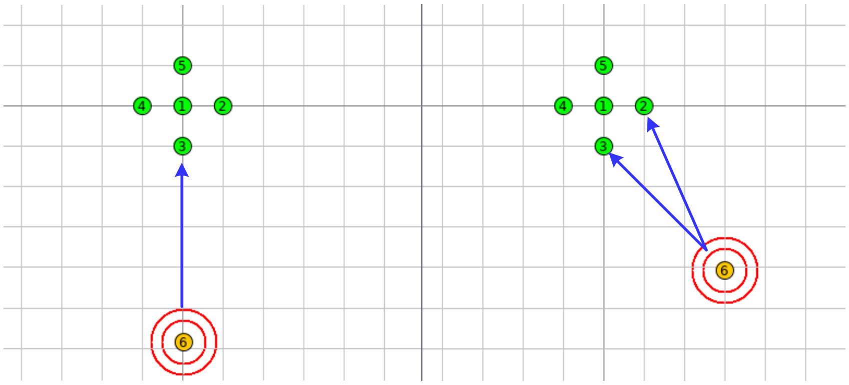


Figure 5.2: The figure in the left show the jammer disrupting the communication on a one transmitter node. Meanwhile, the figure in the right show the jammer disrupting the communication on two transmitters node.

We analyze the results in three parts. First, we simulate the network and we obtain the performance metrics of both TSCH and Orchestra mode in an ideal scenario. Then, we generate the second scenario. We perform the same steps as the first scenario with the presence of the jammer on the network. Finally, we compare the results of the performance metrics in both scenarios with TSCH and Orchestra mode. In the experiments the concurrent transmission of two or more packets always results in a collision and, hence, a transmission failure. Also, in the simulator, the radio medium is simulated and configured as Unit Disk Graph Medium (UDGM) in concordance with the related work. The other related parameters are configured with the default value described in the standard. To obtain the PDR, we use radio message tool. This tool performs a log of the packets generated, transmitted or received for each node of the network with timestamps. Also, the tool incorporates a 6LoWPan analyzer with PCAP option to analyze the packets.

Table 5.1: PDR summary for the experiments. Both protocols are affected by the jammer device.

| Mode | Ideal (%) | Jamming(A) (%) | Jamming (B) (%) |
|---|---|---|---|
| TSCH | 99.3 | 81.04 | 62.78 |
| Orchestra | 99.9 | 80.82 | 63.14 |

In the ideal scenario, TSCH and Orchestra mode have an optimal performance in terms of the evaluated metrics as presented in . Under the jamming attack, the legitimate packets have more chances to collide with the jamming packets. Consequently as shown in Table 5.1, and Figure 5.3 the PDR decreases to 80.82% and 81.04% in the Orchestra and TSCH mode, respectively. Furthermore, as we expected when two transmitter nodes are affected the PDR decreases in 17% for both modes. As a consequence, the scheduling algorithm used in Orchestra mode cannot overperform the random allocation channel of TSCH mode. As a result, PDR is almost the same for both scenarios.

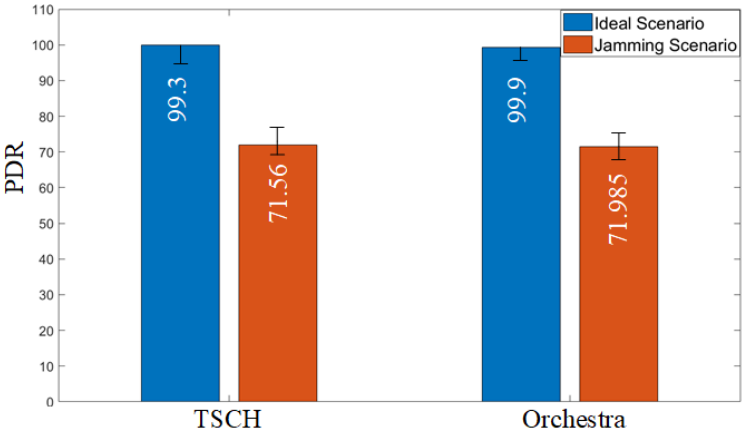


Figure 5.3: Average PDR obtained from both tested scenarios. The bar corresponding to the jamming scenario (orange) is the average value of the two scenarios.

Finally, the energy consumption is analyzed. We acquired the results of the duty cycle and the energy consumption for each node and the network. In the ideal scenario, both modes achieve a low duty cycle and energy consumption. Most of the time, the nodes stay in an 'ON' state when the network is formed, as represented in Figure 5.4.

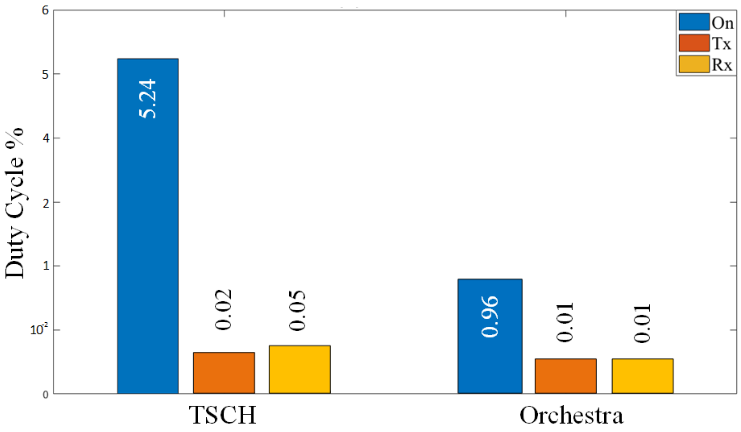


Figure 5.4: Duty cycle of the transmitter node in the ideal scenario for both modes. The transmission and reception states are negligible.

In the jamming scenario, and as expected, a higher energy consumption exists. A higher chance of collision of the packets triggers the retransmission and sense of the channel algorithms frequently. Consequently, the execution of the algorithms demands more energy to the nodes that increase the duty cycle to 96% on average, as shown in Figure 5.5.

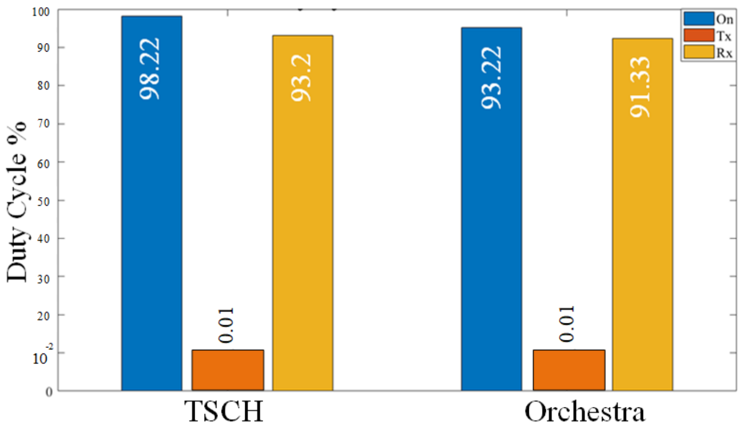


Figure 5.5: Duty cycle of the transmitter node in the jamming scenario. The reception state leads to a considerable increase in energy consumption as show for the reception state that have an average value of 92.265% from TSCH and Orchestra.

Also, we can observe an unusual behavior of the nodes affected by the jamming attack. When a transmitter node is in the presence of the attacker, the synchronization and schedules are affected. As a consequence, the nodes decided to leave the network and enters a steady receiver state. In this state, the node performs a sense of the transmission channels perpetually. Therefore, the duty cycle of the node increases to almost 99% for both MAC modes as represented in Figure 5.6.

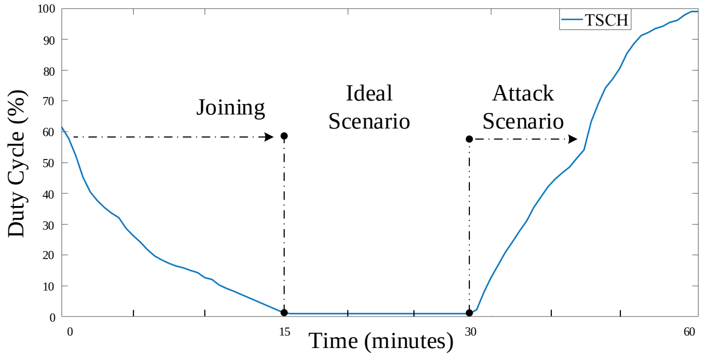


Figure 5.6: Energy consumption as a timeline for TSCH mode in the different scenarios

Furthermore, we obtained a higher energy consumption in the joining process of the nodes for both MAC modes. During the joining time process, the Orchestra mode achieved a lower energy consumption than the TSCH mode by 5% The duty cycle values for the simulated scenarios are summarized in Fig. 5.6 as a timeline for the TSCH mode. Moreover, the timeline for Orchestra mode presents the same behavior to the obtained with TSCH. As a result, the duty cycle is almost five times higher in the network with the presence of an attacker for TSCH mode and twenty times for Orchestra mode, as shown in Table 5.2.

Table 5.2: Average Duty cycle summary for the network in the experiments. Both protocols are affected by the jammer device.

| Mode | Ideal (%) | Jamming(A) (%) | Jamming (B) (%) |
|---|---|---|---|
| TSCH | 5.24 | 24.08 | 42.792 |
| Orchestra | 0.96 | 20.768 | 40.176 |

With the duty cycle obtained, we calculate energy consumption. For both modes in the jamming scenario, the consumption is considerably higher as represented in Table 5.3. The node with orchestra mode is the most affected by the incidence of the jamming attack. To minimize energy consumption when an attack is present, the use of an algorithm that brakes the perpetual receiver state is recommended. Also, the number of documented times that a node synchronize with the coordinator could give insights about a jamming attack.

Table 5.3: Average energy consumption summary for the node in the experiments.

| Mode | Ideal (mJ) | Jamming (mJ) |
|---|---|---|
| TSCH | $6.534 \cdot 10^{-4}$ | $1.6491 \cdot 10^{-1}$ |
| Orchestra | $4.176 \cdot 10^{-4}$ | $1.61463 \cdot 10^{-1}$ |

Finally, we remark that the relative position of the jammer from the transmitter devices is critical. In particular, the impact of the jamming signal is higher from transmitters close to the jammer device. Therefore, the impact of the jammer can be analyzed in terms of distance or signal strengths like the SINR ratio despite the relative position of the jammer device from the transmitters. The results acquired from the simulation for two fixed positions of the jammer can be extended to another position distribution of the devices.

## 5.2 Unslotted CSMA/CA

For the CSMA/CA unslotted mode, we do not perform simulations in the Cooja simulator for inconsistencies with the standard. As stated in the works [52, 53], the CSMA/CA code implemented in the Contiki OS has parameters that are not in line with the specifications of the standard. Specifically, the behavior of the random delays using the Backoff Exponent (BE) is not possible and always is fixed to 125 ms. Moreover, the unicast packets are treated as broadcast packets when the MAC queue is full. As a consequence, no sensing is performed in the transmission of the packets.For these reasons and explained in both works, the comparison with simulated results is not shown.

### 5.2.1 Channel Parameters

The first environment used for the experiment was a office enviroment with the coexistence of different communication protocols. Due to the unique characteristics of each environment, most radio propagation models use a combination of analytical and empirical methods. One of the most common radio propagation models for the indoor enviroment is the log-normal shadowing path loss model. This model can be used for large and small coverage systems; furthermore, empirical studies have shown the the log-normal shadowing model provides more accurate multi-path channel models than Nakagami and Rayleigh for indoor environments. The model is given as follows:

$$PL(\mathrm{d}) = PL(\mathrm{d}_0) + 10nlog_{10}\left(\frac{\mathrm{d}}{\mathrm{d}_0} + X_\sigma\right). \tag{5.1}$$

However, due to the contingency of the COVID-19, the experimental testbed was changed to a new place. The new place used for the experiments consists of a bedroom adapted to implement the devices. Therefore, several considerations needed to take into account. To fulfill the requirements that this kind of experiment needs, several rounds of experiments were performed in the first instance to characterize the environment.

In our new scenario, we obtain that path loss exponent is equal to 1.8 and $PL_0 = 39.616$ dB. This results are consistent with the values presented in the works [54–56] for the indoor office environment with LOS component. For our work, the shadowing component is called $X_\sigma$ .

In Figure 5.7 we plot the theoretical and experimental path loss characterization curves for the obtained values of our scenario, as well as prediction bounds of 95%. Using the spectrum analyzer and the transmission of data with one transmitter, we analyzed the RSS values and behavior of the communications on several days and time hours. The results show that the optimal range of hours to perform the experiments is between 08 AM and 04 PM in the week. In the weekend or outside of this range of hours, the environment has a lot

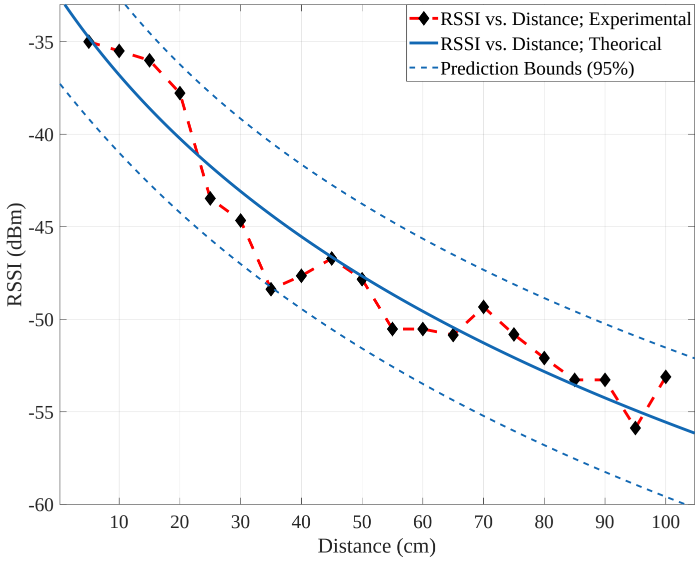


Figure 5.7: Experimental and theoretical path loss characterization with n=1.8, $\sigma = 1.8827$, and $X_\sigma = 53.28$.

of interference signals, and erratic behavior of the RSS values reported. We also found that channel 12 ($f_c = 2410MHz$) is the best for communication through the experiments.

With the results obtained for the channel environment and the protection ratio founded by the experimental results that shows a good agreement with the regression model, we plot the Capture Effect when is accounted in the probability of success. The parameters founded are $\alpha = 3.1$ dB and $\beta = 1.8$ according to the experimental results, and the curve is plotted in Figure (5.8).

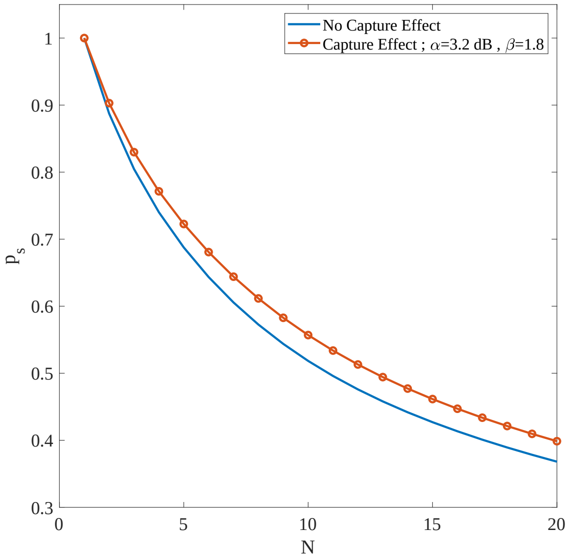


Figure 5.8: Probability of success for length of packet equal to $D = 2$ when the capture effect is accounted using the acquired parameters of path loss $\alpha = 3.2$dB and $\beta = 1.8$

### 5.2.2 General Proccedure

Each device on the network records the data. The registers showed the different processes of the transmission as the reception, transmissions, and ACK in the network. The sink node continuously records the packets that receive from each transmitter with the corresponding RSSI value. The transmitters log the status of each transmission reported by the ACK. Finally, the sniffer records all the data packets that could capture in the experiments. The correlation of the log files is performed by the timestamp of the packets.A dedicated code in Python and Wireshark performs the analysis of the metrics and the transformation from the RSSI to RSS.

Before starting each round of experiments, the transmission of 2000 packets was carried out between one of the transmitting nodes and the sink node to obtain the noise floor. For cases in which the ambient noise is significant, the RSS values present a high variance and therefore are not used for the analysis of the metrics. Besides, the environment was evaluated for different times and locations of the nodes, without presenting great variations. The average noise floor for the different rounds of the experiment is $-82$dBm.

### 5.2.3 PDR and Goodput

Later, we carry out the experiments to analyze the performance of the network composed of the XBee devices under the different jamming strategies. The main difference between the experiments resides in the variation of the BE parameter for the transmitter node to transform into an interferer node. With this modification and the assumptions for our work, this node behaves like a reactive jamming strategy. When the reactive strategy is used, the scenario implemented has a circular distribution of the transmitters nodes to the sink node. Specifically, with the sink node, we deploy the sniffer device in the center of the circle. We also use the same distribution for the constant strategy. However, the distance of the constant jammer device is fixed to one position due to the power output and the impossibility to vary between experiments. The scenarios for the experiment is presented in Figure 5.9. When the transmitter is used as an interferer, the circular distribution is maintained.

A network composed of N transmitting nodes is used using the IEEE 802.15.4 protocol with ACK's. The transmitting nodes are located in random positions and distributed circularly in a radius $R = 70$cm to the sink node as show in Figure 5.9. Also, all the nodes can listen to each other and use a packet length of 25 bytes in the 2.4 GHz band and use the same channel throughout the experiments, so the Channel Hopping mechanism has been deactivated.

The synchronization is critical to evaluate the performance of the network under jamming attacks. In the experiments, the attacker has complete knowledge of the time of the transmission of the packets. Therefore, the overlapping between the legitimate and attacker packets initiates in the headers. The transmission occurs every 100ms, and the turnaround time is 1.728ms. The calculated times are verified using an oscilloscope in the different PIN of communications of the transceiver.

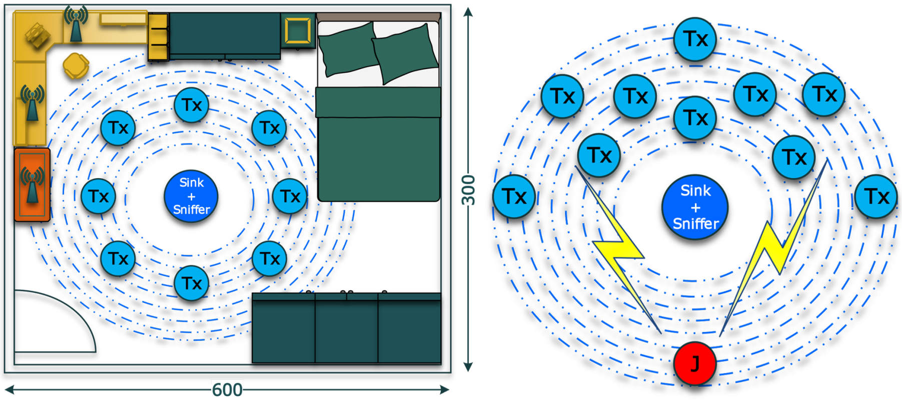


Figure 5.9: The figure on the left shows the bedroom environment used for the experiments of reactive strategy and the channel characterization. Meanwhile, the right figure shows the distribution for the constant strategy where the jammer is fixed to the presented position at 60 cm of the sink. Both scenarios use a circular distribution for the transmitters.

To determine the performance metrics for the scenarios under jamming attacks, we activate the ACK mechanism. Therefore, we have the information of the transmitters, the received packets in the sink, and the registered packets by the sniffer to analyze the behavior. For the first round of experiments, we vary the number of interferers present in the scenario to analyze the performance against one transmitter. Consequently, we start the experiments with one transmitter and one interferer. We remark that the sniffer and the sink node are always implemented in all the experiments.

Using a reactive strategy with one interferer in the scenario, we analyze the PRR from different SINR values. Therefore, we configure a $BE = 0$ for the transmitter and the interferer nodes to generate collisions. The results showed that for values of SINR greater than 4.5dB, the PRR is almost 0.99. We also corroborate this information with the ACK status reported by the transmitters, which show almost null errors in the transmission.

On the contrary, for values of SINR in the range of $[1.07, 4.5]$dB, the PRR does not converge. Therefore, for the interval of SINR values between 0 to 4.5dB, the signal overlaps that induces destructive interferences in the communication as reported in Figure 5.13. The PRR-to-SINR acquired in the multiple experiments with the effect of one interferer is plotted in Figure 5.10. The curve is obtained considering the device with the larger value of average RSS obtained in the experiment as the legitimate sender. Despite the presence of interferers, the capture occurs for multiple values of SINR.

Then we analyze the goodput metric for the same range SINR values with $BE = 0$. For values of SINR greater than 4.5dB, the goodput has its maximum value similar to an ideal scenario in the range of 2902.49 to 3048.38bps. Similar to the behavior of the PRR, for values lesser than 4.5dB, the goodput decreases to values in the range of the 1006.28 to 556.038bps. The goodput for values of $BE = 0$, $BE = 3$ , and $SO = 0$ are plotted in Figure 5.10.

Using the same configuration as above with an interfering node and transmitter transmitting to the sink node, we vary the value to $BE = 3$ in the transmitter node. A round of experiments was carried out for different SINR values, and the effects of using the backoff mechanism for the first iteration of the algorithm were analyzed. The results of the PRR-to-SINR show a constant behavior for the range of SINR values between 1.8 to 12dB. The PRR value is stable and approaches a value of 0.99 for the different SINR values obtained. Figure 5.10 presents the PRR-to-SINR values obtained for the stated configuration.

Similar to the behavior of PRR-to-SINR for $BE = 3$ and , goodput values for an ideal scenario are obtained. The goodput value converges to a value of 2900bps for the different SINR values between 2.3 to 9dB. Only for an SINR value equal to 1.8dB there is a slight decrease in goodput of 2650bps, as shown in Figure 5.10.

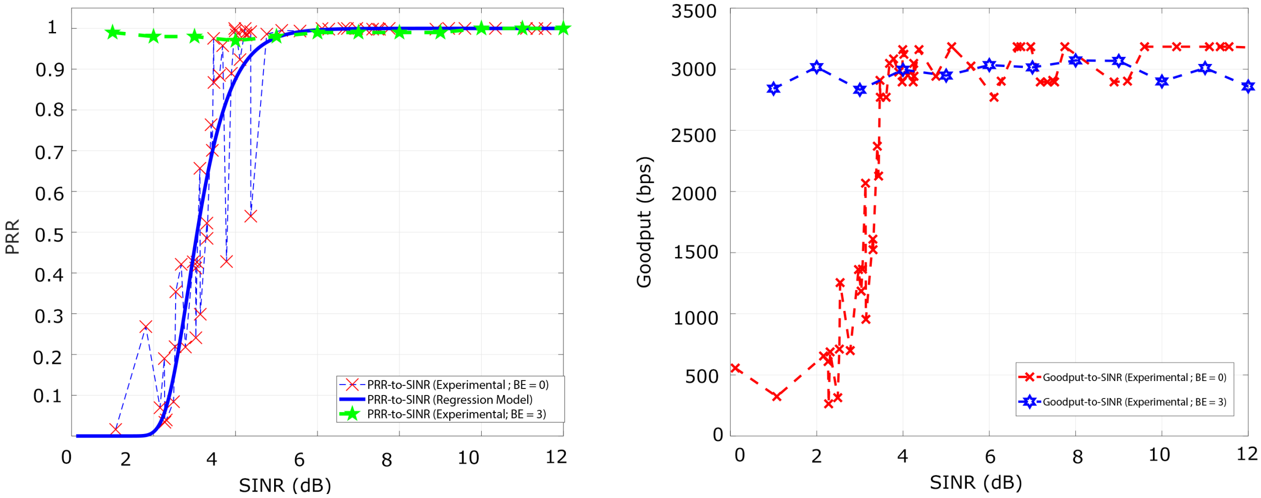


Figure 5.10: On the left, the PRR-to-SINR curve for $BE = 0$ and $BE = 3$ for one transmitter $N_c = 1$ and one interferer $N_\mathrm{i} = 1$. For values of SINR higher than 4.5dB both curves converge. The curve of the regression model is plotted to show a good agreement with the experimental results obtained. On the right side, the Goodput-to-SINR curve for $BE = 0$ and $BE = 3$.

Then, we increment the number of interferer nodes $N_\mathrm{i} = 2$ to analyze the performance of the transmitter $N_c = 1$. Following the circular distribution, we deploy the nodes at different distances from the sink node. From here, we only analyze the performance metrics for a total collision scenario, and all the nodes are configured with $BE = 0$. The results show that the interferers generate a constructive interference that completely blocks the reception of packets, as shown in Table 5.4. Therefore, we focus on finding a threshold value that permits the reception of packets with two interferers.

Table 5.4: PRR values for $N_\mathrm{i} = 2$ and $N_c = 1$, using $BE = 0$ . The PRR is almost zero independent of the SINR values. Two experiments are shown to graph the behaviour.

| **Transmitter** | **RSS(dBm)** | **SINR(dB)** | **ACK** | | **Packets Capture** | **PRR** |
|---|---|---|---|---|---|---|
| | | | **Success** | **Error** | **(Sniffer + Sink)** | |
| t1 | -58.66 | 8.372 | 0 | 2955 | 23 | 0.00067 |
| i1 | -66.5 | | 0 | 2925 | 3 | 0.00103 |
| i2 | -67.5 | | 0 | 2910 | 1 | 0.00034 |
| t1 | -56 | 3.0978 | 0 | 2856 | 2 | 0.00175 |
| i1 | -56.5 | | 0 | 2920 | 2 | 0.00069 |
| i2 | -59.33 | | 0 | 2910 | 3 | 0.00103 |

For the different experiments, the sniffer can capture packets that the sink node has not been able to decode. The packets that have been received and reported as a success by the ACK are tabulated in 5.5. Furthermore, transmission errors reported by the ACK are included. The sniffer captures approximately 45% more packets than the total packets received and reported by the ACK in scenarios with collisions. However, some packets have not been possible to capture by the sink and can not be registered in the log. This behavior is because the ACK will report an error after the specified number of transmissions (three by default) have not been able to receive [1].

The packets captured by the sniffer are always greater than the ones captured by the sink node in the scenarios with collisions. However, if collisions do not occur, the sink and the sniffer have an equal number of packets of data captured. In some cases, CE is also present in the sniffer side. Particularly, the sniffer can capture a major number of data and ACK packets for only one of the transmitters that have a greater RSSI value. The tabulated experiments in Table 5.5 show this behavior.

Table 5.5: Data packets captured by the sniffer and the sink node for differents values of SINR when collisions occur in the transmissions.

| **Transmitter** | **RSS(dBm)** | **SINR (dB)** | **ACK** | | **Sniffer Capture** |
|---|---|---|---|---|---|
| | | | **Success** | **Error** | |
| t1 | -42.87647 | 0.112856 | 4231 | 21785 | 92901 |
| i1 | -42.98956 | | 4334 | 21681 | 2249 |
| t1 | -43.979 | 2.2638 | 3605 | 17467 | 3546 |
| i1 | -46.24354 | | 4400 | 16672 | 29372 |
| t1 | -39.32021 | 4.2475776 | 3988 | 62 | 4286 |
| i1 | -43.56022 | | 4020 | 30 | 4203 |

Next, to encounter the threshold that permits the reception of packets in the sink node for the transmitter node, we use the following methodology. First, we fixed the distance of the transmitter to the sink node. Then, we vary the relative distance of the interferers from the sink and also between them. According to the results acquired, when the second interferer have an threshold of almost 3.1 dbm from the first interferer, the reception of the packets occurs, Table 5.6 shows some experiments performed that reveals this behavior. Additionally, we remark that the threshold between the interferers and the transmitter follows the assumptions analyzed in the scenario with a $N_{\mathrm{i}} = 1$.

Table 5.6: Several experiments were performed to acquire the threshold in RSS from the sink node between the devices. The reported values of PRR corresponds to the average value of the total devices. The experiments show that for a certain RSS threshold between the interferers, the reception occurs. We also found that a similar threshold between the transmitter and the interferer with the higher RSS value is needed.

| **Transmitter** | **RSS(dBm)** | **SINR(dB)** | **PRR** |
|---|---|---|---|
| t1 | -46.1374 | 2.4763 | 0.2525 |
| i1 | -50.09876 | | |
| i2 | -54.1 | | |
| t1 | -45.9178 | 2.6255 | 0.26 |
| i1 | -50.1 | | |
| i2 | -54.12 | | |
| t1 | -47.7676 | 6.160 | 0.2869 |
| i1 | -51.2 | | |
| i2 | -54.3 | | |
| t1 | -47.8103 | 7.819 | 0.3282 |
| i1 | -50.98 | | |
| i2 | -54.1 | | |

After that, we change the interferer node of the reactive strategy to the constant strategy. For this, we deploy the VCO in a fixed position of 60cm from the sink node. Using the SDR as a spectrum analyzer and correlating the gain of SDR with the XBee devices, we fixed the signal strength in $-58$ dBm for the jammer. Then, we modify the distance of the XBee transmitter to achieve different SINR values, as shown in Figure 5.9.The results show that despite the strategy used, the PDR and goodput metrics vary equally. Therefore, the SINR value is critical to ensure the PDR and goodput for the application scenario used in our work.

Finally, we correlate the experimental results of the PDR with the analytical model for the $p_s$ performance metric. Using a fixed value of $N_{\mathrm{i}} = 1$ and $N_c = 1, 2, 3, 4$, we plot the experimental and theoretical curve of $p_s$. For this, we use the protection ratio $\alpha = 3.1$ as used in the work [25] to compare the curves. The experimental curve shows a good agreement with the proposed model under the assumptions used in our work, as shown in Figure 5.11.

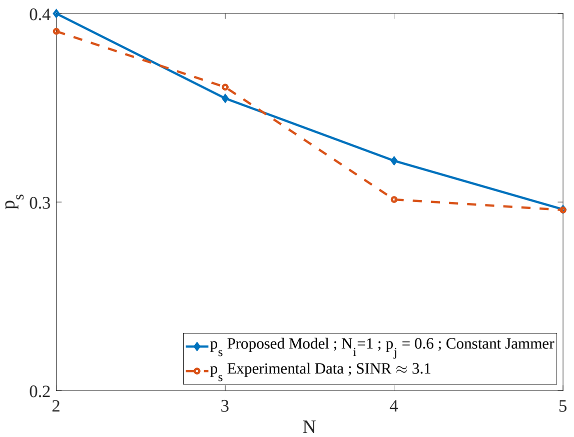


Figure 5.11: Probability of success $p_s$, including the probability of jamming $p_j$, is plotted with repect to $N$. A good agreement exists between the experimental and proposed theoretical model.

The results show that the impact of both attackers' strategies is the same for the range of SINR analyzed for the PRR and goodput metrics. As a consequence, applications that manipulate sensitive data as in the healthcare, industrial or urban enviroments are a notorious risk to be completely denied owing to the data rate requirements for the devices. Therefore, to guarantee the integrity of the communication system, the power output, the time of transmissions, and the distance of the devices are critical parameters.

### 5.2.4 Received Signal Strength and Transmission Status

The graphics presented uses the timestamp of the packets recorded and the RSS value to show the behavior of the link communications, as depicted in Figure 5.12 . Additionally, the reports of the transmission by the ACK are plotted to correlate both graphics, as seen in Figure 5.13 , and Table 5.4. The sniffer is not considered in the graphics of the RSS values given the difference of the hardware and the process to estimate the received signal.

The first experiments are for the ideal scenario and are performed with the ACKs enable in the communications. For ideal scenarios, the transmission status reported by the ACK is always asses as a success. Consequently, the RSS values does not present a significant variance 5.12.

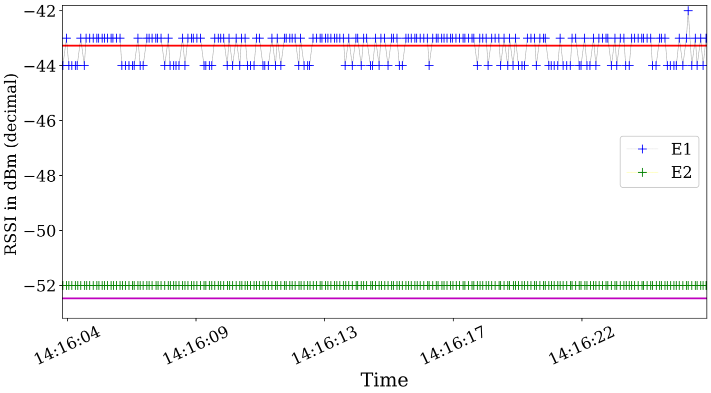


Figure 5.12: RSS values are obtained in an ideal scenario. The graphs use the timestamp of the packets on the x-axis and are plotted for only 20s to show the behavior across the experiment. The straight lines with colors red and purple represent the average value of RSS acquired for the experiment.

Then, we analyze the RSS values and their respective ACK status information in scenarios with the jamming strategy active . For the reactive jammer, we plot the RSS values and the status transmission in Figure 5.14 . Both graphics show a completely different behavior compared to the ideal scenario.

In particular, a lot of errors of the 01 type occurs when the jamming strategy is activated. This means that the packet that was transmitted was reported as a failure transmission due to collisions 5.13.

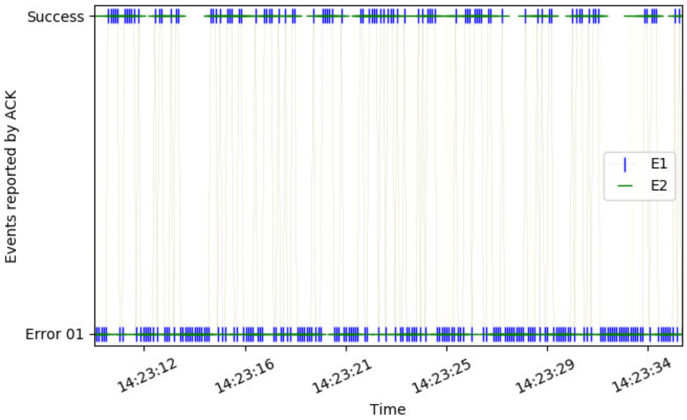


Figure 5.13: Events reported by the ACK in the communications for $SINR = 3.1$ with $BE = 0$ for the transmitter and the interferer as reactive. Only 20s are graphed to show the behavior of the events across the experiment, but the trend is the same for other time periods.

Finally, using the same configuration of the experiments with the reactive jammer, we implement the constant jamming strategy. In the same way as the reactive jammer status report, the constant jammer presents a lot of errors. However, the major difference is in the variance of the RSS values as shown in Figure 5.14

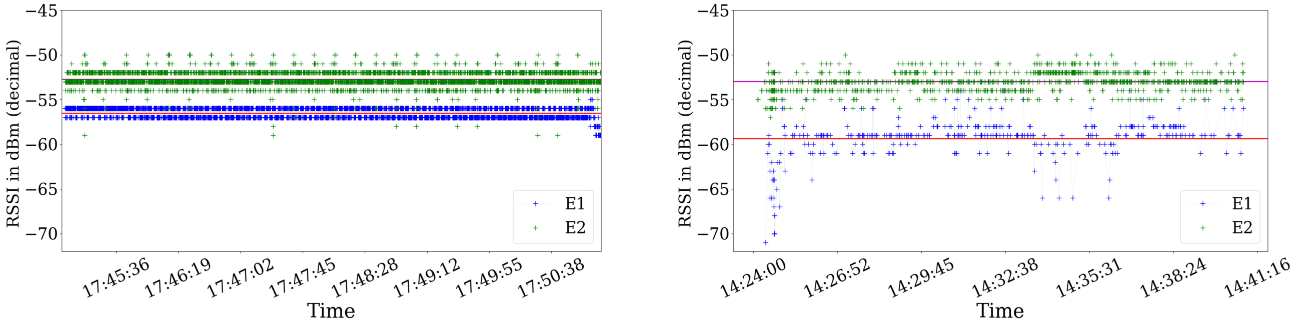


Figure 5.14: The differences of the RSS values for the reactive in the left figure, and constant strategy in the right figure. To show the comparisson, we use the average values of RSS for each transmitter, in each experiment to present the differences in the behavior. The RSS scale is the same for both figures, only the time axis is different and presented.

We also analyze the variance and standard deviation of the RSS values for different values of SINR and jamming strategies. For the reactive strategy, exist a correlation between the variance and the SINR for the round of experiment realized. When the SINR is lower than 4db, the variance present higher values for the range. However, for values of SINR above 7db, the variance achieves its lowest value of 0.3 as shown in Table 5.7.

Nevertheless, the constant jamming behavior is different for all the range of values of SINR analyzed. The variance presents values above of 1.22 for all of the SINR values obtained in the different experiments. Contrary to the reactive strategy, the constant strategy impacts the RSS values reported by the sensing states. As a consequence, the RSS can be used to improve the detection of attacks in the communication channel, under the assumptions of this work.

Table 5.7: Variance and standard deviation for different experiments and for reactive and constant jamming strategies. The variance of the experiments with a reactive jammer is lower than the constant strategy despite the SINR value.

| **Jamming Strategy** | **SINR (dB)** | $\sigma^2$ | **s** |
|---|---|---|---|
| Reactive | 1.07543 | 0.958289 | 0.923695 |
| | 2.77794 | 0.393903 | 0.57733 |
| | 4.02021 | 0.528474 | 0.684472 |
| | 7.75030 | 0.301342 | 0.546662 |
| Constant | 1.18 | 1.20259 | 1.44623 |
| | 2.05376 | 2.538727 | 6.441381 |
| | 4.48245 | 8.4857244 | 2.913026 |
| | 7.0952 | 0.867233 | 0.7564364 |

In some experiments, the channel suffered from impulsive interference noises that affected the variance of the RSS values in specific time ranges. Specifically, when the impulsive burst noise affects the transmitters, the ACK immediately reported a failed transmission status. In Figure 5.15, the occurrence of impulsive burst noise can be appreciated for the timestamp values between 13:48:57 to 13:49:17. As a consequence, the RSS has the highest values across the experiment for this timestamp range for both transmitters.

Summarizing, this behavior shows that the CE can cope with the presence of impulsive interference noises for some packets. For the packets that are not captured, the ACK mechanism can detect the collision and report the transmission failure. We emphasize that the E1 transmitter is under interferences across the experiments but does not lead to an error in the transmission. According to the study of the interferences realized in Chapter 3, the collision occurred outside of the preamble or header bytes of the packet.

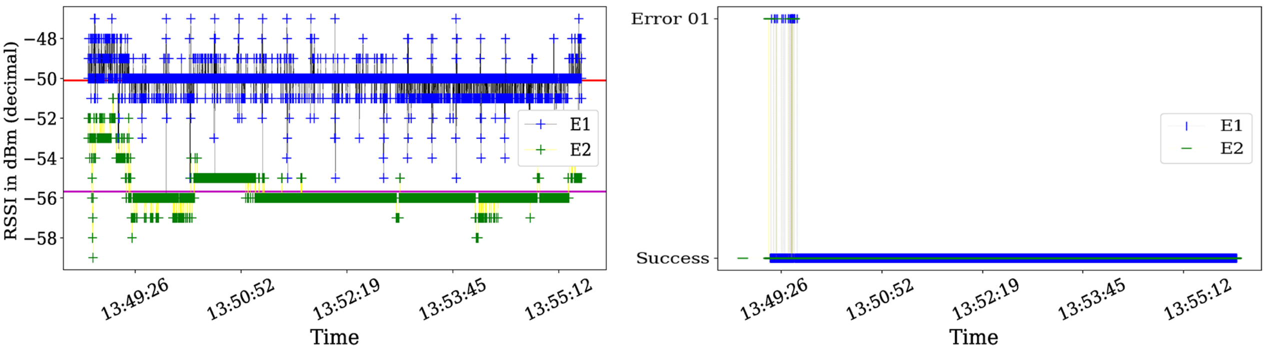


Figure 5.15: Figure in the left show the RSS value across the experiments and the presence of the impulsive interference noise in the range of 13:48:57 to 13:49:17 for both transmitters. Consequently, figure in the right, expose that for that range of timestamp, the ACK reports a failure in the transmission process. However, the presence of interference for the E1 transmitter across the experiments does not lead to error in the transmission.

The variance that the noise of the burst type and the constant strategy provokes in the RSS values are critical for localization applications [57]. To correctly distinguish the presence of attackers, the analysis of various performance metrics as RSS, PDR, and goodput is mandatory. Therefore, it is important to use countermeasures that combine use various performance metrics with the RSS values to analyze the presence of attackers.

### 5.2.5 Energy Consumption

The energy consumption is calculated using the assumption and associations described in Section 4.1.2 for the single packet transmission. Consequently, we need to calculate the energy consumption for the total packets that are transmitted in the time of the experiment $t_{xp}$ in each scenario. Finally, we correlate the ideal and worst-case scenario with the XBee processes to obtain the time in each scenario for the ATMega2560. Using the time of the experiment and the total transmissions generated by the master clock, we know that a 9000 process of transmission will be generated. Hence, in Table 5.8, we present the different timing and energy consumption for each scenario

Table 5.8: Duty cycle and electrical characteristics of each device and strategy of the attacker used in the experiments. Finally, the energy consumption for each scenario is calculated based on the estimation and considerations detailed in this section.

| **Device/Rol** | **Scenario** | **Duty Cycle** | | **Current Consumption** | | **Vcc** | **J** |
|---|---|---|---|---|---|---|---|
| | | tat | tid | On | Idle | | |
| XBee (Transmitter) | Ideal | 15 s | 885 s | 45 mA | 50 mA | 3.3 V | 148.253 |
| | Worst | 173 s | 727 s | | | | 145.646 |
| ATMega2560(Transmitter) | Ideal | 8.676 s | 891.324 s | 4 mA | 14 mA | 5 V | 62.567 |
| | Worst | 16.452 s | 883.548 s | | | | 62.177 |
| VCO(Constant Jammer) | - | 900 | - | 27 mA | - | 12 V | 291.6 |
| XBee(Reactive Jammer) | - | | | 45 mA | - | 3.3 V | 133.65 |

The results are consistent with the methodology and the works that analyze these types of strategies. The constant jammer has higher energy consumption than the other devices and the reactive strategy. However, is interesting to remark that the energy consumption of the transceiver does not present great variations. Moreover, in the worst-case scenario, the XBee has a lower energy consumption than the ideal scenario. This behavior is because the current consumption in the transmitting mode is lower than the idle mode. As a consequence, when a lot of retransmission occurs, the transmitting mode generates more active time, and this compensates for the energy consumption of the ideal scenario. A similar behavior accounts for the reactive jamming implemented in the XBee devices, as shown in Figure 5.16

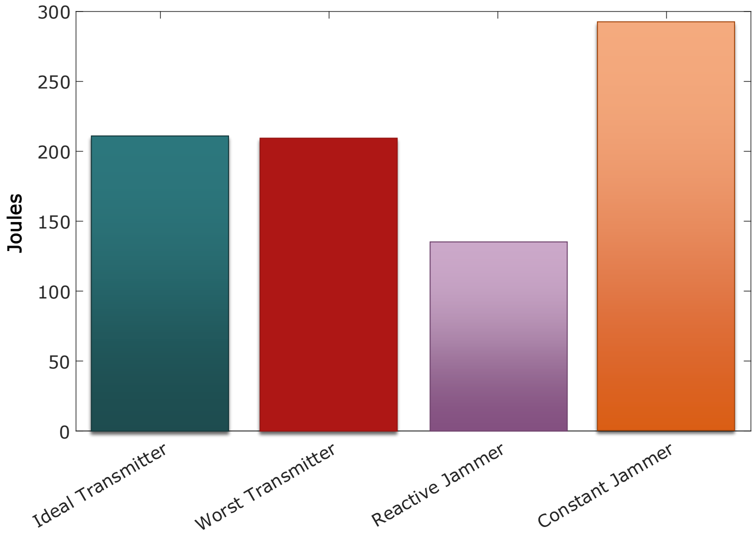


Figure 5.16: Bar plot of the energy consumption of each device with their corresponding role in the experiments. The transmitters' consumption groups the consumption of the XBee and ATMega2560 MCU. With the used assumptions, the reactive jammer has lesser energy consumption due to only needs the XBee device. Conversely, the VCO has a higher consumption owing to the strategy followed.

Specifically, the energy consumption of the transmitters in the worst scenario from the reactive strategy is 35% lower with a $r_j = 0.192$. As a consequence, the attacker could severely impact the lifetime of the networks using transceivers with similar characteristics. Therefore, the integrity of the patients using devices that provides medicine is at notorious risk. We recommend the use of devices with higher energy efficiency between the transmitting and idle state to improve the lifetime of the network. However, the detection of the attacker is mandatory to preserve the integrity of the network and the commmunication systems.

# Chapter 6

# Conclusions and Future Work

In this work, we presented an analytical and experimentally evaluation of the performance of an IEEE 802.15.4 network using CSMA-CA in the presence of reactive and constant jamming strategies. Furthermore, using different backoff times, we analyze the scheduling of the protocol to evaluate its impact as a countermeasure of the attackers. Using the PDR, SINR, goodput, energy consumption , and the RSSI values, we compare the performance of the network in the presence and absence of the attackers. The results show that both strategies have a significant impact on the analyzed metrics.

By analyzing the performance metrics, we proposed an extended probabilistic model to incorporate the presence of attackers. The analytical and experimental results show a good agreement for the considerations and assumptions used in this work. In particular, the SINR and the synchronization of the signals are critical factors that diminish the performance of the network. Specifically, the performance metrics are intrinsically correlated with the SINR values in the communication link. Therefore, there is a range of SINR values that permits the reception of the packets, despite the jamming strategy used and synchronization of the signals. However, this highly depends on the number of interferers present in the network.

The principal differences of the jamming strategy are in terms of energy consumption and the statistics of the RSSI values . The reactive jamming consumes 54% less energy than the constant jamming, with the same impact on the network. Moreover, the variance of the RSSI values is notoriously higher for the constant strategy compared to the reactive strategy. Although, the implementation of the reactive strategy represents several difficulties that make this strategy complex to implement.

With the analysis of the experimental, we correlate the probability to jam with the MAC model. The proposed model for the jammer shows a good agreement with the experimental data obtained for different numbers of nodes. However, the curve is valid only for one interferer ($N_{\mathrm{i}} = 1$) and considering the specific protection ratio of our scenario. Also, the curve is valid under the assumptions of synchronization and SINR used in this work.

Furthermore, we found that the capture effect is not able to cope with impulsive interference noise. Therefore, when the countermeasure mechanisms are implemented, we need to consider that some variations of the RSSI or report status can be the product of impulsive interference noise. As a consequence, the transmission status can improve the detection of attacks in the network. However, the ACK by itself can not distinguish the real cause of the failures.

Moreover, the CSMA/CA algorithm can avoid most of the collisions that are generated in the transmission by using the backoffs. In any case, to counteract the attacker's effect, the only way to do it is by knowing the attacker's strategy and thereby adjusting the $BE$ values accordingly.

Finally, more experiments, with different packet sizes and different attack strategies need to be carried out to extend the evaluation of the network under jamming attacks, and the probabilistic model for a major numbers of nodes.

# Annexes

## Appendix A:

### International Conferences

- **Nicolás López-Vilos**, C. A. Azurdia-Meza, Samuel Montejo-Sanchez and Claudio Valencia, 'Experimental Evaluation of Capture Effect in an IEEE 802.15.4 WSN based on Unslotted-CSMA/CA,' *in Proc. 2020 IEEE 12th Latin-American Conference on Communications (LATINCOM)*, Virtual Conference.

- **Nicolás López-Vilos**, C. A. Azurdia-Meza, Claudio Valencia and Samuel Montejo-Sanchez, 'On the performance of 6LoWPAN using TSCH/Orchestra mode against a jamming attack,' *in Proc. 2019 IEEE CHILECON* , Valparaiso , Chile.

### Journals

- **Nicolás López-Vilos**,Claudio Valencia, C. A. Azurdia-Meza and Samuel Montejo-Sanchez, 'Performance Analysis of the IEEE 802.15.4 protocol for WBAN in a Smart Home Enviroment Under Jamming Attacks,' *Special Issue "Electronics for E-health Sensor Systems", Sensors 2020.*

## Appendix B: Codes

All the codes used in this work are available in the following link:

```
https://github.com/xb33/Thesis
```

# Bibliography

[1] D. International, “Xbee/xbee-pro s1 802.15.4 (legacy) user guide,”

[2] N. Instruments, *Specifications USRP-2921; Software Defined Radio Device.*

[3] F. Semiconductor, “Mc13211/212/213, zigbee compliant platform 2.4 ghz low power transceiver for the ieee 802.15.4 standard plus microcontroller,” tech. rep.

[4] L. S. C. of the IEEE Computer Society, “Ieee std 802.15.4 2015, ieee standard for low-rate wireless networks.”

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” vol. 104, pp. 1727–1765, Institute of Electrical and Electronics Engineers (IEEE), sep 2016.

[6] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, “Jamming attacks on wireless networks: A taxonomic survey,” *International Journal of Production Economics*, vol. 172, pp. 76–94, feb 2016.

[7] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attack strategies and network defense policies in wireless sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119–1133, 2010.

[8] Y. M. Amin and A. T. Abdel-Hamid, “A comprehensive taxonomy and analysis of ieee 802.15.4 attacks,” *Journal of Electrical and Computer Engineering*, vol. 2016, no. 7165952, p. 12, 2016.

[9] P. Park, P. D. Marco, P. Soldati, C. Fischione, and K. H. Johansson, “A generalized markov chain modelfor effective analysis of slotted ieee 802.15.4,” IEEE, 2009.

[10] D. Striccoli, G. Boggia, and L. A. Grieco, “A markov model for characterizing ieee802.15.4 mac layer in noisy environments,” *IEEE Transactions on Industrial Electronics*, vol. 62, no. 8, 2015.

[11] D. D. Guglielmo, B. A. Nahas, S. Duquennoy, T. Voigt, and G. Anastasi, “Analysis and experimental evaluation of IEEE 802.15.4e TSCH CSMA-CA algorithm,” *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 1573–1588, feb 2017.

[12] P. D. Marco, P. Park, C. Fischione, and K. H. Johansson, “Analytical modeling of multi-

hop IEEE 802.15.4 networks," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 3191–3208, sep 2012.

[13] X. Cao, J. Chen, Y. Cheng, X. S. Shen, and Y. Sun, "An analytical MAC model for IEEE 802.15.4 enabled wireless networks with periodic traffic," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 5261–5273, oct 2015.

[14] A. Faridi, M. R. Palattella, A. Lozano, M. Dohler, G. Boggia, L. A. Grieco, and P. Camarda, "Comprehensive evaluation of the IEEE 802.15.4 MAC layer performance with retransmissions," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 3917–3932, oct 2010.

[15] N. Lopez, C. Azurdia-Meza, C. Valencia, and S. Montejo-Sanchez, "On the performance of 6lowpan using tsch/orchestra mode against a jamming attack," in *IEEE Chilean Conference on Electrical, Electronics Engineering, and Informatics and Communication Technologies*, IEEE, 2019.

[16] N. A. Lopez, C. A. Azurdia-Meza, S. Montejo-Sanchez, and C. Valencia, "Experimental evaluation of capture effect in an ieee 802.15.4 wsn based on unslotted-csma/ca," in *IEEE Chilean Conference on Electrical, Electronics Engineering, and Informatics and Communication Technologies*, IEEE, 2020.

[17] P. Park, P. D. Marco, C. Fischione, and K. H. Johansson, "Modeling and optimization of the ieee 802.15.4 protocol for reliable and timely communications," *IEEE Trans Parallel Distrib Syst*, vol. 24, no. 3, 2013.

[18] P. D. Marco, C. Fischione, F. Santucci, and K. H. Johansson, "Modeling IEEE 802.15.4 networks over fading channels," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 5366–5381, oct 2014.

[19] C. Buratti and R. Verdone, "Performance analysis of ieee 802.15.4 non beacon-enabled mode," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 3480–3493, sep 2009.

[20] C. Buratti, "Performance analysis of IEEE 802.15.4 beacon-enabled mode," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2031–2045, may 2010.

[21] M. Gribaudo, D. Manini, A. Nordio, and C.-F. Chiasserini, "Transient analysis of IEEE 802.15.4 sensor networks," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 1165–1175, apr 2011.

[22] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. V. der Perreand Ingrid Moerman, A. Bahai, P. Varaiya, and F. Catthoor, "Performance analysis of slotted carrier sense ieee 802.15.4 medium access layer," *IEEE Transactions on Wireless Communications*, 2008.

[23] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, 2000.

[24] M. P. R. S. Kiran and P. Rajalakshmi, "Performance analysis of CSMA/CA and PCA for

time critical industrial IoT applications," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 2281–2293, may 2018.

[25] C. Gezer, C. Buratti, and R. Verdone, "Capture effect and in ieee and 802.15.4 networks and modelling and experimentation," IEEE, 2010.

[26] S. Amuru, H. S. Dhillon, and R. M. Buehrer, "On jamming against wireless networks," *IEEE Transactions on Wireless Communications*, 2017.

[27] D. Yuan and M. Hollick, "Let's talk together: Understanding concurrent transmission in wireless sensor networks," pp. 219–227, 2013.

[28] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1746–1759, 2014.

[29] A. Tsiota, D. Xenakis, N. Passas, and L. Merakos, "On jamming and black hole attacks in heterogeneous wireless networks," *IEEE Transactions on Vehicular Technology*, 2019.

[30] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of ieee 802.11 under jamming," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 1265–1273, 2008.

[31] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 1593–1603, mar 2014.

[32] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192 – 219, 2016.

[33] C. Bormann, M. Ersue, and A.Keranen, "Terminology for constrained-node networks rfc 7228," May 2014.

[34] D. D. Guglielmo, S. Brienza, and G. Anastasi, "IEEE 802.15.4e: A survey," *Computer Communications*, vol. 88, pp. 1–24, aug 2016.

[35] "Zigbee specification v1.0."

[36] "Hart field communication protocol specification."

[37] "Rfc 4944 : Transmission of ipv6 packets over ieee 802.15.4 networks [online],"

[38] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent manufacturing in the context of industry 4.0: A review," *Engineering*, vol. 3, pp. 616–630, oct 2017.

[39] X. Cheng, J. Shi, and M. Sha, "Cracking the channel hopping sequences in ieee 802.15.4e-based industrial tsch networks," in *Proceedings of the International Conference on Internet of Things Design and Implementation*, IoTDI '19, (New York, NY, USA), p. 130–141, Association for Computing Machinery, 2019.

[40] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?," in *WiSec 11*, 2011.

[41] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks:the case of jammers," *IEEE Commun Surveys Tuts*, 2011.

[42] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks : A survey," *IEEE Communications Surverys and Tutorial*, 2014.

[43] A. Proano and L. Lazos, "Selective jamming and attacks in wireless and networks," IEEE, 2010.

[44] S. Duquennoy, B. A. Nahas, O. Landsiedel, and T. Watteyne, "Orchestra robust mesh networks through autonomously scheduled tsch," 2015.

[45] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery," in *The Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II.*, pp. 45–52, 2005.

[46] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," IEEE, 2004.

[47] B. Bloessl, C. Leitner, F. Dressler, and C. Sommer, "A gnu radio-based ieee 802.15.4 testbed," IEEE, 2003.

[48] T. Instruments, "Cc2420 2.4 ghz ieee 802.15.4 / zigbee-ready rf transceiver datasheet (rev. c)," tech. rep.

[49] Microchip, *ATmega640/V-1280/V-1281/V-2560/V-2561/V.*

[50] *Voltage Controlled Oscillator ZX95-2650+.*

[51] Zolertia, "Z1 datasheet." Z1 Datasheet, 2010.

[52] M. O. Farooq and T. Kunz, "Contiki-based ieee 802.15.4 channel capacity estimation and suitability of its csma-ca mac layer protocol for real-time multimedia applications," *Hindawi Publishing Corporation*, vol. 2015, 2015.

[53] H. Tall, G. Chalhoub, and M. Misson, "Implementation of ieee 802.15.4 unslotted csma/ca protocol on contiki os," *International Journal of Engineering Research and Technology (IJERT)*, 2016.

[54] A. F. Molisch, K. Balakrishnan, D. Cassioli, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "Ieee 802.15.4a channel model and final report," tech. rep., IEEE, 1000.

[55] K. Takizawa, T. Aoyagi, J. ichi Takada, and N. Katayama, "Channel models for wireless body area networks," in *30th Annual International IEEE EMBS Conference Vancouver,*

*British Columbia, Canada, August 20-24, 2008*, IEEE, 2008.

[56] R. D. Francisco, “Indoor channel measurements and models at 2.4 ghz in a hospital,” 2010.

[57] V. Bianchi, P. Ciampolini, and I. D. Munari, “RSSI-based indoor localization and identification for ZigBee wireless sensor networks in smart homes,” *IEEE Transactions on Instrumentation and Measurement*, vol. 68, pp. 566–575, feb 2019.

[58] R. Xu, L. Lei, X. Xiong, K. Zheng, and H. Shen, “A software defined radio based ieee 802.15.4k testbed for m2m applications,” *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, 2016.

[59] D. Son, B. Krishnamachari, and J. S. Heidemann, “Experimental study of concurrent transmission in wireless sensor networks,” in *SenSys 06*, 2006.

[60] R. Alexander, A. Brandt, J. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, and T. Winter, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” Mar. 2012.

[61] C. A. Boano, Z. He, Y. Li, T. Voigt, M. Zuñiga, and A. Willig, “Controllable radio and interference for experimental and testing purposes and in wireless and sensor networks,” IEEE, 2009.

[62] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki - a lightweight and flexible operating system for tiny networkedsensors,” *29th Annual IEEE International Conference on Local Computer Networks*, 2004.

[63] L. Kanaris, C. Sergiou, A. Kokkinis, A. Pafitis, N. Antoniou, and S. Stavrou, “On the realistic radio and network planning of iot sensor networks,” *IEEE Journal Sensors*, 2019.

[64] O. F. Mottola, Luca, Voigt, Thiemo, Tsiftes, Nicolas, and A. Dunkels, “Strawman: Resolving collisions in bursty low-power wireless networks,” in *Proceedings of the 11th International Conference on Information Processing in Sensor Networks*, IPSN ’12, (New York, NY, USA), p. 161–172, Association for Computing Machinery, 2012.