Instituto Politécnico
de Viana do Castelo

EXPLORING IOT SECURITY VULNERABILITIES IN LPWANS: THE IPVC BIRA BICYCLE USE CASE

Nuno Miguel Gramoso Rodrigues Torres

Escola Superior de Tecnologia e Gestão

Instituto Politécnico
de Viana do Castelo

Nuno Miguel Gramoso Rodrigues Torres

EXPLORING IOT SECURITY VULNERABILITIES IN LPWANS: THE IPVC BIRA BICYCLE USE CASE

Nome do curso de Mestrado

Mestrado em Cibersegurança

Trabalho efetuado sob a supervisão de

Professor Sérgio Ivan Fernandes Lopes

Professor Pedro Filipe Cruz Pinto

Março de 2022

Mestrado em Cibersegurança
Master in Cybersecurity

Exploring IoT Security Vulnerabilities in LPWANs: The IPVC BIRA Bicycle Use Case

a master's thesis authored by

Nuno Miguel Gramoso Rodrigues Torres

and supervised by

Sérgio Ivan Fernandes Lopes
Professor Adjunto, Instituto Politécnico de Viana do Castelo

Pedro Filipe Cruz Pinto
Professor Adjunto, Instituto Politécnico de Viana do Castelo

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

29 of March, 2022

Abstract

Due to its pervasive nature, the Internet of Things (IoT) is demanding for Low Power Wide Area Networks (LPWAN) since wirelessly connected devices need battery-efficient and long-range communications. By using LPWAN technologies, the IoT devices are less dependent on common infrastructures, can operate using small batteries (up to 10 years), and can be easily deployed within wide areas (above 2 km). On the other hand, LPWAN-based IoT applications need to be secure since its data could contain confidential users' information.

This work provides a systematic overview regarding the security vulnerabilities that exist in LPWANs, followed by a literature review with the main goals of substantiating an attack vector analysis specifically designed for the IoT ecosystem. With the knowledge from the systematic overview, a secure LoRa-based tracking system for the BIRA bicycle was proposed. The system consists of BIRA bicycles equipped with low-cost Global Positioning (GPS) trackers. Lastly, an experimental setup was developed with a focus on hacking the Radio Frequency (RF) physical layer with Software Defined Radio (SDR) techniques, performing GPS Spoofing, Replay Attacks, Denial-of-Service (DoS) and Jamming, in an environment that relies on LoRaWAN networks.

Results have shown that LPWANs contains security vulnerabilities that can lead to irreversible harm. Also, the conception and implementation of up-to-date defenses are relevant to protect systems, networks, and data. It was possible to verify that depending on the type of activation method used between the devices and the LoRaWAN server, the communications and the devices can be compromised.

Keywords: LPWAN. IoT. Cybersecurity. Hacking. LoRaWAN. Smart Campus. Smart Mobility.

Resumo

Devido à sua natureza pervasiva, a Internet das Coisas (IoT) necessita de Redes de Baixo Consumo e Longo Alcance (LPWAN) uma vez que os dispositivos sem fios necessitam de comunicações de longo alcance e eficientes em termos de bateria. Ao utilizar as tecnologias LPWAN, os dispositivos IoT ficam menos dependentes de infra-estruturas existentes, podem funcionar com baterias pequenas (até 10 anos), e podem ser facilmente instalados em áreas amplas (acima de 2 km). Trabalhar em ambientes IoT baseados em LPWAN, faz com que aplicações críticas necessitem de ser seguras, visto que os seus dados podem conter informações confidenciais dos utilizadores.

Neste trabalho é apresentada uma revisão sistemática sobre as vulnerabilidades de segurança existentes em LPWANs, seguida de uma revisão da literatura com o principal objectivo de sustentar uma análise de vetores de ataque especificamente concebida para o ecossistema IoT. Com os conhecimentos da revisão sistemática, foi proposto um sistema de localização seguro para a bicicleta BIRA, baseado em tecnologia de comunicações LoRaWAN. O sistema consiste em bicicletas BIRA equipadas com localizadores GPS de baixo custo. Por fim, foi implementado um conjunto de testes com foco na exploração da camada física de Rádiofrequência (RF) através de técnicas de Rádio Definido por Software (SDR), tendo sido executados vários tipos de ataques, nomeadamente GPS *Spoofing*, *Replay Attacks*, *DoS* and *Jamming*, considerando uma infraestrutura LoRaWAN de comunicações.

Os resultados demonstram que as LPWAN contêm vulnerabilidades de segurança que podem levar a danos irreversíveis. Além disso, a conceção e implementação de defesas atualizadas são relevantes para proteger sistemas, redes, e dados. Foi possível verificar que, dependendo do tipo de modo de activação utilizado entre os dispositivos e o servidor LoRaWAN, as comunicações e os dispositivos podem ser comprometidos.

Palavras-chave: LPWAN. IoT. Cibersegurança. Hacking. LoRaWAN. Campus Inteligente. Mobilidade Inteligente.

Acknowledgements

First, I would like to thank my advisor Professor Sérgio Lopes and co-advisor Professor Pedro Pinto, for all the availability and effort shown throughout this long journey, which always helped me when I needed it most. Without them, I would not be able to present this work. Then, I want to thank my colleague Pedro Martins for his availability during the development of the BIRA bicycle application. Thanks also to Rafael Pereira from DIGIHEART for assisting me with the LoRa server integrations. Last but not least, I want to thank my family and friends for all their support and encouragement demonstrated over these months. Lastly, a very special thanks to my girlfriend, who is one of the main reasons for my happiness, who supports and motivates me every day.

Contents

List of Figures

List of Tables

List of Listings

List of Abbreviations

ABP Activation by Personalization

AES Advanced Encryption Standard

AppKey Application Key

AppSKey Application Session Key

CMAC Cipher-based Message Authentication Code

COTS Commercial-Off-The-Shelf

CPU Central Processing Unit

CSS Chirp Spread Spectrum

DDoS Distributed-Denial-of-Service

DevAddr Device Address

DoS Denial-of-Service

FCNT Frame/Header Counter

FTDI Future Technology Devices International

GPS Global Positioning

GRC GNU Radio Companion

HSM Hardware Security Module

IC Integrated Circuit

ID Identification

IDS Intrusion Detection System

IoT Internet of Things

IP Internet Protocol

IPVC Instituto Politécnico de Viana do Castelo

IPVC S2C IPVC Smart & Sustainable Campus

ITS Intelligent Transportation Systems

LPWAN Low Power Wide Area Networks

LTE Long-Term Evolution

M2M Machine-to-Machine

MAC Message Authentication Code

MCU MicroController Unit

MCyber Master in Cybersecurity

MIC Message Integrity Code

MitM Man-in-the-Middle

NB-IoT Narrowband IoT

NwkSKey Network Session Key

O-D Origin–Destination

OTAA Over The Air Authentication

QoS Quality of Service

RF Radio Frequency

RFID Radio Frequency Identification

RSSI Received Signal Strength Indicator

SDN Software-defined Networking

SDR Software Defined Radio

SF Spreading Factor

SN Sequence Number

SNR Signal-to-Noise Ratio

SoA Software-oriented Architectures

SPI Serial Peripheral Interface

TTN The Things Network

UART Universal Asynchronous Receiver/Transmitter

UNLV University of Nevada in Las Vegas

WN Wireless Network

WoI Wake-on-Interrupt

WUR Wake-Up-Radio

Chapter 1

Introduction

The Internet of Things (IoT) is commonly known for the integration of computing and communication capabilities into everyday objects, allowing them to send and receive data through the Internet, providing interaction between the physical and digital world, via sensors and actuators. However, the storage and processing capabilities of an IoT device are restricted due to size limitation, energy, power, and computational capability [1].

Low Power Wide Area Networks (LPWAN) technologies play a crucial role in enabling the IoT. This type of network makes it possible to have thousands of sensors/devices sending and receiving data at a lower cost, long-range, and with better battery life than other connectivity options [2]. Sensors/devices can send data over miles of range instead of feet and can last for years on battery instead of weeks or months. When working with thousands of sensors spread over a large area, wireless communications are required over a long-range and with low energy consumption. In other technologies, it is necessary to change the batteries in thousands of sensors frequently, and sending messages in another type of protocol, such as mobile phones, depends on an operator and its service charge.

IoT-based tracking applications, such as smart mobility applications, tracking of users, objects, animals, etc.) is demanding for LPWAN. When compared with other types of technologies, such as 4G, that is widely used for mobile tracking applications, LPWAN plays a crucial role equally due to the long-range coverage, although with low-energy consumption during communications.

In tracking applications, it is necessary to locate movable objects in an Urban/Rural context. As IoT devices are generally small in size, they can be easily installed, for

instance, on bicycles to protect them against theft. By combining IoT devices with LP-WAN communications, the best of both worlds can be used such as great portability due to the size of the devices, low-power consumption, and long-range due to the type of communications that normally allows coverage ranges at city levels.

1.1 Context

The Internet of Things can be defined as a network of devices or physical objects with electronics, sensors, software and a network connection that allows them to communicate with each other. These type of devices typically use LPWANs and most of these technologies include diverse vulnerabilities. IoT applications can be used in critical scenarios, such as smart homes, factory monitoring, agriculture, smart buildings, etc. When working with this type of critical applications is crucial to guarantee the security of the users, data and communications. For example, device tampering and jamming or transmitting false signals to the application are some examples of attacks that could harm the user's experience.

1.2 Problem Statement and Motivation

The LPWAN communications are used worldwide in several IoT applications with thousands of connected devices. Despite these networks support "built-in encryption", they are vulnerable to security attacks. Regardless of this security mechanisms, LPWAN is vulnerable to a wide range of attacks by using, for instance, Software Defined Radio (SDR) techniques while using the correct hardware.

Nowadays IoT devices are increasingly used to facilitate daily tasks, but in critical scenarios, this type of communications can be vulnerable, making IoT devices a target to attack [3]. When working with critical applications, it is important to make a survey on security specifications and identify the attack vectors that could be present in the application context.

Exploring these attack vectors, which are mainly composed by implementation errors and possible vulnerabilities, allow to know the impact of these attacks and to design countermeasures. This triad relationship (LPWAN-IoT-Critical Applications) is increasingly

present in daily tasks, making it the main motivation to develop this work.

1.3 Objectives

The main objective of this work consist on the study and identification of the core vulnerabilities that exist in LPWAN-based, perform an attack vector analysis, exploit some of the most relevant identified vulnerabilities, and finally to analyze and report the results. This research work is divided in the following tasks:

1. Review the most used technologies in LPWANs, to understand what the main trends are nowadays. After completing this study, identify and detail possible vulnerabilities present in this type of technologies, as well as defense strategies and solutions to mitigate this type of threats. Finally, perform an attack vectors analysis for the LPWAN-based IoT applications environment.

2. Develop an application, where LPWAN technology and IoT devices are considered, and detail its architecture, implementation, and security mechanisms. Analyze the type of threats that may arise in this application context that can be mapped into the attack vectors referred in the previously defined model.

3. Explore the security mechanisms and vulnerabilities previously identified, proposing and exploiting the attack vectors that can affect this type of communications. Once completed, present the entire process performed, as well as all the results obtained.

1.4 Contributions

This dissertation resulted in the following contributions:

- **N. Torres**, P. Pinto, S. I. Lopes, "Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem". Appl. Sci. 2021, 11, 3176, DOI: http://doi.org/10.3390/app11073176, JCR Impact Factor (2019): 2.474, SJR (2018): 0.42 (Q1).

- **N. Torres**, P. Martins, P. Pinto and S. I. Lopes, "Smart & Sustainable Mobility on Campus: A secure IoT tracking system for the BIRA Bicycle," 2021 16th Iberian

Conference on Information Systems and Technologies (CISTI), 2021, pp. 1-7, DOI: http://doi.org/10.23919/CISTI52073.2021.9476495.

- **N. Torres**, P. Pinto, S.I. Lopes, "Exploring Security Vulnerabilities in LPWANs: The IPVC BIRA Bicycle Case", SASYR - 1st Symposium of Applied Science for Young Researchers, 7 July 2021, online, Portugal, URL: http://sasyr.ipb.pt/files/SASYR_Book_Abstracts.pdf

  This work has been distinguished with the **Best Research Poster Award**, Appendix A.1.

1.5 Document Organization

The rest of this document is organized as follows. In Chapter 2, it is presented the Related Work divided in three different steps, (1) Smart Mobility and Bicycle Tracking Applications, (2) LPWANs: Systematic Overview, and (3) SDR: Techniques and Methods. The Chapter 3 details the topic of LPWANs in IoT Ecosystem, which is organized in Technologies, Security, and an Attack Vector Analysis. The Chapter 4 details the developed BIRA Bicycle Application. In this section is presented the System Architecture and the Security Mechanisms of the application. In Chapter 5, the Attack Vectors that were found before are explored and mapped to a real life scenario, in this case, to the BIRA Bicycle Application. In this section is described the defined Experimental Setup, the Implementation where some potential attacks were described and performed, and also the obtained Results and Analysis made. In Chapter 6, a discussion regarding the security analysis is presented. In Chapter 7, the main conclusions are taken.

Chapter 2

Related Work

In this chapter will be presented the State of Art, describing the research work made regarding the area of the proposal. As well will be mentioned the background needed for this proposal elaboration, such as tools, systems and platforms that are related with the proposal, including:

- Smart Mobility, including some kind of applications, such as bicycle tracking;
- LPWANs such as e.g. LoRa, Sigfox or NB-IoT;
- SDR techniques.

2.1 Smart Mobility and Bicycle Tracking Applications

Smart mobility strategies are important in a campus context. A bike-sharing program within a campus aims to provide access to a safe, healthy, and environmentally sustainable transport system for students, faculty, and administrators. Bike-sharing has the potential to increase active transport on a college campus [4]. The increased use of bicycles improves public health, reduces pollution, and resolves traffic congestion problems [5, 6].

More than 18 million bicycles are available for public use worldwide and the loss of bikes, which can be stolen or simply left in unknown places, is one of the key concerns impacting bike-sharing business models [7]. Normally, these bikes are tracked using GPS and costly cellular connections.

The work presented in [8], presents a methodology that relies on Origin–Destination (O-D) matrix to identify appropriate bike station locations, that could be replicated and used on other university campuses, helping further projects related to bike-sharing programs. Moreover, in [4], the authors present a study that serves as a starting point in understanding some important issues around free-floating bike-sharing systems on the university campus. In [6], authors assess the existing research on the effects of infrastructure (e.g., bicycle paths and parking), integration with public transport, education and marketing programs, bicycle access programs, and legal issues. The results have shown that almost all cities adopting comprehensive packages of interventions experienced large increases in the number of bicycle trips and share of people bicycling.

In [9] the authors propose a solution to integrate renewable energy sources and shared transport in a university campus. This solution is aimed to bring economic benefits to the environment and mobility, by reducing the impact of emissions and by optimizing traffic flows of vehicles in the local towns where the campus is located.

Some public bike-sharing platforms use electronic and wireless communications for tracking bicycles. These systems usually allow program operators to track bicycles and access user information that can improve the management of the system and prevent bicycle theft. Latest innovations include real-time integration of transit information and GPS tracking of bicycles. In [10], authors propose a bike-sharing program at the University of Nevada in Las Vegas (UNLV), to decrease congestion on nearby roads. This study concludes that a bike-sharing program is feasible at UNLV. However, for the success of the system, a fee structure better suited to UNLV should be developed to attract people to participate in the program.

LoRa-based bicycle tracking systems have also been proposed. In [7], a prototype of a LoRa-based tracker was developed, that may be embedded in a bicycle and tested in a large area. Results have shown that the performance of LoRa in crowded scenarios can be quite limited when using high Spreading Factors (SFs). The positioning of the gateway is critical and should be carefully studied for optimal coverage in urban environments. In [11], authors used LoRaWAN to develop a bicycle tracking and managing system. They designed the overall system, identified the necessary services, and developed and implemented the system. The tracking device was attached to the bicycle and its practicability

was analyzed. If the bicycle is moving at 15km/h, the tracker wakes up every 100 to 100m and performs a GPS fix to obtain valid coordinates. If the bike is not moving, the tracker wakes every 3 minutes, to increase the battery life.

2.2 LPWANs: Systematic Overview

To perform the systematic overview, the PRISMA checklist [12] was used as a reference, where some parts have been adapted to the topic under study. Initially, the following set of Questions were defined and the systematic overview is expected to answer each of these questions:

- **Q1**—Given the technologies LoRa, Sigfox, LPWAN, and Narrowband IoT (NB-IoT), what is the progress in the number of papers published?
- **Q2**—In the specific range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT), which security-related topics have been addressed by the researchers?
- **Q3**—Given a set of security related topics, what are its relation to LPWAN, LoRa, Sigfox, and NB-IoT?
- **Q4**—What is the progress of research papers using the range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT) and the set of security-related topics?
- **Q5**—What is the progress of research papers using the range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT) and the set of security-related topics regarding the smart application's context (such as smart campus, smart environment, and smart monitoring)?

The systematic overview follows a defined process, to structure and organize the entire research. A diagram of the systematic process is presented in Figure 2.1, which identifies all the phases, from the questions to the results.

After defining the questions, the selection of the search engine was performed. In this work, the IEEEXplore database was selected, since when compared to other types of search engines (Google Scholar, Scopus, Arxiv, MDPI, DOAJ), it was the one that demonstrated greater capacity and being user-friendly when using relatively elaborated queries (with

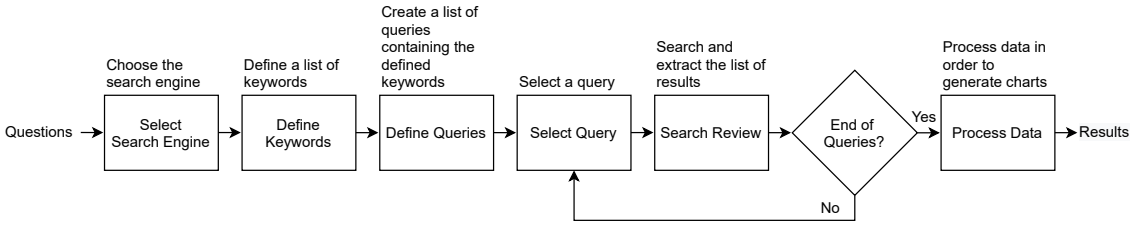


Figure 2.1: Systematic Process Diagram.

different types of fields). Specifically, it can use more than four types of keywords in one search query, and thus, all the queries defined could be easily implemented.

In the "Define keywords" step, a list of keywords was defined to be used in the construction of the queries. Defining the right keywords (e.g., attack, lora, LPWAN, exploit, security) according to the theme under study, are relevant to answer the questions. The keywords were divided into three main categories: Security-related "Security", Technology-related ("Tech"), and smart-based environments ("Smart"). In each category, the keywords were defined as presented in Table 2.1.

Table 2.1: Defined keywords.

Security Keywords	**Tech Keywords**	**Smart Keywords**
generic	lora	generic
attack	sigfox	smart
defense	lpwan	smart campus
exploit	nb-iot	smart environment
security	-	smart monitoring
privacy	-	-
vulnerabilities	-	-

The following step is to "Define Queries". To elaborate the queries, the keywords were arranged and combined. The queries accepted by IEEExplore search engine obey to the following format: ("Document Title":lora OR "Document Title":sigfox OR "Document Title": LPWAN OR "Document Title":nb-iot) AND ("All Metadata":attack)—this query returns articles where the document title includes "lora" or "sigfox" or "LPWAN" or "nb-iot" and in all metadata, the word "attack" exists.

The queries were defined and grouped in the same categories of the keywords and, in total, sixteen queries were performed as follows in Figure 2.2.

In the "Data extraction & synthesis" step, all the publications obtained by the queries had their information collected regarding the following information:

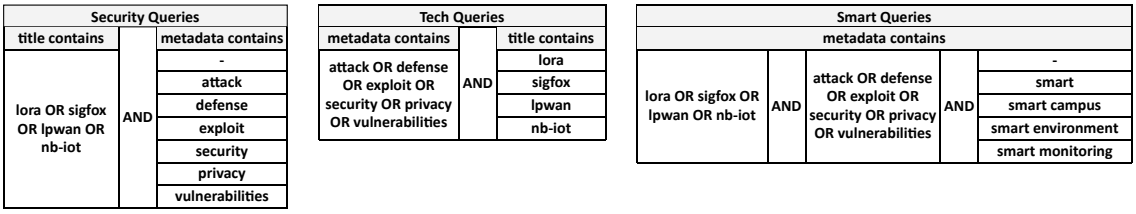


Figure 2.2: Queries defined for each category ("Security", "Tech" and "Smart").

- Title and abstract of the articles;

- Authors names;

- Publication year;

- Type of vulnerabilities/attacks/security mechanisms/defenses.

In the "Process Data" step, to select the relevant literature, inclusion and exclusion criteria were set. The adopted inclusion and exclusion criteria are presented in Table 2.2.

Table 2.2: Inclusion and Exclusion criteria for this systematic overview.

Inclusion Criteria	**Exclusion Criteria**
Papers about LPWAN communication technologies	Papers that are duplicate
Papers about LPWAN security	Papers older than 2010
Papers about LPWAN in smart environments	Papers that are not about LPWAN

After performing all the steps of the systematic process, the results were obtained and presented as a heatmap in Figure 2.3. These results are expressed in the same three categories defined in the keywords and the queries: Security, Tech, and Smart.

As final remarks, it can be highlighted that, since the queries in the "Security" and "Tech" categories depended on technologies launched around 2015 like LoRa [13] and NB-IoT [14], the results appear after 2015. In the "Security" category, the query obtaining a higher number of total papers was the more general query including the *security* word in the metadata, totaling 95 papers. In this general query, the results jump from 2 papers at the beginning of 2016 to 35 papers, in 2019. The second query with more papers in the "Security" category was the query using the *exploit* word, with a total of 57 papers. The queries related to *defense*, *vulnerabilities*, and *privacy*, obtained the least number of papers, totaling 9, 7, and 6 papers, respectively.

For the queries defined under the category "Tech", the query with *lora* counted 89 papers, more than the double of the query in second, that is, it is followed by the query with *nb-iot*, with 42 papers, the one using *lpwan*, with 24 papers, and finally *sigfox* with only 3 papers.

	title contains	metadata contains	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL
Security:	lora OR sigfox OR lpwan OR nb-iot	-	0	0	0	0	0	0	3	14	35	57	45	154
		attack	0	0	0	0	0	0	0	1	2	9	4	16
		defense	0	0	0	0	0	0	0	1	3	3	2	9
		exploit	0	0	0	0	0	0	1	6	10	21	19	57
		security	0	0	0	0	0	0	2	7	25	35	26	95
		privacy	0	0	0	0	0	0	0	0	1	4	1	6
		vulnerabilities	0	0	0	0	0	0	0	1	1	4	1	7
	metadata contains	title contains												
Tech:	attack OR defense OR exploit OR security OR privacy OR vulnerabilities	lora	0	0	0	0	0	0	2	11	14	34	28	89
		sigfox	0	0	0	0	0	0	0	0	0	2	1	3
		lpwan	0	0	0	0	0	0	1	1	9	6	7	24
		nb-iot	0	0	0	0	0	0	0	2	11	17	12	42
	metadata contains	metadata contains	metadata contains											
Smart:	lora OR sigfox OR lpwan OR nb-iot	attack OR defense OR exploit OR security OR privacy OR vulnerabilities	-	3	2	2	3	2	4	11	42	84	119	97	369
			smart	0	0	0	0	1	1	3	12	22	35	12	86
			smart campus	0	0	0	0	0	0	0	1	0	1	0	2
			smart environment	0	0	0	0	0	0	0	4	5	5	2	16
			smart monitoring	0	0	0	0	0	0	0	5	8	7	5	25

Figure 2.3: Systematic overview results by category ("Security", "Tech" and "Smart").

Regarding the topic "Smart", the generic query *smart* obtained 86 papers, with a maximum in 2019. Within the specific queries including *smart environment*, *smart campus*, and *smart monitoring*, the one that ranked higher numbers was the last, with 25 related works. It was followed by the query including *smart environment*, with 16 works, and finally *smart campus* with only 2 papers. The results regarding these specific queries are diverse over the years, without a pattern or peak that could be indicative of any factor.

The results obtained are important to understand the dynamics around security-related topics and the selected technologies and are highly dependent on: the search engine, the keywords, the queries defined, and the inclusion and exclusion criteria.

Given this, the questions initially defined can be answered as follows:

- **Q1**—Given the technologies LoRa, Sigfox, LPWAN, and NB-IoT, what is the progress in the number of papers published?

  Answer: The first results obtained date from 2016, with 3 research papers, increasing to 57, in 2019.

- **Q2**—In the specific range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT), which security-related topics have been addressed by the researchers?

  Answer: Regarding the chosen technologies, the security-related topics addressed were: *attack* with 16 papers, *defense* with 9 papers, *exploit* with 57 papers, *security* with 95 papers, *privacy* with 6 papers and *vulnerabilities* with 7 papers. All results date from the period between 2016 and 2020.

- **Q3**—Given a set of security related topics, what are its relation to LPWAN, LoRa, Sigfox, and NB-IoT?"

  Answer: With the set of security-related topics, the technology that ranked higher was *LoRa* with 89 papers, starting in 2016 with 2 studies and reaching 34 in 2019. Secondly, *NB-IoT* obtained a total of 42 papers, starting with 2 studies in 2017, and rising to 17 in 2019. Then, *LPWAN* scored 24 papers, starting with 1 study in 2016 and achieving 9 in 2018. Lastly, *Sigfox* presents a total of 3 results, starting with 2 studies in 2019 and finishing with 1 in 2020.

- **Q4**—What is the progress of research papers using the range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT) and the set of security-related topics?

  Answer: The results obtained date form 2010 and, in this year, 3 research papers were counted, increasing to 119 in 2019.

- **Q5**—What is the progress of research papers using the range of technologies (LoRa, Sigfox, LPWAN, and NB-IoT) and the set of security-related topics regarding the "smart" application's context (such as *smart campus*, *smart environment*, and *smart monitoring*)?

  Answer: The general term *smart* was the one that ranked higher with a total of 86 studies, starting in 2014 with 1 study and reaching 35 by 2019. In second appears *smart monitoring* with 25 papers, starting in 2017 with 5 studies and achieving 8 in 2018. In third place appears *smart environment* with 16 papers, with 4 studies in 2017 and rising to 5 in 2018 and 2019 respectively. Lastly, *smart campus* presented only 2 papers, with 1 in 2017 and another in 2019.

The type of LPWAN communication is used everywhere for smart cities, industrial IoT, smart homes, etc. One of the most popular protocols that use this type of communications is LoRaWAN, which has millions of connected devices. Despite being advertised as containing built-in encryption making this protocol secure by default, it makes users not worry too much about their security; however, implementation problems and some vulnerabilities that may exist make this type of network very easy to hack. These days, security vulnerabilities in LoRaWAN are not well known, neither exists any kind of tools to test it. This can make this type of communications an easy target for potential attackers [15].

2.3 SDR: Techniques and Methods

SDR is a communications system standard in which many of the traditional functions of the radio transceiver, frequently signal processing, are performed by software commands instead of hardware deployment either analog or digital [16].

The main idea of a SDR is to transfer tasks performed by hardware to software. System attributes, such as signal modulation scheme, operation frequencies and bandwidth, no longer rely on analog circuits, which are usually pre-defined in traditional radio equipment. In a SDR, they depend on a system that integrates programmable hardware and software, which provides the flexibility to modify these features. Therefore, this type of radio can be operated in different ways, making it possible to perform changes in the system features, only by simply changing the parameters in the software, even in runtime. In addition, it is possible to have a completely different communication system just by replacing the software that is executed and keeping the same hardware [17].

GNU Radio is a free and open-source software development toolkit that provides signal processing blocks to implement and simulate SDR systems [18]. It is used to design and execute algorithms that define a desired communication system [17]. There are three ways to use GNU Radio.

From a high-level perspective, it can be used with GNU Radio Companion (GRC), which is a graphical tool where it can build a SDR system by connecting signal processing blocks and establishing a processing chain or flow, from signal input to system output [17]. The types of signal processing blocks are: signal generators, filters, modulators/demodula-

tors, synchronizers, graphical skins. Each block has a predefined number of input/output interfaces and performs one or more communication functions in the software domain [19]. Every block can be independently edited, upgraded or even implemented without interfering with the entire communication chain [20].

In an intermediate level, it can be used with the programming language Python as a way of describing block connections, or at its lowest level, it can use C++ to modify or create new processing blocks, selected due to performance issues, and use these blocks in higher levels (Python or GRC) [17].

2.4 Summary

After completing the state of the art, it is possible to identify some use cases in the context of smart mobility, some of the most used LPWAN communication technologies and some potential vulnerabilities. A diversity of tools were identified (hardware, software) that could be used to exploit this type of threats present in LPWAN networks. The next chapter will be focused on LPWANs in IoT Ecosystem. It will be presented a set of technologies existing nowadays and also some vulnerabilities and threats that may arise from them. Some types of attacks will be identified and described that could be performed on these types of technologies, as well as mitigation strategies. Finally, possible attack vectors will be defined that could be present in LPWAN-based IoT applications.

Chapter 3

LPWANs in the IoT Ecosystem

The Internet of Things ecosystem, due to its pervasive nature, demands low-power and wide-area communications, particularly in applications, where IoT devices do not require high speed nor high bandwidth, but still need extended coverage. Generally, an IoT device is typically composed of: a sensing/actuating element, a small-sized battery, a low-cost microprocessor (typically a microcontroller), limited memory, and a radio module that enables low-power wireless communications. When operating, the power budget of an IoT device is mostly affected by the computing and communications tasks. This means that to increase the autonomy of an IoT device, the reduction of the computational cost and the minimization of the communication load (mainly affected by the duration and duty-cycle of data transmission, and the available bandwidth) must be a priority.

3.1 LPWAN Technologies

Reducing the computational cost from an IoT device can be achieved by selecting state-of-the-art ultra-low-power microprocessors and by using event-triggered programming techniques, such as Wake-on-Interrupt (WoI) [21] or Wake-Up-Radio (WUR) [22, 23], and by forcing the microprocessor into an ultra-low-power "sleep" state, until a WoI or WUR event occurs. These strategies can considerably reduce the overall Central Processing Unit (CPU) execution time and therefore contribute to more efficient power management of the IoT devices.

Reducing the communications power consumption can be achieved by using specific

wireless communication technologies, such as LPWAN, which represents a class of wireless technologies that have been designed for the specific needs of Machine-to-Machine (M2M) communications and the Internet of Things. LPWANs are typically used with resource-constrained IoT devices, with a focus on intermittent communications with long duty-cycles (minutes, hours, days) contributing to a huge reduction of power in the transmission task.

Battery-efficient IoT devices can operate reliably for up to 10 years [24, 25] on a single battery charge and perform long-range wireless communication at a regional/city level. Figure 3.1 depicts a set of IoT devices used in multiple application scenarios, for example, authentication using Radio Frequency Identification (RFID) [26], to a bike with a tracking device, using a LoRa network [27, 28]. These IoT devices are deployed at different communications ranges from their gateways and, in the case of the IoT devices using long-range distances, they must use efficiently the computational and communications resources.

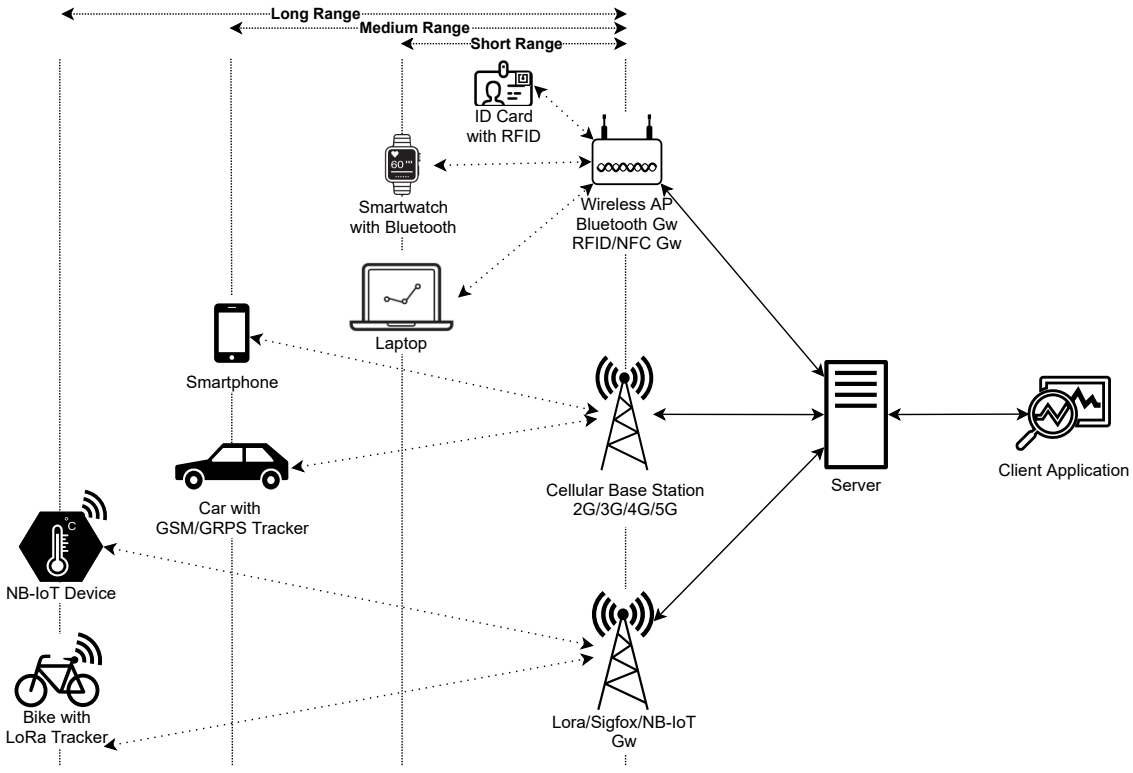


Figure 3.1: Communication Technologies in IoT applications by range.

When compared with other technologies, cf. Figure 3.2, LPWANs present higher cost-benefit and higher power/bandwidth efficiency for long-range communications, which

results in less infrastructure/hardware needs.

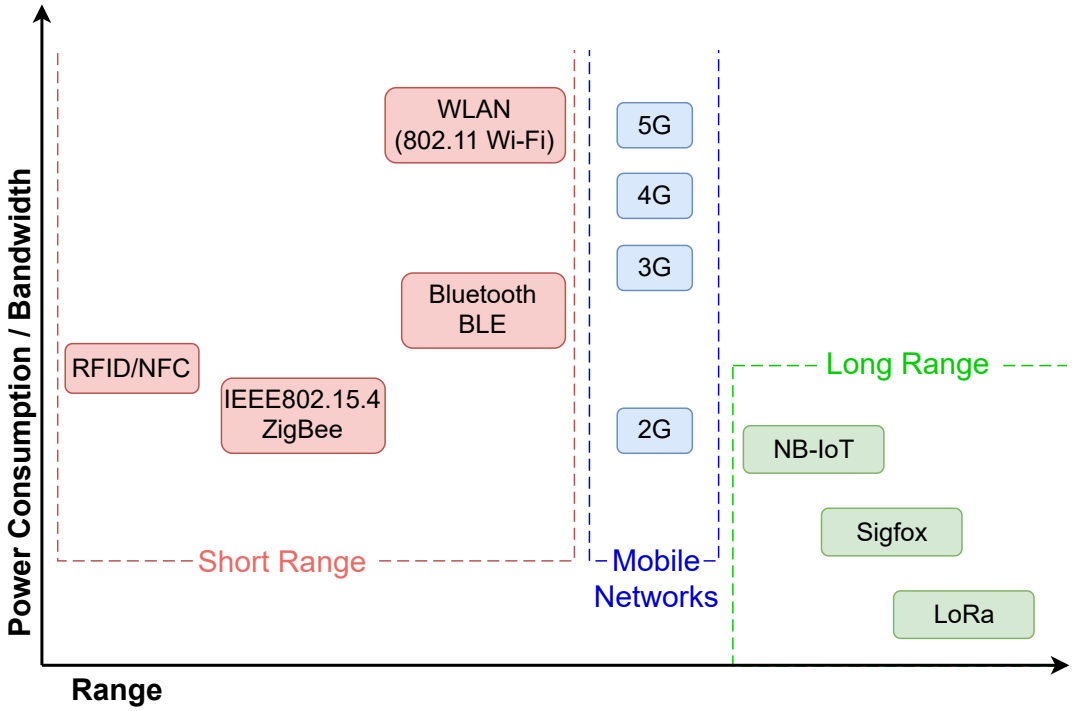


Figure 3.2: Power/Bandwidth vs Range in wireless communication Technologies. Adapted from [29].

By using LPWAN technologies, communications become less dependent on common existing infrastructures—for example, Wi-Fi, which is widely available but presents major drawbacks such as high power consumption and short-range communications—enabling IoT devices to operate on small and inexpensive batteries, and be easily deployed within a wide area, typically more than 2 km in urban zones [30]. Mobile networks like 3G and Long-Term Evolution (LTE) deliver high-speed Internet access [31]. This type of communication is characterized by a high battery drainage which does not prove to be suitable for the IoT ecosystem.

Zigbee is a worldwide standard for low-power mesh networks with enhanced security features, built on top of the IEEE 802.15.4 standard, that has been mainly used in home automation and smart building applications [32]. However, Zigbee operates on private networks [33, 34, 35], and has not been designed for long-range communications—only for small-scale projects (10–75 m) [14]— but rather to implement mesh networks. In its turn, mesh networks suffer from many factors, such as limited network coverage and high

response time [36].

NB-IoT is an LTE-based protocol that has been designed to address the needs of very low data rate and low-power devices that need to connect to the Internet using standard mobile networks [37]. It can be operated in LTE or GSM under licensed frequency bands [38], which is a major drawback, due to the use of licensed spectrum, which increases considerably the operational cost.

Mobile LPWA technologies, such as 5G-IoT and LTE-LPWA are still under development. It is anticipated that about 80 billion devices will be linked within a network, and 20.5 billion will be associated per user by 2030 [39, 40, 41]. The 5G network will be conceived to engage high data transfers and small packet transfers, that do not consume symbolic network signaling and power resources [42]. The reduction of energy consumption in 5G technologies can be accomplished by using green technologies and it can be capable of extensive connectivity and a high amount of data [43]. To make 5G-IoT less expensive over time, some solutions like large-scale manufacturing and common platforms optimization have been recommended [42].

LPWANs have been widely used in several IoT applications as the main communication technology [44]. This type of network is known for its low-power usability, long-range, low-cost, and high availability, being in use in several application domains, such as environmental monitoring for natural disaster detection [45], smart security [46], smart agriculture [47] and smart health [48]. This variety of application domains can work adequately on this technology. For example, in an e-Health IoT application, the body temperature or the blood pressure can be coded in small payloads and reported to Health Care centers, in a specific time interval (hours/days) [48]. However, if these communications are compromised, several high-risk attacks can be performed. In a scenario where a malicious agent interferes with the communications between the IoT devices and the Health Care centers, the user's health can be severely impacted. In other application domains, for example, in a bicycle sharing scenario, an attacker can compromise the location of a bicycle—by attacking the bicycle tracking system—to subtract/steal the bicycle from the system.

Moreover, LPWAN technologies can lead to security issues that were aimed to explore in this work. For instance, SigFox does not encrypt the transmitted frame (i.e., the encryption is done by the developer, in the application layer) [49]. In LoRaWAN, the join

request is not encrypted in any way, which can lead to a possible eavesdropper that could gain information about the topology of the network [49]. Moreover, LPWAN technologies use, in general, symmetric-key cryptography in which, the end devices and the network, share the same secret key [44].

3.2 LPWANs Security

Security is one of the main requirements in real-world IoT deployments. Most of the IoT devices share a simple design that is based on the premise that they can be operated remotely and integrated with third-party applications through simple mechanisms. The pressure of releasing a device quickly can, in some cases, lead to skipping non-visible aspects like security and reliability. It is obvious that security concerns are not always considered as part of the IoT device production life cycle, such as hardware and firmware in the bottom layers, but also in higher layers, such as frameworks and applications. Many IoT devices does not support updates to the firmware/software (i.e., typically cable-based or over-the-air updates), turning them extremely exposed and vulnerable to eventual exploits and attacks [50]. Security must protect services, devices, information, and data, not only during communication but also data storage [51].

To protect privacy, it must be ensured that communication and collected data met the following requirements, as defined in [52, 53, 54]:

1. Confidentiality: transmitted data, communication between endpoints, sensors, and readers are secured and encrypted;

2. Integrity: transmitted data is accurate and cannot be modified or utilized, by unauthorized users and objects;

3. Authenticity: transmitted data is genuine, and come from authorized sensors, endpoints, and readers;

4. Availability: computing resources and information are available when requested by a service.

3.2.1 Vulnerabilities

Vulnerabilities can be discovered in a diversity of fields in IoT systems. Specifically, they can be shortcomings in system software, hardware, weaknesses in policies and procedures used in the frameworks, and flaws of the system clients themselves [55].

IoT frameworks depend on system hardware equipment and system software, and both have design and configuration defects frequently [51]. Equipment vulnerabilities are exceptionally hard to identify, due to hardware compatibility and interoperability issues, that are difficult to fix [51]. Software weaknesses are present in operating systems, application software, and control software such as communication protocols and device drivers. Some factors can lead to software design flaws, namely, human factors and software complexity [56]. Technical vulnerabilities normally occur due to human errors, failing to understand the application requirements can result in starting the project without a plan, weak communication between developers and users, lack of resources, skills, knowledge, and failure to manage and control the system [55].

LoRaWan [57] technology includes end-to-end security using network and application keys. Despite this, a malicious agent that obtains physical access to the devices can eventually compromise them; with physical access to the devices, it is possible to extract the keys. Typically, end-devices are characterized by a LoRa radio module and a host MicroController Unit (MCU). The radio module performs communications between the host microcontroller via Universal Asynchronous Receiver/Transmitter (UART) or Serial Peripheral Interface (SPI) interface. The data exchange and commands between the host and the radio module can be intercepted using external hardware to the device. An example of this type of intrusion is, for example, if a UART interface is used between two Integrated Circuits (ICs), the basic Future Technology Devices International (FTDI) interface can be used to extract all the key exchanges. Most present-day radio modules do not provide any built-in cryptography support to protect the interactions between the host microcontroller and the radio module. In this way, it is not possible to determine whether the commands issued to the radio module were sent by the MCU host or by an attacker. A malicious entity can also intercept all data exchanges between the host MCU and the radio module, and eventually use all of this information to create simulated devices with

the same credentials or even shape data payload.

Chirp Spread Spectrum (CSS) modulation is known for its firmness facing interferences, despite this, LoRa devices suffer from coexistence issues [58]. Simultaneous LoRa transmissions at the same frequency and spreading factor can meddle with each other. This weakness in LoRa physical layer permits attackers or outsiders to utilize Commercial-Off-The-Shelf (COTS) LoRa devices to jam LoRa networks.

Moreover, IoT devices typically have limited storage, being only capable to store small size group keys. If a specific key is not updated over time, using the same key makes the communications vulnerable to ciphertext-only attacks [59].

3.2.2 Threats

Threats can be defined as actions intended to explore security flaws in a system [60]. Threats derive from essentially primary sources such as human and nature [61, 62]. Natural threats are defined by earthquakes, energy flaws, hurricanes, floods, and fire. These types of threats can cause serious harm to computer systems. Security plans against natural threats can be implemented, but it is hard to prevent them from occurring. Human threats happen when people have malicious behaviors against systems, networks, or data. This threats can consist in internal or external sources. Internal threats are normally performed by someone with authorized access, and external threats are performed by groups or individuals outside the network, to sabotage and interfere with the system. Human threats are classified by Unstructured and Structured threats [51]. Unstructured threats are composed principally by inexpert individuals who use simply available hacking tools. Structured threats are composed of persons who recognize system vulnerabilities and can acknowledge, develop and exploit codes and scripts.

3.2.3 Attacks and Defense Strategies

In IoT applications such as smart campus, attacks need to be anticipated since this environment is serving the campus community, depending on a wide range of technologies and types of equipment. This normally includes several unsecured devices, systems and applications that communicate information via insecure media and use weak protocols such as HTTP, FTP, telnet [63]. Attacks are activities taken to harm a system or disturb

ordinary tasks by exploiting vulnerabilities using different techniques and tools. Attackers launch attacks to accomplish objectives either for individual realization or rewards [51]. An attack could be presented in numerous structures, including network attacks to monitor unencrypted traffic in pursuit of sensitive data; passive attacks, for example, monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication data; close-in attacks; exploitation by the users of the system [51]. The attackers can make use of these weaknesses to gain access to the systems, swipe sensitive data, and acquire confidential information for later manipulation [64]. Malicious entities can also harm the devices and stop the functionality of the services [63]. In this document, attacks will be classified into five distinct categories, cf. Table 3.1.

Table 3.1: Types of possible attacks. Adapted from [63].

Attack Type	**Description**
Physical	Attacks targeting hardware components such as device theft or malicious node injection.
Software	Attacks exploiting systems by using malicious software such as worms, viruses.
Encryption	Attacks intended to crack ciphered data.
Data Privacy	Attacks where sensitive and protected data are modified, copied without permission or erased.
Network	Unauthorized access or mapping of the network to impact availability or obtain sensitive information.

The attacks presented in Table 3.1 could be performed in LPWANs. Regarding this defined set, some mitigation and defense strategies are presented focusing on the previously described attacks. Some of the countermeasures require short modifications on the firmware or the way some technologies, for example, LoRaWAN, transceivers are integrated into an IoT device. Others require modifications to the standard to mitigate the attack vector at the beginning of the problem.

Physical-Related Attacks

If an intended individual gets access to an IoT device or a gateway, without strong hardware security policies, the whole device or even the network may be assumed as compromised. The gateway in LoRaWAN is a single failure point for the network, and it could be manipulated to disconnect hundreds of end-devices [57]. Besides, physical access by malicious entities may compromise the security keys and other data [3]. The messages could be manipulated and sent as if they had been originated from the IoT device, every message passing through it could be intercepted or even the device could be destroyed. If

security keys are stolen, the confidentiality and integrity of the message are compromised, because the attacker can intercept, decrypt or forge any messages sent within the LPWAN system [65]. Some types of attacks that can arise are:

- **Theft of devices**: The theft of physical objects helps the intruder to obtain physical access to the systems to perform several attacks that breach people's privacy and disrupt the system's availability and confidentiality [66].

- **Social Engineering:** This attack aims to manipulate individuals to divulge confidential and sensitive data [67] about the network or the devices.

- **Sleep Deprivation Attack:** This attack aims to increase the power consumption of the IoT device to decrease their lifetime by keeping the devices awake, resulting in more power consumption and forcing the IoT devices to shut down [68].

- **Malicious Node Injection:** A new malicious IoT device is physically inserted by the attacker between two or more devices to be used as a regular IoT device. It can be used to modify, capture, retrieve, process, and redirect incorrect information to other devices [69].

- **Environment:** Changing the conditions of the environment where a node is installed. This could tamper the values that are being monitored by a sensor, cf.Figure 3.3.

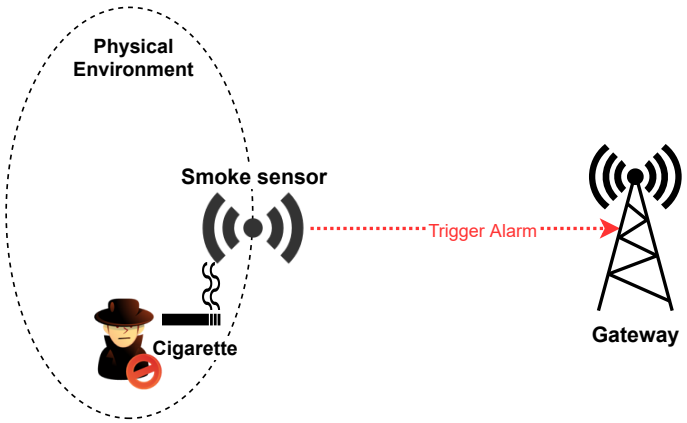


Figure 3.3: Example of physical-related attack.

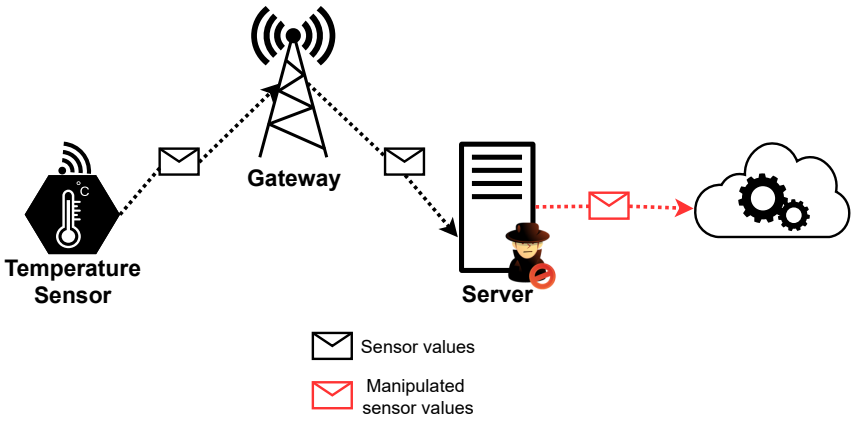
Defense Strategies: End devices should be physically protected to prevent a malicious entity to perform a system reset. This is hard to achieve in different IoT deployment environments. Design changes such as non-volatile memory may preserve the frame

counter value between resets [70]. The devices can also be protected with, for instance, Hardware Security Module (HSM). This module contains security keys and cryptography functions (e.g., encryption algorithms) and must be tamper-proof to guarantee that the keys are deleted when an attacker tries to extract them. Without using HSM, the keys have to be preserved in unsafe storage conditions (e.g., simple non-volatile memory) and may be at risk of being extracted by malicious individuals [65].

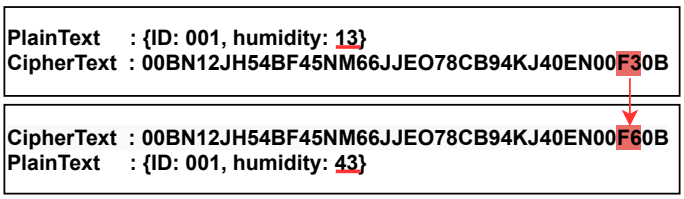
Bit-Flipping Attack

Bit-Flipping is a common attack, cf. Figure 3.4, performed to prove that the integrity between the network server and the application server is not protected. In LoRaWAN, different research studies have identified a security vulnerability that can lead to a bit flipping attack [71]. The goal of this attack is to demonstrate that the integrity between the network server and the application server is not protected. If the attacker compromise the transmissions, the application server cannot detect if the message is from the attacker or the network server [72]. Between the network and the application server, the data may be transformed during manipulation because the integrity of the encrypted text is no longer controlled when the messages arrive at the application server [73]. This means that in between the infrastructure operator's network server and the IoT solution provider's application server, the integrity and authenticity of the data is not guaranteed [70]. If an attacker gains access to a network server, they can eavesdrop on the communication between the network and the application server, which can potentially result in a bit flipping attack [72]. Bit flipping attack can be performed in a simple method, but besides simple, it can cause tragic damage even though this attack is not specifically against the cipher itself [73]. In this security attack, it is possible to change specific fields without decryption of the ciphertext [74]. The bit flipping attack is workable in specific encryption modes where a plaintext has the same bit order with a ciphertext [75], cf. Figure 3.4. An attacker can modify specific fields, just by modulating bits in the same positions of the ciphertext [71]. With this, it is only necessary to change certain fields of the ciphertext, for later when deciphered, the plaintext will be manipulated, cf. Figure 3.4b).

Defense Strategies: A malicious bit flipping of the sensor values in between the infrastructure operator and application provider is achievable due to the too-early termi-



(**a**) Bit-Flipping attack example.



(**b**) Sensor data manipulation.

Figure 3.4: Bit-Flipping attack example with manipulated sensor data. Adapted from [71].

nation of the message integrity code in the system architecture [70]. Since the protocol allows providers to choose the transmission method between two servers, there are numerous decisions, for instance, Ethernet, WiFi, 3G. For this situation, since LoRaWAN did not provide any insurance strategy between the two servers, the security between the network server and the application server relies upon the transmission method selected by the provider. Consequently, the application owner should be comfortable with the security of the transmission method and be aware of potential threats [76].

The straight solution to avoid an attack featuring a malicious change of the payload content is to run the integrity check value at the application server and not at the network server. Theoretically, a modern protocol design should implement authenticated encryption instead of simple encryption [70]. Considering the integrity protection, it is better if the protocol can provide end-to-end encryption. Therefore the security between the application server and the network server can be independent of the transmission method. Apart from that, if the transmission method is not secure, the LoRaWAN network is not secure any longer. One strategy to secure the integrity between the network server and the application server is to check the Message Integrity Code (MIC) again when the message

arrives at the application server. In the LoRaWAN specification, the MIC is checked in the network server ensuring that the messages received are not modified. After verification, the message is transmitted to the application server, but it does not verify the MIC again. The application server can also check the MIC with NwkSKey to ensure that the message is not modified during the communication between the two servers.

Jamming Attack

The jamming attack is one of the most serious problems for IoT security [77]. The communication bandwidth is small (100Hz for Sigfox, 125/250/500kHz for LoRaWAN, 180kHz for NB-IoT) and relies on low-power for data transmission [65]. The jammer does not need complex hardware as long as it transmits the jamming signal with enough power. Malicious entities can transmit powerful radio signals near the application devices and interrupt the radio communications, cf. Figure 3.5, because LoRa transmissions at the same frequency and spreading factor can interfere with each other [58]. This is possible by using COTS LoRa hardware [57].

A low-cost microcontroller-based platform equipped with a LoRa radio module can be used to perform jamming attacks. An attacker with malicious intentions can flood LoRa messages at a certain frequency to clean out all the transmissions in that frequency. According to [57], about 99% of LoRa transmissions are damaged by this jamming technique. Typically, this approach uses low-cost devices (Arduino Leonardo [78] board and a Semtech LoRa radio module [79] breakout board) with a total cost of around 30 euro. Jamming attacks could be pointed to different layers of the OSI model: (1) Physical layer jamming, where the malicious actor assign any wideband signal with a higher Signal-to-Noise Ratio (SNR) than the user; (2) MAC layer jamming, where the malicious actor just jams explicit pieces of the message (e.g., message signatures), guaranteeing that the packet is disposed of by the recipient [65].

Defense Strategies: Defending against jamming attacks is hard because this type of attack is always possible. Initially, the jamming of the entire network or frequency can be easily detected since all the devices that communicate in that frequency would abruptly start to drop out from the network. By recognizing such behavior, network administrators can take appropriate actions to prevent the impact of such attack [3]. Jamming detection

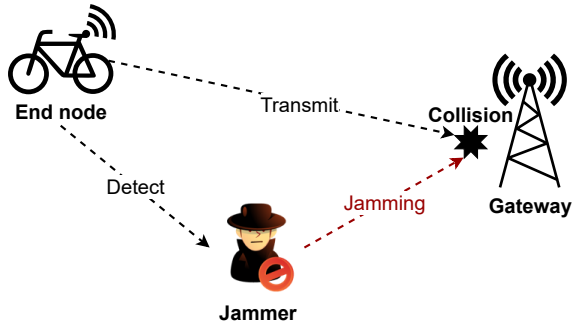


Figure 3.5: Example of jamming attack. Adapted from [80].

mechanisms can also be useful, for example, changing the used frequency channels [65]. Some low-level techniques [81] that should be used are:

- Create dense LoRa networks with overlapping coverage regions. By deploying LoRaWAN end-devices within the range of different gateways, increases the reliability of LoRa communication. This feature is critical in beating jamming attacks, as to ensure that a message is jammed, the jammer should guarantee it is heard at no gateway in the network. Since the jammer requires high Received Signal Strength Indicator (RSSI) compared with the end-device, the jammer is more effective when it is near the gateway. Subsequently, the jamming is more complex within the presence of various gateways [65], as the attacker must map the gateways in range of each target end-device to successfully jam the transmissions.

- Maximize the utilization of channel hopping. LoRa devices hop between multiple channels when sending messages as dictated by LoRaWAN specification, to reduce the opportunity of collisions. The more channels utilized, the more complex the jammer must be, as it needs to listen on all of those channels. This forces a move from basic low-cost LoRa hardware to more expensive multi-channel LoRa receivers as found in gateways.

- Move to a higher Spreading Factor (i.e., SF12) to beat the jammer RSSI. The higher SFs require higher dB differentials between the jammer and target message. With higher spreading factor transmissions, the jammer has less time to act and requires the jammer to be closer to the gateway. Note that numerous transmissions in higher SF rapidly exhaust the duty cycle allowance.

By performing traffic analysis and profiling (at the gateway or server level), it is possible to distinguish varieties in the pattern of incoming messages demonstrating the presence of a jammer and to trigger alerts or adaptations to the network. On the other hand, some application-level [81] techniques that should be addressed are:

- When the transmission rate is known, the normal rate of traffic analysis is aware of the sending rate of the LoRa end-devices, it can easily recognize unplanned changes in traffic patterns and respond accordingly.

- When the transmission rate is unknown, the typical rate of traffic should be established over time, or through past continuous profiling. Once the baseline rate is understood, it becomes possible to recognize deviations.

Replay Attack

A replay attack is an attack which consists of re-sending or repeating the legitimate data transmission by the malicious actor. The primary motivation behind this attack is tricking the device or module by utilizing handshake messages or old data from the network. To perform this attack in wireless networks, the malicious entity should know the communication frequencies and channels to sniff data from transmission between devices. The attacker receives and transmits data exchange between two trusted parties as an authorized unit, which conducts the participants to accept that the transmission of information has been finished. The malicious actor can capture and store a duplicate genuine request to a service, from a specific device in the system. After that, it can be replayed to get services that are only available to authenticated users.

For replay attack in Activation by Personalization (ABP) method in LoRaWAN, cf. Figure 3.6, the objective is to accomplish Spoofing and Denial-of-Service (DoS). After the attack execution, the server gets a malicious repeat message from the malicious actor's end device, and the server accepts that the message comes from the working end associated device. For end-user devices, the objective is to perform a DoS attack. After the effectively executed attack, the server will not get a message from the end-user devices. For development devices, which often use ABP activation to join networks, it is necessary to consider that this method is less secure. In ABP method, the devices use static keys

and after a reset, the keys continue the same as before and may be used in future sessions. Afterward, the network server may receive a malicious message that agrees with: (1) the session keys are the same as one accepted end device; (2) DevAddr is the same as one accepted end device; (3) if the counter value is acceptable. An attacker can choose and resend messages before a reset, and the server cannot figure if these messages are from this session or the session before the recovery. The LoRaWAN 1.0 protocol states that after a JoinReq—JoinAccept message exchange or a reset for a personalized end-device, the frame counters on the end-device and the frame counters on the network server for that end-device are reset to zero [70]. For this situation, the attacker can use messages from the last session with the high values counters and repeat them in the current session. In both of device is activation methods (ABP or Over The Air Authentication (OTAA)), it is possible to perform a replay attack [72]. When the frame counter value reaches its maximum value, the counter is reset and restarts from 0. With frame counter values from the last session and with the same session keys, the attacker can also repeat past messages to disconnect communications between the end device and the server [72]. However, attacking an ABP-activated end device will take less time as both reset and overflow work if the attacker has the ability and opportunity to reset end devices [70].

Defense Strategies: The replay attack depends on the perception that the NwkSKey and AppSKey are used as the long-term key material that stays unaltered after a counter reset, rather than being restricted to a single session [70]. To prevent this attack from occurring, the following measures could be taken:

End devices should be physically secured to prevent a malicious entity to start a system reset [3]. While this is hard to achieve in an assortment of IoT deployment contexts, design changes, such as non-volatile memory may maintain the counter value in between resets. If the attacker cannot reset the counter by resetting the end devices, the only way to accomplish the attack is to wait for a counter overflow [76]. This change essentially decreases the exposure, however requires an adjustment in the LoRaWAN specification. The end device should change its session keys each time when the counter reaches its maximum value. If the device is utilizing OTAA method, it should experience the OTAA activation procedure again to acquire new session keys. If the end device is using a ABP method, it should be re-configured, and session keys should be changed. For this situation,

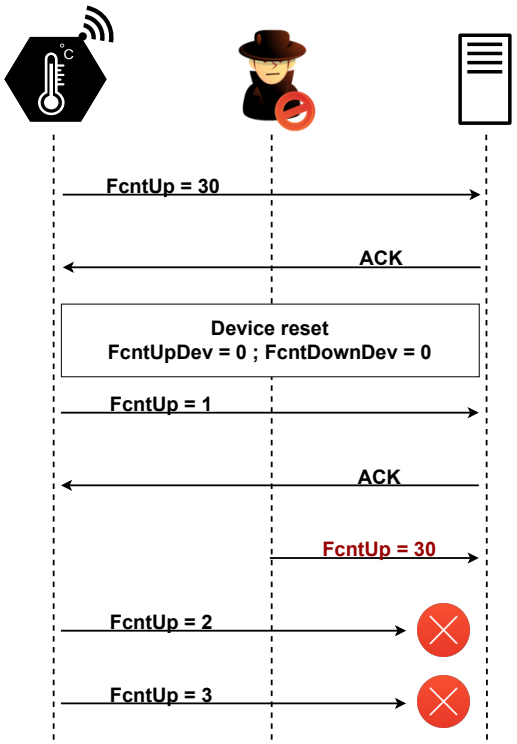


Figure 3.6: ABP device exploiting the Replay Attack. Adapted from [80].

however, the counter values are reused, session keys will prevent the server from accepting malicious messages. It is inconvenient to manually re-activate and configure an end device each time it overflows. Besides, for end devices situated in a remote area, this mitigation will cost an enormous amount of resources since it should be operated manually.

One approach to increase the security level is to remain the counter value in the server after resetting. Thereby, each time an ABP activated end device resets, its counter value will restart from zero while the relating counter value in the server will not be changed. At that point when the end device sends messages to the server, the server will not accept the messages until the counter value of the end device becomes larger than the counter value in the server. This strategy prevents all the messages with reused counter value. With that, resetting ABP activated end devices is pointless for an attacker in the replay attack. The attacker can just accomplish this attack by waiting for counter value overflowing [76].

Another technique is to add a function to end devices. Each time it resets or the counter value reaches its maximum value, the end device should be triggered and then be able to re-activate automatically. Regardless, if the end device is activated by OTAA or ABP in the last session, it should utilize OTAA to rejoin the network. This implies that

the end device should experience the "Join request—Join accept" procedure again. This technique is conceivable to be passed automatically [76].

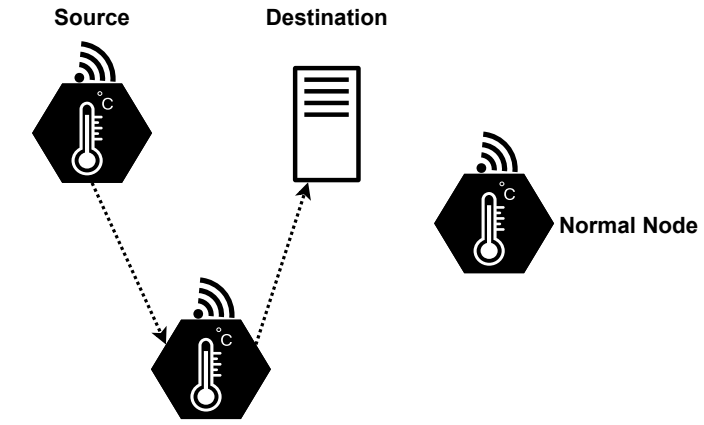
To protect against replay attacks in Sigfox communications, a 12-bit Sequence Number (SN) is used and transmitted with every uplink frame and protected by a specific Message Authentication Code (MAC). If the actual received Sigfox frame contains a lower SN than the latest received frame, the actual frame will be discarded by the Backend Server. The actual algorithm employed to compute the MAC is proprietary, but it applies Advanced Encryption Standard (AES) in Cipher-based Message Authentication Code (CMAC) mode like in the LoRaWAN protocol, with the secret not acknowledged and the 12-bit SN (for uplink messages), as some of its inputs. For downlink messages, there is no public information related to the SN size, which does not allow us to claim that the same security level is achieved when compared with uplink messages [65].

Wormhole Attack

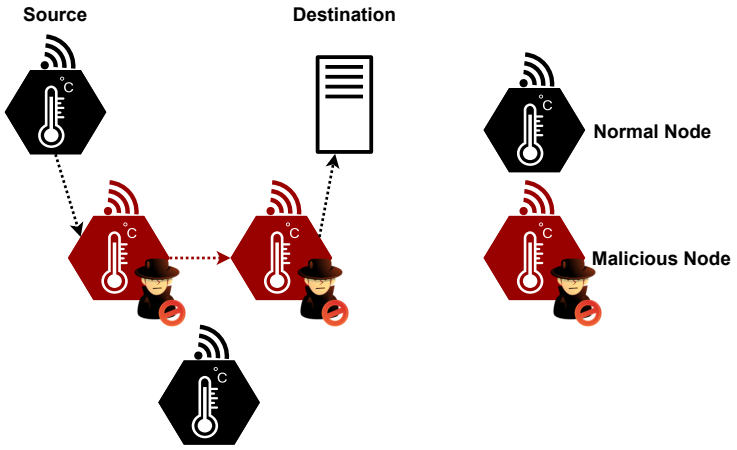
A wormhole is an out-of-band connection between two IoT devices, cf. Figure 3.7, using wired or wireless links. Wormholes can be used to forward packets faster than via typical paths. A wormhole can be used to forward critical messages where high throughput is fundamental, and the rest of the traffic follows the normal path. Although, a wormhole generated by an attacker and combined with other attacks, can lead to a serious security threat [82].

A classic wormhole attack requires two malicious devices in the network, that is, a sniffer and a jammer. End-devices in LoRaWan can be jammed by using off-the-shelf hardware [57]. Combining with replay attack, a wormhole attack [83] can be performed against the LoRaWAN network. In this kind of attack, one malicious device captures the packets from one device and sends them to another distantly located device to replay the captured packet. This can easily be initiated by malicious actors without previous knowledge of the network or cryptographic mechanism [3]. The sniffer device captures packets and signals to the jammer device, to notify that it captured the packet. The captured packet never reaches the gateway and the captured message stays valid. The captured message can be replayed at any time. As a result, critical alarm messages can be jammed, and regular messages that were previously captured and never reached the

gateway can be sent to the gateway, and be forward to the application layer [81]. Wormhole attacks can become a serious security breach and are very difficult to detect particularly when the wormhole is systematically switched on and off [82].



(**a**) Normal Network.



(**b**) Network with wormholes.

Figure 3.7: Wormhole attack example. Image adapted from [84].

Defense Strategies: A possible solution is to beat jammer response time. Moving to low SF to beat jammer response time. Reducing SF decreases the airtime of messages, which in turn reduces the time the jammer has to reach. This has several expenses, however: (1) Lower SFs have lower reliability and lower range, and (2) Lower SFs require less power output from the jammer to be disrupted. Drop packet size to beat jammer reaction time. Packet size has a significant impact on message air time. Reducing the size of these messages could permit messages to beat the jammer's reaction time [81].

A general mechanism, called packet leashes could be used for detecting and defending against wormhole attacks [3]. Any data appended to the packet for limiting its maximum

transmission distance is referred to as leash. These are designed to protect single wireless transmissions from wormholes. In this case, if the packets are transmitted over several hops, another new leash is required for each transmission [85]. A leash is any information that is added to a packet designed to limit the packet's maximum permitted transmission distance. There are two distinguish leashes, namely, geographical and temporal leashes. A geographical leash guarantees that the recipient of the packet is within a certain distance from the sender. A temporal leash guarantees that the packet has an upper bound on its lifetime, which restricts the maximum travel distance since the packet can travel at most at the speed of light. Each type of leash can prevent the wormhole attack since it allows the receiver of a packet to distinguish if the packet traveled further than the leash permits [83].

Denial of Service Attack

DoS is a popular cyber-attack in computer networks [86]. It consists on the deliberate interruption of network connectivity, making services inaccessible to applications and users. DoS attacks consist in flooding the specific target—a server or other computational entity—with superfluous requests, that prevent IoT devices from obtaining access to specific services [68], which are typically delivered by Software-oriented Architectures (SoA) or microservices architectures. When the attack is accomplished, the system's processing power gets compromised and is loaded with numerous spam requests that result in a system overload with a high likelihood of crashing. This attack can be achieved through distinct methods, being the most commonly known as botnets and buffer overflow attacks [87]. Although not so common, Distributed-Denial-of-Service (DDoS), cf. Figure 3.8, is considered as one of the most dangerous DoS attacks. In this type of attack, the malicious entities use thousands of Internet Protocol (IP) addresses to request IoT services, making it difficult for the server to distinguish legitimate DoS devices from attacks [88]. The most common victims of this type of attack are, typically, high-profile organizations such as banking and government, that rely on highly confidential information. DoS attacks can take a lot of time to resolve, result in high monetary losses, and, in the worst case, cause data loss for the organization [87].

Defense Strategies: This type of attack can be recognized with the use of signature-

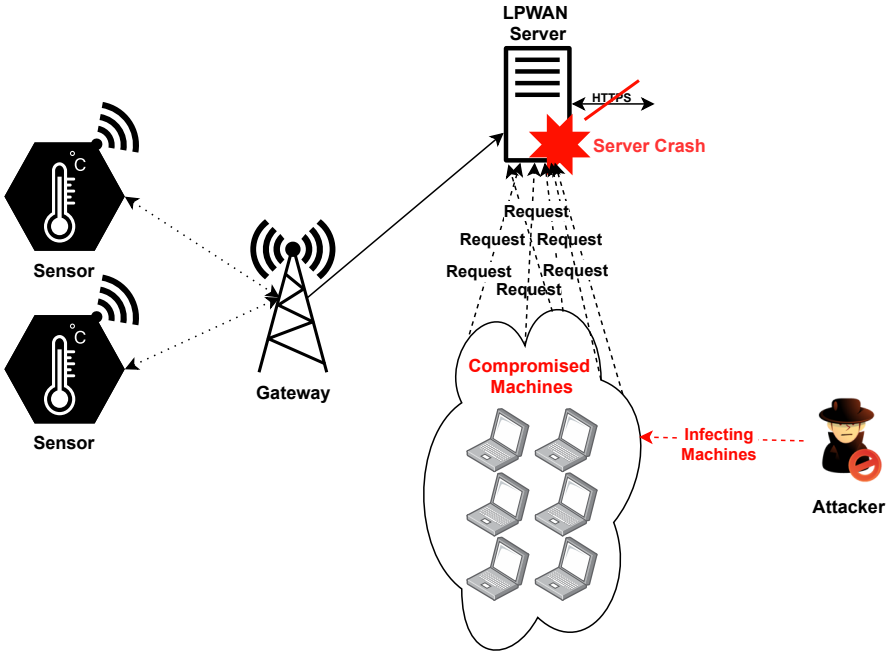


Figure 3.8: Distributed Denial of Service Attack.

based detection (known as rule-based or misuse-based Intrusion Detection System (IDS)). This technique consists of comparing known attack signatures—that is, patterns, malicious instruction sequences used by malware (such as specific byte sequences—with the monitored network traffic, where a match generates an alarm that signalizes a potential attack. The response is characterized by a fast detection time and high detection rate, and generally, has a low false-positive rate. Signature detection is based on well-known DoS attack patterns, which are frequently detected as protocol attacks and malformed packets.

Another technique is to use anomaly-based IDS (known as behavior-based detection). Operates by comparing the network traffic behavior against previous normal traffic. Any deviation in the comparison is an indication of an attack. The system acquires a normal traffic profile through training and monitoring the traffic against any differences with the normal profile. However, it generally produces higher false-positive rates than signature-based systems [89].

In [90] the proposed DDoS attack prevention mechanism uses a cloud-based Software-defined Networking (SDN) framework, and machine learning for attack detection. A semi-supervised machine learning algorithm is used for blacklisting malicious devices and filters the traffic using OpenFlow switches and an SDN controller.

Another solution is to use SDN-based honeypots. Honeypot is a computer security mechanism that is used to detect, deflect, or counteract attacks. It has positive effects in defending against DDoS attacks on the Internet [91]. The SDN controller is used to mimic IoT nodes in the network to attract the attackers. The SDN controller changes the address of the devices while mapping it to their original addresses, making it difficult for the attackers to find the active devices to attack [92]].

3.3 Attack Vector Analysis

The Internet of Things ecosystem is presented as an integrative model in which plenty of the objects around us are expected to be networked and connected to the Internet to arrange new types of services and increase its efficiency [93, 94]. This type of device can improve the execution of daily tasks, but the increasing connectivity and computational power of such devices result in a natural increase of related vulnerabilities (hardware, firmware, communications), which can be exploited and therefore increase the probability of being attacked. Additionally, some Internet of Things devices can be classified as security-critical and their malfunction can lead to irreversible harm to the physical system being controlled and to the users who depend on it [95]. The main activities stage of an IoT application includes data acquisition, data processing, data storage, and data transmission [31].

Generally, the IoT ecosystem includes a physical environment where the device is deployed to perform some specific function (i.e., operate as a sensor or actuator), which communicate through a LPWAN up to the cloud, where data is then pre-processed and aggregated for analytics on the business side of the network. However, there are several constraints and challenges associated with the design, development, and deployment of IoT applications, which include limited resources, interoperability, device heterogeneity, and security. Additionally, many companies tend to accelerate the development of their products, often leaving security behind [96]. This may cause several security issues in the IoT ecosystem, such as backdoors that are inadvertently created in the design and development stages.

Therefore, due to the pervasiveness of IoT technologies, its designers and developers

must reinforce security into applications and devices from scratch, rather than chasing the loss. Given this, it is crucial to have a specific and precise set of attack vectors to easily put forward a strategy to better respond to increasing threats that affect the overall IoT ecosystem. This approach will ensure that vulnerable points are identified in a general architecture and specific responses are used to prevent an attack or to mitigate its impact if it occurs. Thus, it is relevant to describe in detail all the attack vectors and provide, for each of them, a defense strategy. To systematize this environment, a set of attack vectors for LPWAN-based IoT applications is proposed in Figure 3.9, which includes three different communication networks, namely LPWAN, Backhaul Network, and Internet, of which, different types of malicious attacks can be put forward. In the attack vectors set, IoT devices are represented by a bicycle and a temperature sensor, that communicate using LPWAN technologies. These communications are carried out wirelessly to the LPWAN gateways, which are connected using a backhaul network with the LPWAN server. This architecture is common to those found in technologies like LoRaWAN [97, 98, 99, 100, 101, 102], Sigfox [103, 104, 105] and NB-IoT [65, 59, 106]. The gateways form the bridge between IoT devices and the LPWAN server through a backhaul network. In turn, the LPWAN server uses an internet connection (typically over HTTPS) to the Cloud/Analytics Services to process the data transmitted by the IoT devices. After processing, information is transmitted using an internet connection (typically over HTTPS) to client applications on the business side.

As described in Figure 3.9, a malicious agent, typically, can explore six different attack vectors, which may represent, the physical environment, infrastructure elements (such as gateways), communication networks and protocols, and network servers. Table 3.2 compiles and maps the attacks identified in Section 3.2.3 to the attack vectors depicted in Figure 3.9, respectively, with focus on the physical environment, where IoT devices are deployed, and in the LPWAN and backhaul networks.

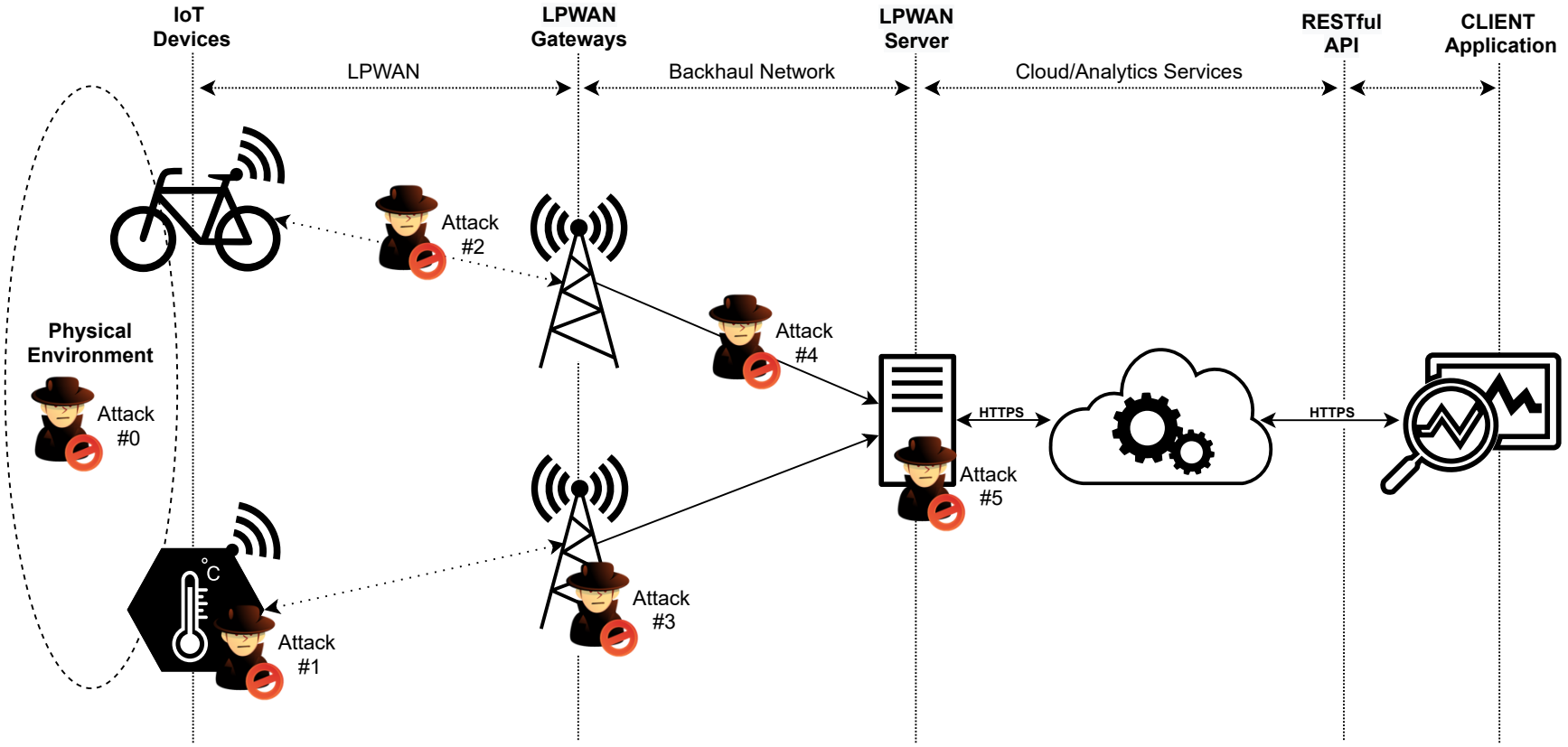


Figure 3.9: Definition of Attack Vectors in Low Power Wide Area Networks (LPWAN)-based Internet of Things (IoT) applications.

Table 3.2: Attack Vectors and their characterization according to Figure 3.9.

Attack Vector	Description	Attack	Attack Type (Table 3.1)	References
#0	An attack that forces a change in the physical environment. Can consist of physical environment manipulation to produce malicious sensor readings that may wrongly trigger a system malfunction.	Physical-related (Section 3.2.3)	Physical	[63, 65, 3, 57, 76]
#1	An attack that has compromised a sensor (or actuator). Can consist of the injection of false sensor signals, causing the control logic of the system to act on malicious data.	Wormhole (Section 3.2.3)	Software Physical	[63, 81, 82, 83, 85]
#2	An attack that has compromised the wireless communications between the IoT device and the gateway. Can consist of eavesdropping the connections secretly, between the target devices to collect information.	Jamming (Section 3.2.3)	Network	[3, 77, 65, 57, 81]
#3	An attack that has compromised the LPWAN gateway. Can consist of any kind of capture attack (Sniffing) or even physical attacks, this can block the communications between the devices and the rest of the network.	Physical-related (Section 3.2.3)	Physical	[63, 65, 3, 57, 76]
#4	An attack that has compromised the Backhaul communications between the gateway and the LPWAN server. Can consist of delaying the communications or, for instance, MitM (Man-in-the-Middle) attacks where the malicious agent could modify the communications transmitted.	Replay (Section 3.2.3)	Network	[3, 81, 63, 72, 70, 107, 76, 65]
#5	An attack that has compromised the LPWAN server. Can consist of multiple service requests (DoS), overwhelming the server resources and leading to server malfunction.	Bit Flipping (Section 3.2.3) Denial-of-Service (Section 3.2.3)	Software Data Privacy Network Encryption	[71, 72, 70, 73, 76, 92, 68, 86, 87, 88, 89, 90, 91]

3.4 Summary

In this chapter was observed the main differences between wireless communication technologies. Focusing on LPWAN-type networks, some relevant comparisons are made between them, in terms of energy consumption, as well as the range of communications. Some threats and vulnerabilities in this type of technology were presented, possible attacks that may arise and also some defense strategies. Finally, an attack vector model is presented, where the previously described attacks could fit. In the next chapter, the BIRA Bicycle application will be described, which uses the bicycles from the Instituto Politécnico de Viana do Castelo (IPVC) BIRA project, equipped with an IoT device that communicates its coordinates through the IPVC LoRaWAN network. The system architecture, security mechanisms and their vulnerabilities are presented, as well as possible attack vectors in this context.

Chapter 4

The BIRA Bicycle Application

The digital transformation is taking place in many areas and is also envisioned in educational institutions. The smart campus concept is intended to empower the universities to use next-generation technologies to enhance the campus experience in areas such as environment, governance, economy, social and mobility [9]. Within campuses, mobility-related data can be collected from persons and vehicles to infer mobility patterns that, when processed and analyzed, could predict future patterns, aid mobility management agents, and strengthen sustainability in academia. This occurs by engaging users with more sustainable practices, that typically begin inside the campus, and quickly reach the external public, given the synergistic relationship between the academia and the local community where it is located.

BIRA bicycle is an initiative of IPVC, which is a part of the national project U-bike Portugal [108]. It consists of a group of 200 bicycles, shared by all IPVC community (students and staff), in which, 160 are electrical and 40 are conventional bicycles. The main objective of this project is to promote smooth mobility, encourage the adoption of more sustainable mobility habits in higher education scenarios. It is focused on the young sections of the population and by the extent to all academic communities, promoting the transportation shift, from the car to a healthier and environmentally friendly bicycle.

By implementing certain technologies, a smart system must be able to recognize and protect the system from malicious attackers. Attackers can intercept the communication network or physically harm the devices. As a result, false data exchanges or even device tampering could affect the functionality of the system.

In this chapter, was proposed a secure IoT and LoRa-based tracking system for the BIRA bicycle. The system consists of BIRA bicycles equipped with low cost Global Positioning (GPS) trackers. Data collected is then transmitted using a LoRaWAN infrastructure — which guarantees coverage at a city/regional level — to the application server, which is responsible for storing and serving the client application with several relevant parameters, such as location, route, speed, and battery level. The BIRA client application tracks the bicycles in real time and can be used for historic/route analysis. Furthermore, the client application will allow to obtain the most used routes, and prevent bicycles from being stolen. By knowing their position in real-time, virtual fencing techniques can also be applied, which can, on the server-side, generate alerts for the BIRA bicycle managers.

Promoting more sustainable mobility practices also implies the adoption of privacy and security principles, from the initial design stage to the end of the product life cycle. In this sense, the main security mechanisms of the proposed architecture are presented in detail — for this specific application case — and its main vulnerabilities are identified and briefly described.

4.1 System Architecture

Figure 4.1 depicts the overall architecture of the BIRA bicycle client application. Each bicycle is assigned to a specific IPVC community member and has a GPS device attached, that tracks several context information parameters such as location, route, speed, and battery level, communicating over the IPVC LoRaWAN network.

To view the collected data, a front-end application, displaying a geographic information system map with the last known location of the bicycle, after the user authentication, is displayed, allowing the visualization of historic data by displaying multiple points (routes) on the map according to the selected data range picker. The BIRA application is divided into four main component blocks [27]:

1. IoT and Communication: includes the BIRA U-Bikes and LoRaWAN communication protocols;

2. FIWARE App Server: application server that handles all the data coming from the IoT devices throughout a Orion context broker;

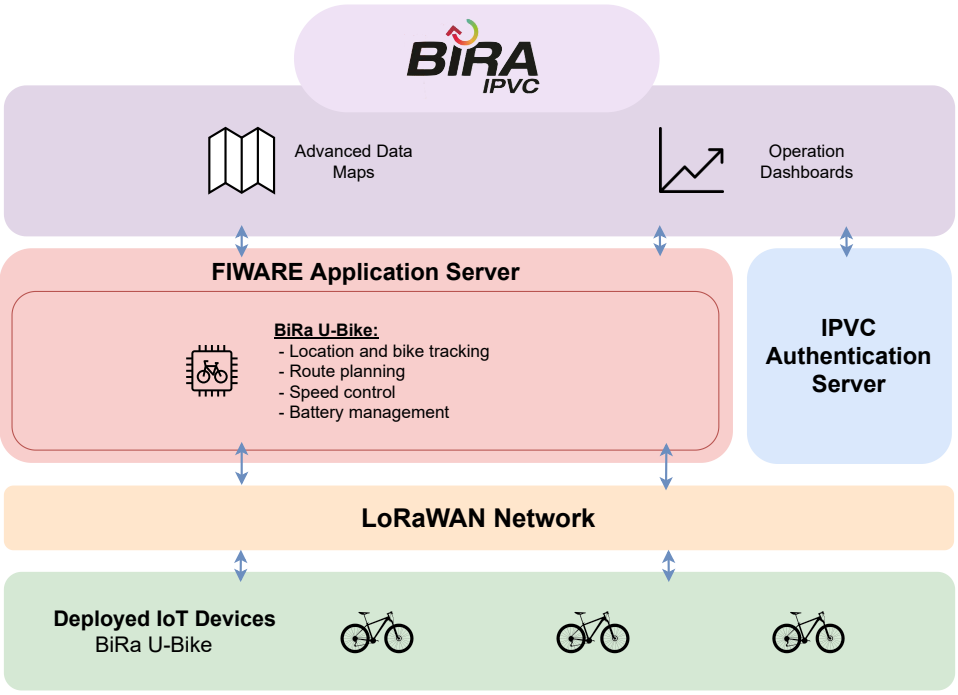


Figure 4.1: IPVC BIRA Bicycle Architecture. Image from [27].

3. IPVC Authentication Server: includes the IPVC authentication databases and external services;

4. Web Application: includes the front-end application and its features, which are available to the end-user.

The usage of the IPVC Smart & Sustainable Campus (IPVC S2C) platform is essential since it allows a product-ready application that standardizes the adoption of a common interface for IoT and Big Data analytics, allowing better management of the usage and maintenance of the BIRA bicycles [109].

4.1.1 LoRaWAN Connectivity

Each bicycle is equipped with a low cost GPS tracking system with LoRaWAN connectivity. LoRaWAN is a LPWAN protocol that supports low-cost and secure bidirectional communications for Cyber-Physical Systems and the IoT. As the area of interest for tracking the BIRA bicycle spreads over a large urban area, which includes the center and surroundings of Viana do Castelo, a city in Northern Portugal. Connectivity between the IoT devices (bicycles) and the network server (LoRaWAN server) is guaranteed by the

IPVC LoRaWAN communication infrastructure, whose coverage can be seen in Figure 4.2.

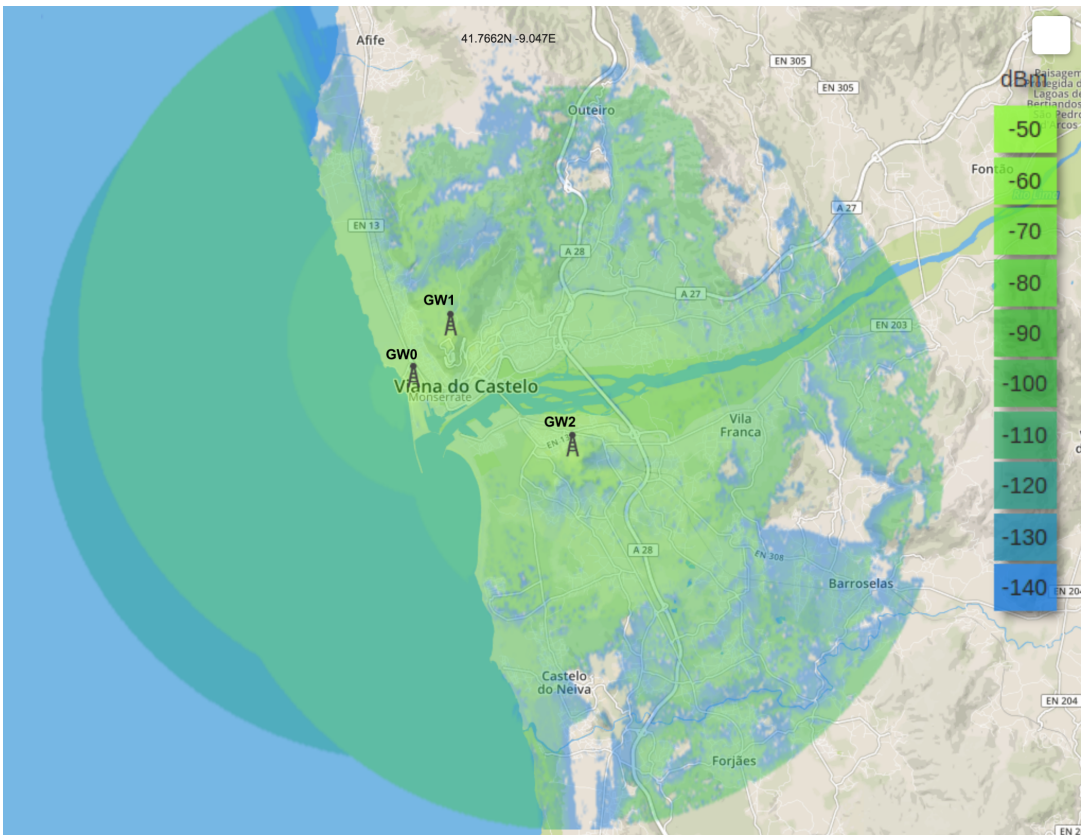


Figure 4.2: LoRaWAN estimated coverage in Viana do Castelo. Image from [101]

4.1.2 IoT-enabled BIRA Bicycle

This section is divided into two different parts: Firstly, the LoRa-based GPS Tracker (Section 4.1.2) presents an overall description of the device used in the proof-of-concept, describing all the components equipped as well as the autonomy of the battery. Secondly, the Firmware Development (Section 4.1.2) describes all the code programmed for the device, as well as a flowchart describing the principal functions of the firmware.

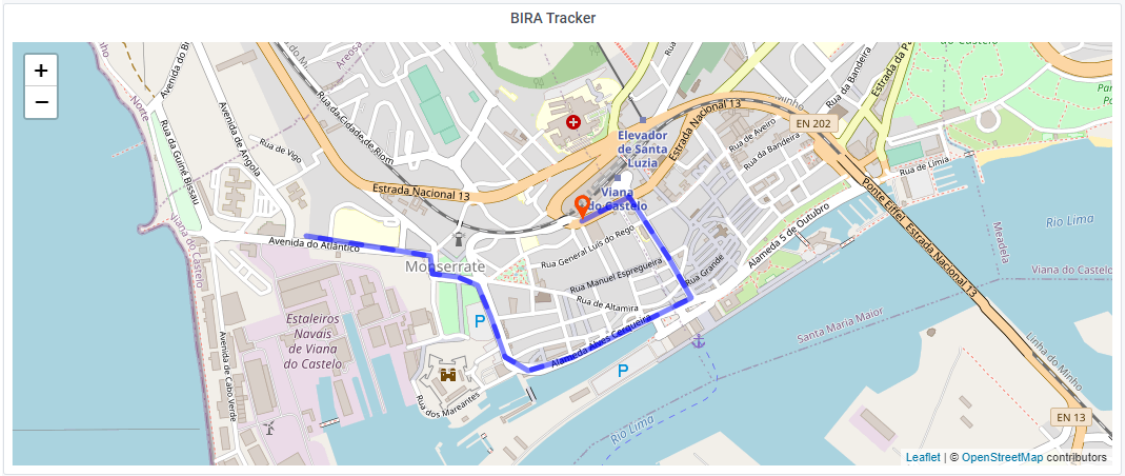
LoRa-based GPS Tracker

The proof-of-concept was implemented using the low-cost TTGO T-Beam dev board, as presented in Figure 4.3b, which presents an average cost of 20€. The TTGO T-Beam dev board is equipped with an Espressif ESP32 chip, which provides built-in Wi-Fi and Bluetooth Low Energy (using a 3D antenna), and has an onboard flash with 4 MB. LoRa connectivity is supported by an SX1276 chip (which can operate at 433MHz, 868MHz,

or 915MHz), and an SMA antenna. Position tracking is provided by an onboard U-Blox NEO-6M GPS module that is equipped with an external ceramic antenna. The board has in the bottom a Li-Ion TR 18650 3.7V battery cell with a capacity of 9900 mAh, that can be charged through the available micro-USB port. With this type of battery used in the proof-of-concept, the device presents an average consumption of 131 mA, reaching 75 hours of autonomy. The dev board comes with 26-pin external headers pins with GPIO, ADC, VPVN, DAC, touch, SPI, I2C, UART, and has both 5V and 3.3V power signals, which are of great value for implementing additional features.

(a) BIRA Bicycle.

(b) LoRa-based tracker detail.



(c) Application front end with trajectory example.

Figure 4.3: BIRA bicycle with LoRa-based tracking device installed and application frontend.

Firmware Development

Figure 4.4 depicts the embedded firmware flowcharts. The method of device activation chosen was the OTAA method. According to The Things Network (TTN) [110] and LoRa Alliance [111], OTAA is the preferred method to join any LoRaWAN network because it offers more security, flexibility and scalability when compared with ABP method. OTAA method is more reliable because the activation will be confirmed, and more secure due to the negotiation of the session keys with every activation.

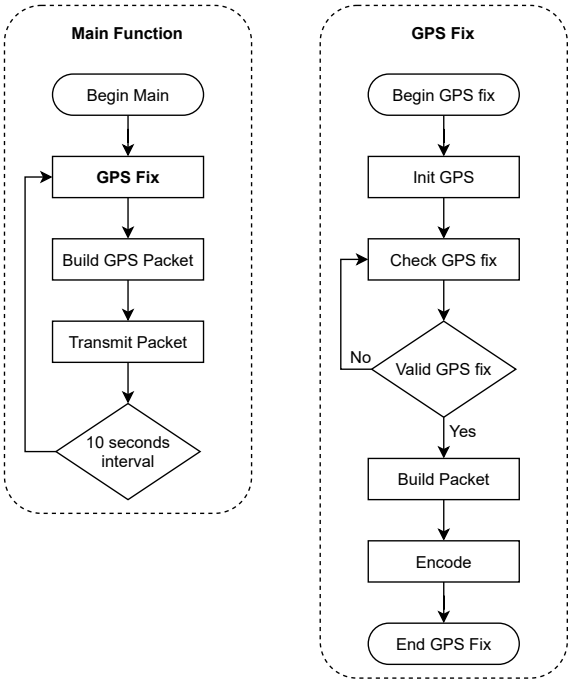


Figure 4.4: Embedded firmware flowcharts.

The device perform a join-procedure with the network, in which a dynamic Device Address (DevAddr) is assigned.

The application starts with a GPS fix and repeats the process until it obtains the device's coordinates. After obtaining the coordinates, creates a packet (array), with the GPS data into bits. Finally, sends this payload to the gateway. On the LoRa server-side, a Decode function is used to do the reverse operation done in the application, decoding the bit values back into floats. After this Decode operation, it is possible to visualize the data in decimal degrees, e.g. lat: 41.6947979, lng: 8.8471761. The process of the coordinate's communication occurs every 10 seconds. Note that the device only communicates with the gateway after being able to get the GPS coordinates, while this operation is not achieved,

the device does not perform any type of communication.

4.1.3 BIRA Bicycle Client Application

The BIRA client application focus on mapping the BIRA bicycles in real-time, as well to obtain some additional information, such as routes historic, and other relevant metrics, e.g. average km/day, velocity, etc. With that, it is possible to get information about the most used routes and prevent bicycle theft, by knowing its real-time position and by taking advantage of geofencing strategies, which can provide security by using predefined virtual borders, that when violated, can be used to trigger alerts to the bike-sharing application manager.

The BIRA bicycle client application, cf. Figure 4.3c, is instantiated in the IPVC S2C platform, an application based on a layered architecture that consumes multiple built-in micro-services that are ready-to-use, to ease and simplify the development of IoT applications, from the start to the end. As depicted in Figure 4.1, the application is divided into three different layers. The top layer is composed of components for the user interface, mostly based on GIS-based maps and dashboards with data from the BIRA tracking device. In the middle layer, several micro-services from the FIWARE application server are consumed to manage data. Lastly, the bottom layer is presented by the tracking devices installed in multiple bikes around the IPVC community. An asynchronous notification mechanism is also used, allowing subscriptions to changes of context information, enabling the user to know when a certain condition occurs, thus, removing the permanent poll and the repetition of query mechanisms, implying a lower usage of computational resources, resulting in a faster response time. Since the application is based on the IPVC S2C, it allows an easier and faster approach and integration of the final application, removing several layers of development, from the back end to the data management.

4.2 Security Mechanisms

Figure 4.5 depicts the overall architecture with all the functional elements identified, the bicycles, the LoRaWAN Gateways, the LoRaWAN Server, the Application Server, and the Client Application. This section was focused on the LoRaWAN security mechanisms,

in the first place, its security properties will be identified and briefly described, and secondly, the LoRaWAN packet protection mechanism is introduced and detailed. Lastly, an overview of the LoRaWAN end-to-end security is put forward.

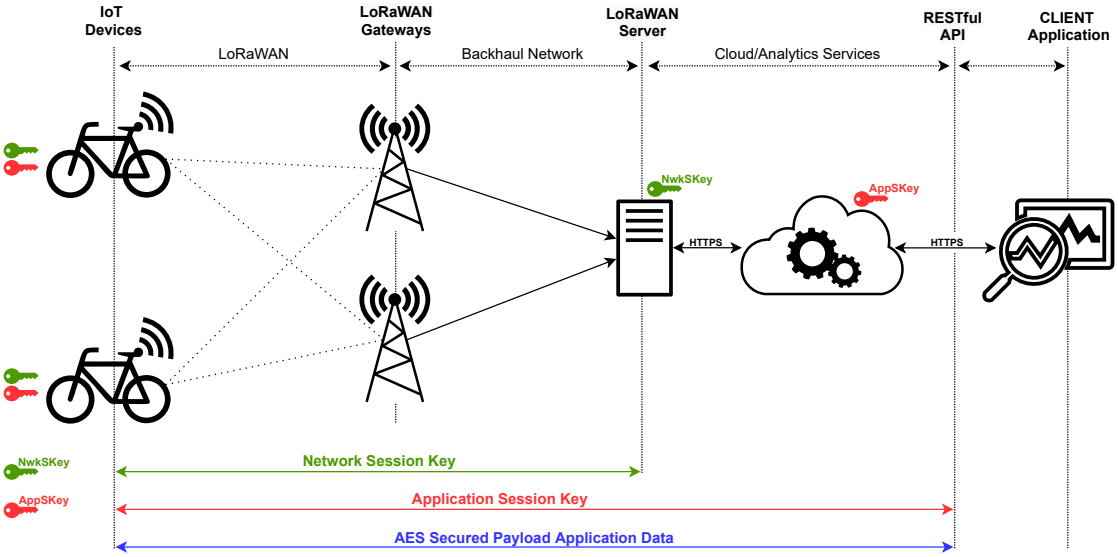


Figure 4.5: BIRA Bicycle Secure Tracking System.

4.2.1 LoRaWAN Security Properties

LoRaWAN technology has three fundamental security properties that enhance its usage in several IoT application domains:

Mutual Authentication

This type of authentication is established between a LoRaWAN end-device and the LoRaWAN network as part of the network join procedure. This ensures that only genuine and authorized devices will be joined to genuine and authentic networks. The join procedure in OTAA is possible after both, the end device and the network, make proof of having the Application Key (AppKey). This proof is made by computing an AES-CMAC4 (using the AppKey) by both the device that is joining the network and the backend receiver. Two session keys are then derived, cf. Figure 4.1, one for providing integrity protection and encryption of the LoRaWAN MAC commands and application payload (green Network Session Key (NwkSKey)), and the other for end-to-end encryption of application payload (red Application Session Key (AppSKey)). With the NwkSKey, LoRaWAN network can

prove/verify the authenticity and integrity of the packet. The AppSKey is distributed to the application server to encrypt/decrypt the application payload. AppKey and AppSKey can be hidden from the network operator so that it is not able to decrypt the application payloads.

Integrity Protection

The integrity protection mechanism is provided in two steps, the first is when the packet is over the air being the integrity protection provided by the LoRaWAN protocol and the other step is between the LoRaWAN network and the application server, which uses transport solutions such as HTTPS and VPNs. Note that, LoRaWAN MAC and application messaging are authenticated at the origin, integrity protected, replay protected, and encrypted. This protection, combined with mutual authentication, ensures that the network traffic has not been altered, is coming from a legitimate device, is not comprehensible to eavesdroppers, and has not been captured and replayed by external actors.

Confidentiality

All LoRaWAN traffic is protected using the two session keys. Each payload is encrypted by AES-CTR and carries a frame counter (to avoid packet replay) and a MIC computed with AES-CMAC (to avoid packet tampering).

4.2.2 LoRaWAN Packet Protection Mechanisms

Next is presented an example of a LoRaWAN packet (structured in JSON format) received at the LoRaWAN Network Server. Figure 4.6 presents the payload in red color, which is decrypted and encoded in Base64, and, in green color, the DevAddr and the Frame/Header Counter (FCNT).

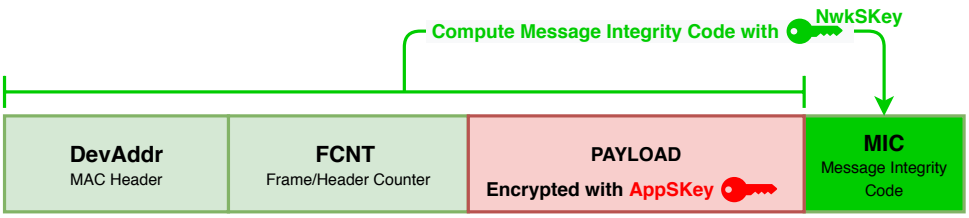


Figure 4.6: LoRaWAN packet protection mechanism.

Due to this protection mechanism, it is impossible to read these messages without the AppSKey, due to AES encryption. Moreover, it is not possible to tamper LoRaWAN messages without the NwkSKey, because it will make the MIC check fail. However, it is possible to re-transmit the messages, which can result in the so-called replay attacks, that can still be detected and blocked — at the application layer — using FCNTs. Next, an example of a LoRaWAN uplink packet (LoRa server-side) is depicted.


```
{
"type": "uplink",
 "payload": {
  "adr": true,
  "applicationID": "6",
  "applicationName": "BIRA",
  "data":"bGF0OjQxLjY5NDc5NzksbG9uOi04Ljg0NzE3NjE=",
  "devEUI": "88138f386f4e6be4",
  "deviceName": "BIRA001",
  "fCnt": 11844,
  "fPort": 1,
  "rxInfo": [{
    "gatewayID": "b827ebfffee8ec4a",
    "loRaSNR": -4.8,
    "location": {
      "altitude": 0,
      "latitude": 41.6947979,
      "longitude": -8.8471761 },
    "name": "GW_ESTG_b827ebfffee8ec4a",
    "rssi": -119 }],
  "txInfo": {
    "dr": 5,
    "frequency": 868500000 }
  }
}
```


Listing 4.1: Example of LoRaWAN Uplink Frame in JSON Format.

After the device activation, the frame counters (uplink and downlink FCNTs) are both reset to zero. For each new uplink message transmitted by a LoRaWAN device, the uplink FCNT increments, and for every new downlink message sent by the network server, the downlink FCNT is incremented. Whenever the device or the network receives a message with an FCNT value that is lower than the last one, the message can be discarded by the application layer.

When using ABP activation, which relies on the static definition of AppSKey and NwkSKey, this security mechanism can be a problem, since these FCNT reset to zero every time the device restarts. As a result, the application layer can block all messages that are arriving from the device until the uplink FCNT reaches a value higher than the one stored in the network server. Therefore, the device should be re-registered in the application server every time it restarts.

4.3 Vulnerabilities and Attack Vectors

In this application context, different types of vulnerabilities are present that can cause warm not only to IoT equipment, but also to the functioning of the application. Free access to the bicycle's IoT device is one of the main threats presented. If the equipment case is not physically secure, anyone can tamper the LoRa antenna or the GPS antenna, perform a device reset, turn off the device or even break it. Another type of threat could be the so-called Replay Attack, which is based on capturing and retransmitting packets emitted by the device, impersonating a trusted device on the network. As the main function of the hardware installed on bicycles is to transmit its location, it is possible to perform a GPS Spoof in order to transmit fake GPS coordinates close to the device, making it receive this stronger GPS signal thinking that it is a reliable satellite. Finally, and not expendable, is the DoS/Jamming Attack that are present in all wireless communication technologies. In case it is used hardware capable of transmitting high radio signals, this may cause the IoT device to be unable to communicate with the LoRa gateway due to the high noise present in its periphery, thus causing an interruption in the application communications. All the described vulnerabilities are related to the attack vectors presented in the previous chapter. With that, it can be verified that these possible attacks are mapped in the attack

vectors model defined above, and can be exploited by someone with bad intentions.

4.4 Summary

The BIRA Bicycle Application is an application based on the presentation of paths and coordinates during the usage of IPVC BIRA bicycles. This application relies on a web page where the user can consult the trajectories made in a defined time space. It is also composed by an IoT device installed on the bicycles, which communicates its GPS position via the LoRaWAN network. After presenting the entire architecture and security mechanisms, it can be verified some existing points that could constitute serious threats to the application functionality, from which some type of attacks may eventually arise. In the next chapter, a proof of concept is made where the attack vectors referred in this application context are explored. Six different potential attacks that may be present in this application are defined and executed, and the results and analysis of this entire process are presented.

Chapter 5

Exploring the Attack Vectors

The previous attack vector analysis (Section 3.3), resulted in some possible vectors that could be exploring by someone with bad intentions. Meshing these results with the BIRA Bicycle context lead to a proof of concept where these attack vectors are explored. This chapter is organized by the description of the proof of concept, with all the devices, hardware and software described. Furthermore, all the experiences and attacks performed are reported step by step.

5.1 Experimental Setup

To begin the experimental setup, cf. Figure 5.1, it was necessary to establish a set of tools to make possible the exploitation of the attack vectors mentioned before. These tools are divided in software and hardware. The objective of the tests was to develop an environment that mirrored as much as possible a real life environment. The TTGO LoRa device was used, which communicates through LoRa networks and contains a GPS module. To program this IoT device in order to achieve some type of interactions with the LoRa Gateway and with the LoRaWAN server, the Arduino IDE software was used. To implement the attacks, a virtual machine with the Ubuntu 20.4 LTS operating system was used. In this virtual environment the GNU Radio software was installed. This software is a free development toolkit that provides signal processing blocks for deploying software-defined radios and signal-processing systems [18]. It can also be used with external Radio Frequency (RF) hardware. In this case it was used with the HackRF One. This Software

Defined Radio peripheral, by Great Scott Gadgets corporation, is characterized by transmitting and receiving radio signals from 1MHz to 6GHz. It is an open source hardware platform that can be used as a USB peripheral [112].

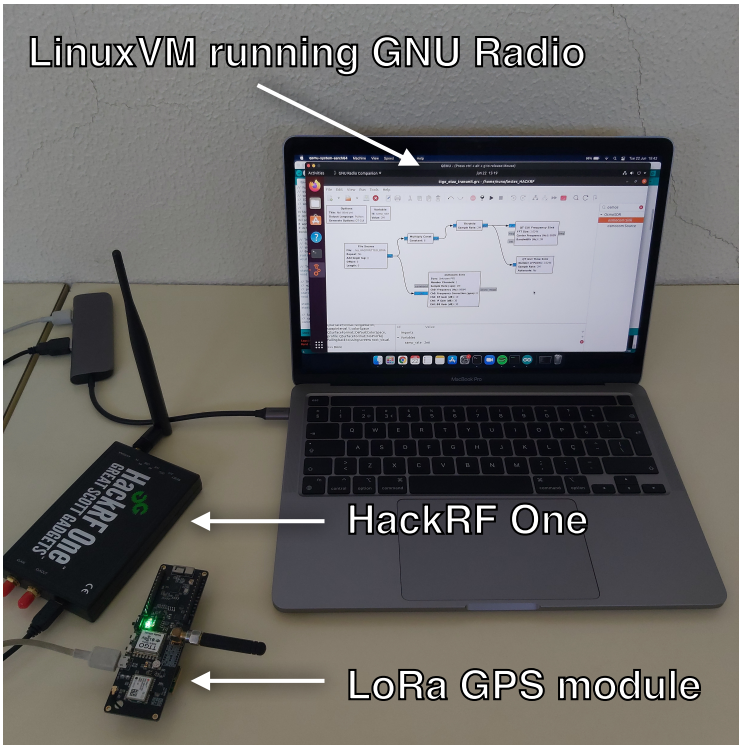


Figure 5.1: Experimental setup.

5.2 Implementation

All the experiences were made in a controlled environment, without causing any trouble or malfunction to the existent infrastructure. The implemented attacks were chosen according to the previously study that resulted in different attack vectors, cf. Figure 3.9. Among these represented, the vectors that best fit into the context of the IPVC LoRaWAN network were the following:

- **A - GPS Spoofing (Attack Vector #0)**, the main objective of this attack is to trick the device with false GPS coordinates, previously chosen and transmitted. The final goal is to send the payload with the coordinates to LoRa Server as if they were the real position of the device.
- **B - Physical Access (Attack Vector #3)**, this type of attack is the easiest one

because it does not need any type of specific knowledge, since everyone can tamper a device, for instance, by simply disconnecting an antenna. In this context, it is even more dangerous because the room where the LoRa gateway is installed has the door open for everyone inside the IPVC.

- **C - Replay Attack between devices (Attack Vector #4)**, this attack relies on the capture of a legitimate signal from a sender device while communicating with another receiver device. After that, the captured signal was replayed with another type of hardware in order to mislead the receiver device. For the receiver device, the re-transmitted signal will look like a legitimate signal from a trusty sender device.

- **D - Replay Attack (ABP) (Attack Vector #4)**, the goal of this attack is to capture a legitimate signal from a device and then replay it with another type of hardware in order to mislead the LoRa gateway and server. For the LoRaWAN network, the re-transmitted signal will look like a legitimate signal from a trusty device. In this attack the ABP method was used.

- **E - Replay Attack (OTAA) (Attack Vector #4)**, it is the same kind of attack that the previous one, the only thing that changes between them is the activation mode. In this case, the OTAA method was used.

- **F - Denial-of-Service and Jamming (Attack Vector #5, #2)**, the main objective of this attack is to generate a high noise source near a legitimate device, making it unable to communicate with the LoRa gateway due to noise. By succeeding with this attack, the device is also prevented from communicating with the LoRaWAN network, so it can be called a "double attack" (DoS and Jamming).

5.2.1 A - GPS Spoofing

GPS spoofing occurs when a radio transmitter is used, in this case the SDR HackRF One, to send fake GPS signals to the receiver antenna to counter legitimate GPS satellite signals [113], cf. Figure 5.2. Most navigation systems are designed to use the strongest GPS signal that can be received, and with that, false stronger GPS signals could override weaker but legitimate satellite signals.

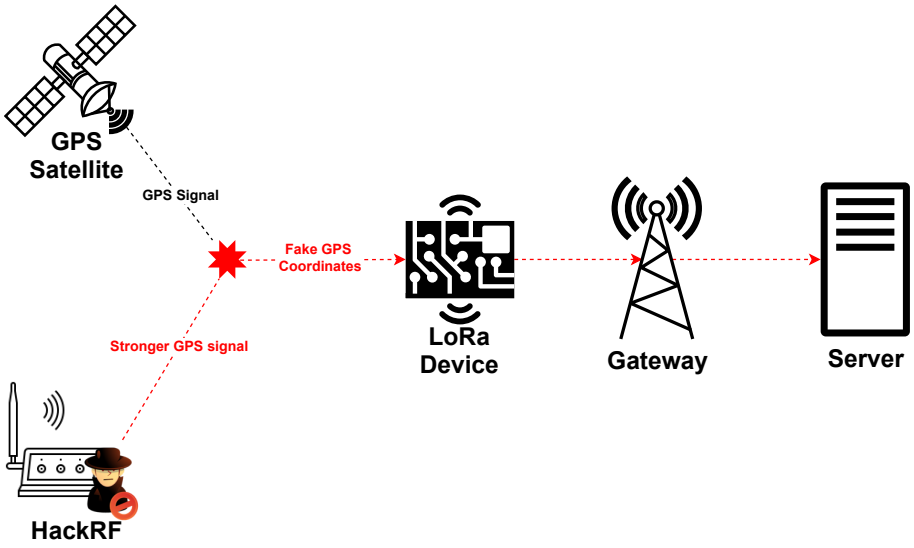


Figure 5.2: Implemented GPS Spoofing Attack.

To execute a GPS Spoofing Attack, it was necessary to generate GPS baseband signal data streams, which could be converted to RF using SDR platforms, such as HackRF. To create the broadcast file it was required to access the daily GPS broadcast ephemeris file (brdc) [114], that is a merge of the individual site navigation files into one. These files are then used to generate the simulated pseudorange and doppler for the GPS satellites in view. After that, this simulated data range is used to generate the digitized I/Q samples for the GPS signal.

The GPS-SDR-SIM application was used in command line, cf. Figure 5.3 to generate a GPS-SIM bin file, with some predefined GPS coordinates from another city. After that, another application called hackrf_transfer was used in command line as well, cf. Figure Figure 5.3 to transmit the gpssim.bin file generated, as a RF signal from the HackRF. The real position of the device attacked was in Viana do Castelo and after the GPS Spoof, the position changed to another location near the city of Porto in Portugal, cf. Figure 5.4, that were the coordinates chosen to generate the gpssim.bin bin file transmitted.

Figure 5.3: Commands used to generate and transmit gpssim.bin (Fake GPS coordinates) file.

(a) (b)

Figure 5.4: Device UPLINK to LoRa Server before and after GPS Spoofing. a) Real coordinates; b) Spoofed coordinates.

5.2.2 B - Physical Access

When someone has free physical access to an IoT device or a gateway, without strong hardware security policies, the whole devices or even the network may be assumed as compromised. The gateway in LoRaWAN is a single failure point for the network, and it

could be manipulated to disconnect hundreds of end-devices [57].

The room where the LoRa Gateway is installed at IPVC was open for everyone as depicted in Figure 5.5. Any person with malicious intentions can easily tamper the Gateway without any evidences. Just by unplugging the network cable, the LoRa connection in the IPVC becomes compromised. Another kind of action can be to turn off the electricity from the room that feeds the LoRa Gateway, just by pressing the circuit breaker switch from the electrical panel.

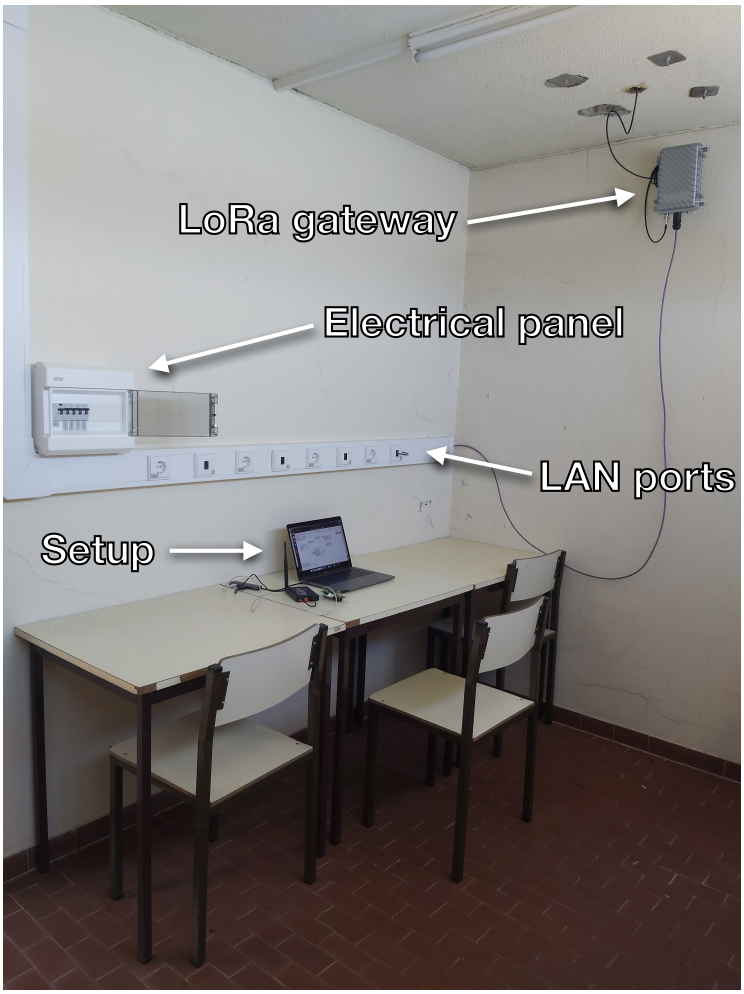
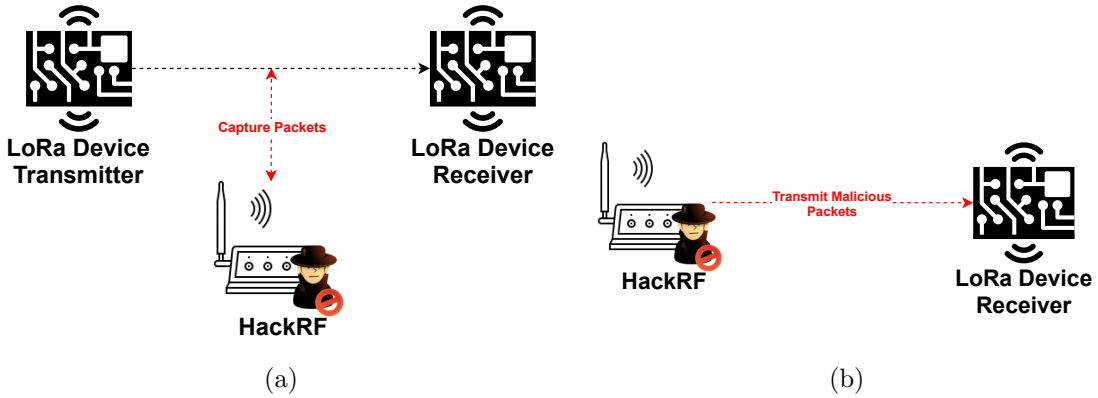


Figure 5.5: LoRa Gateway room.

5.2.3 C - Replay Attack between devices

The replay attack is typically characterized by re-sending or repeating legitimate data transmission by someone with bad intentions. The goal of this attack is tricking the device or module by utilizing handshake messages or old data from the network.

To perform this attack in wireless networks, as depicted in Figure 5.6, the communication frequencies and channels to sniff were previously identified, due to LoRaWAN specifications. Two devices were used and configured in order to communicate between each other. One device, as a sender and the other, as a receiver. The first device (sender) contained a simple code to send LoRa packets, while the second (receiver) had a function to receive the LoRa packets sent by devices. In this case, the LoRa packets only communicated between devices, and not through the LoRa Gateway.



(a) (b)

Figure 5.6: Implemented Replay Attack. a) Capturing packets (packet sniffing); b) Replaying the malicious packets.

The first step to perform this attack was to start the transmitting device, and by using HackRF, its packets were captured, cf. Figure 5.7, as shown in Figure 5.6a, and saved into a file using GNU Radio. Secondly, a flowgraph was configured in GNU Radio, cf. Figure 5.8, which had as transmission source the file with the LoRa packages captured previously. After starting the transmission with the HackRF, cf. Figure 5.6b, the receiver device was switched on and it was verified that it received the malicious LoRa packets, cf. Figure 5.9, thinking that the transmitter was the authentic sender device.

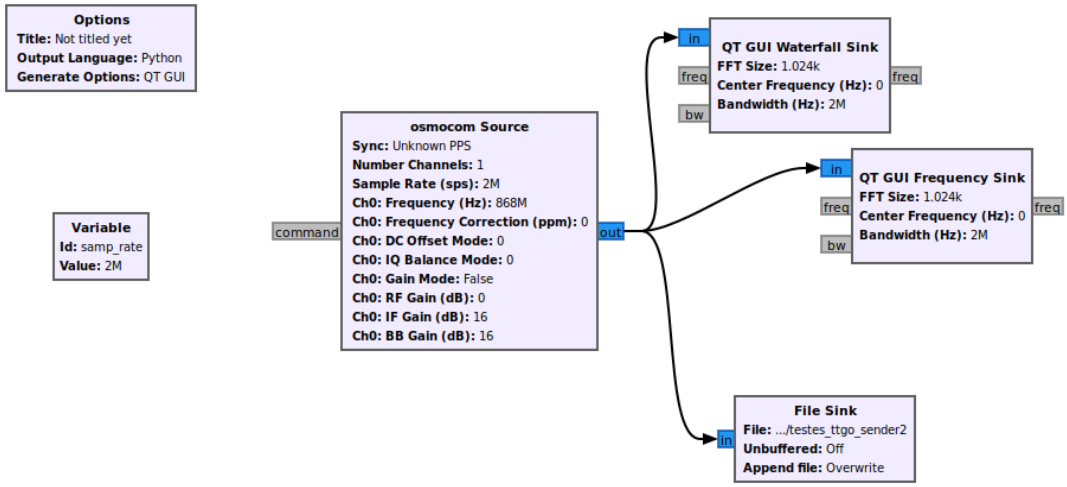


Figure 5.7: GNU Radio flowgraph for LoRaWAN packet capture.

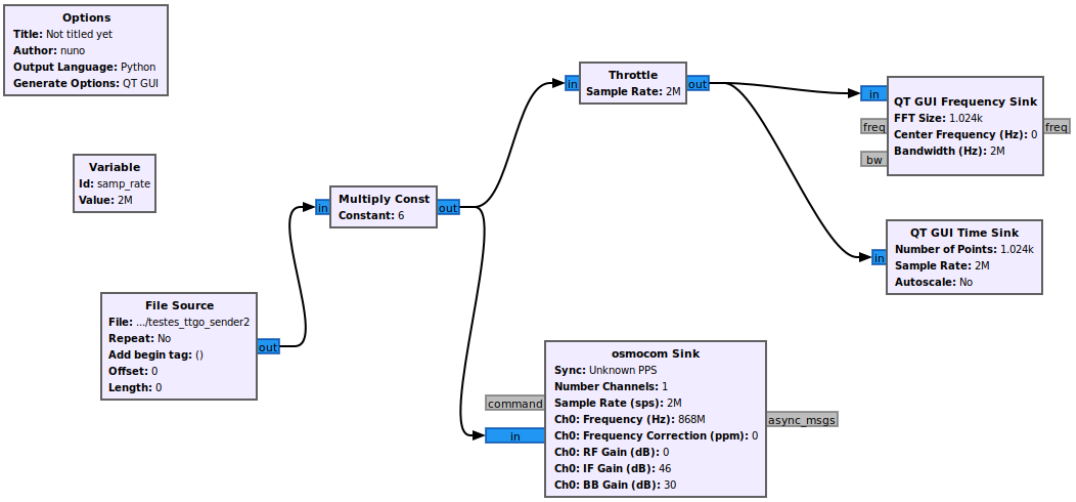


Figure 5.8: GNU Radio flowgraph for the Replay Attack implementation.

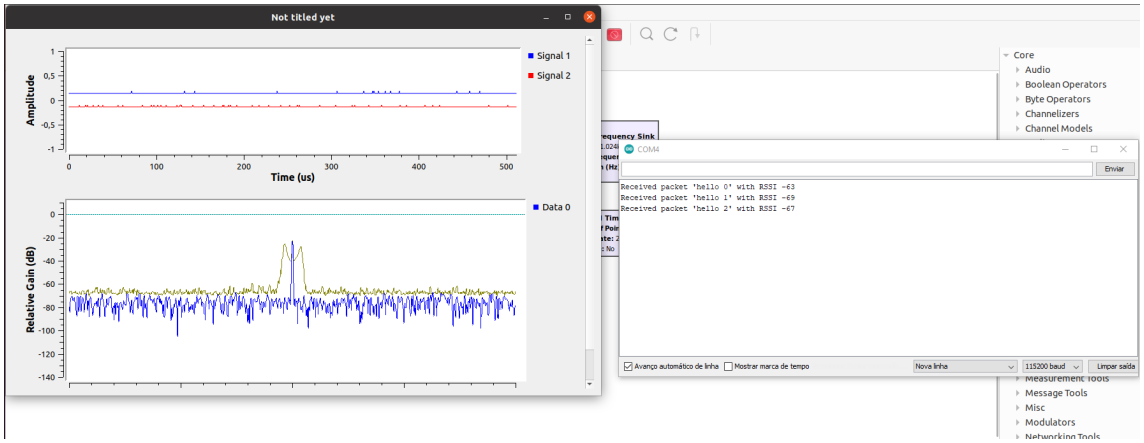
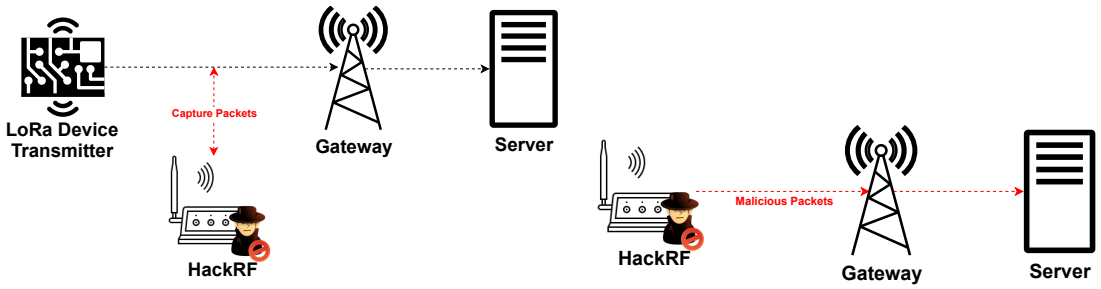


Figure 5.9: Time and frequency plots obtained while replaying the packets previously captured and the serial monitor of the attacked device showing its successful reception.

5.2.4 D - Replay Attack in ABP

This type of attack is very similar to the previous attack described above which refers to replay attacks. The entire process performed before was replicated, cf. Figure 5.11, but in this case the packets instead of being transferred between two devices, they were send through the LoRa Gateway and could be displayed on the LoRa Server, cf. Figure 5.10.



(a) (b)

Figure 5.10: Implemented Replay Attack in ABP mode. a) Capturing packets (packet sniffing); b) Replaying the malicious packets.

As depicted in Figure 5.10a, the first packets sent by the device after a reset, were captured by the HackRF. In this case, the device communicates via the ABP method. In this type of activation, when a device performs a reset, the FCNT are also reset and start a new counting again from 0 value. As the frames with FCNT=0 were captured, it is always possible to perform this type of attack, because the LoRa Gateway thinks the device was reset, and always accepts these frames that were captured and then transmitted by HackRF. After that, as depicted in Figure 5.12, the LoRa Server associates the malicious UPLINKS to the device that was attacked.

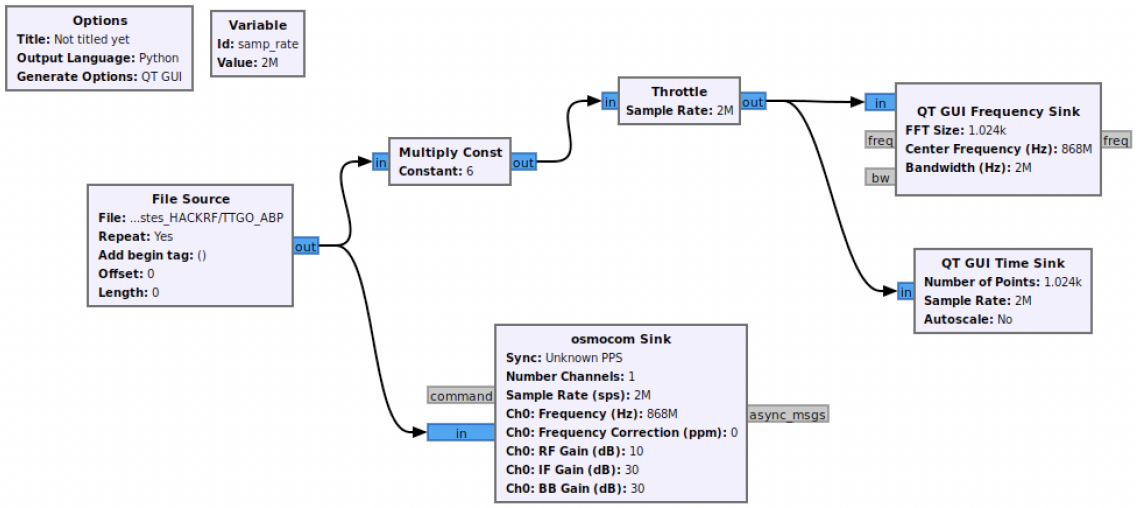


Figure 5.11: GNU Radio flowgraph for the Replay Attack in ABP.

DOWNLINK	3:46:53 PM	UnconfirmedDataDown	0149a976
UPLINK	3:46:53 PM	UnconfirmedDataUp	0149a976
DOWNLINK	3:46:48 PM	JoinAccept	
UPLINK	3:46:48 PM	JoinRequest	0000000000000044

Figure 5.12: Log of the malicious device in the LoRa server, icluding a malicious network join and data transmission.

5.2.5 E - Replay Attack in OTAA

To test this type of attack using OTAA method, is not as simple as the ABP, due to the fact that it is mandatory that the devices perform a join-procedure with the network, in which a dynamic DevAddr is assigned and security keys are exchanged with the device. Anytime the device is reset, new keys are generated and the previous captured frames cannot be replayed. With the FCNT it is not possible to replay messages, because the LoRa Server will not accept packets with the same FCNT or lower than the previous received.

5.2.6 F - Denial-of-Service and Jamming

DoS Attack consists on the deliberate interruption of network connectivity, making services inaccessible to applications and users. It is known for flooding the specific target with superfluous requests, cf. Fig 5.13, that prevent IoT devices from obtaining access to

specific services [68].

In other hand, when performing jamming attacks it is not necessary to have complex hardware, as long as it could transmit powerful radio signals near the application devices. This type of attack will cause the interruption of the communications between the devices and the network server, because LoRa transmissions at the same frequency and spreading factor can interfere with each other [58]. LoRaWAN bandwidth is small (125/250/500kHz) and relies on low-power for data transmission [65].

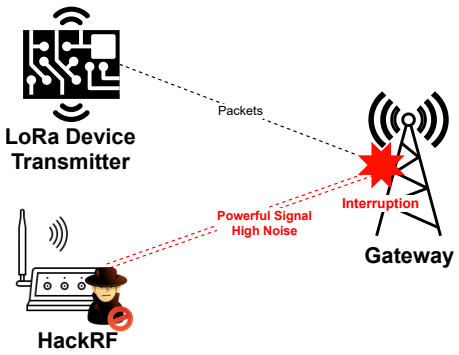


Figure 5.13: Implemented DoS/Jamming Attack.

So, by reaching Jamming it can also be achieved the DoS attack, in which the target cannot communicate while being under attack, cf. Figure 5.13. For the configuration the GNU Radio was used with a noise source, cf. Figure 5.14. The HackRF was placed near the targeted device, and the noise transmission was started. After some seconds, the device was unable to communicate with the LoRa Gateway.

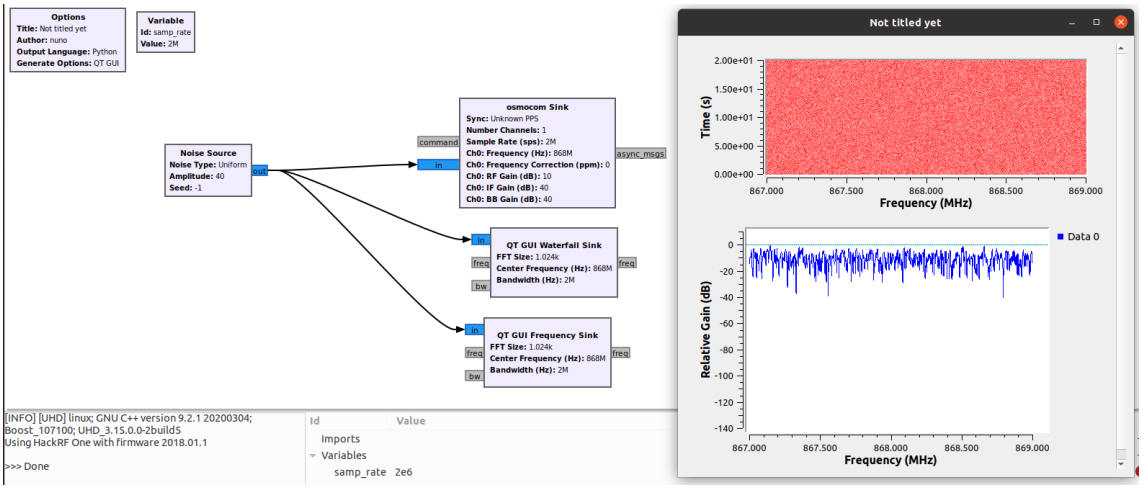


Figure 5.14: Flowgraph of the implemented Jamming Attack. Time and frequency plots obtained while jamming.

5.3 Results and Analysis

In this section the overall results achieved are presented. Table 5.1 illustrates all the attack vectors that have been implemented in this chapter.

ID	Description	Attack Vector	Results	Comment
A	GPS Spoofing	#0	✓	Successful
B	Physical Access	#3	✓	Successful
C	Replay Attack between devices	#4	✓	Successful
D	Replay Attack (ABP)	#4	✓	Successful
E	Replay Attack (OTAA)	#4	✗	Not Successful
F	Denial-of-Service and Jamming	#5, #2	✓	Successful

Table 5.1: Implemented attacks and results achieved.

To execute GPS Spoofing it was required to be close to the target device due to the fact that the produced GPS signal needs to be accepted from the device because the GPS antenna always searches for the strongest signal. If the fake GPS signal transmitted by another type of hardware is strong enough, it is always possible to carry out this type of attack, without leaving any type of evidence. The LoRa gateway will receive the packets and the LoRa server will display them through an application with the wrong GPS coordinates values. This attack was executed in the BIRA Bicycle Application, and the points received in the web application were not the real ones and were displayed to the user in another fake location.

For the Physical Access Attack, it was verified that this attack vector is the more dangerous due to room where the LoRa gateway is installed. This room is always open, and everyone inside IPVC can enter this room without leaving any kind of evidences. This attack was considered the most dangerous because of two main things:

1. To perform this attack, it is not necessary to have any type of technical knowledge, because everyone could tamper the gateway by simple disconnecting the LAN cable, that connects the LoRa Gateway to the IPVC backhaul network.

2. Tampering the gateway, or even turning the lights of from the room, could lead to serious damage because all the LoRa network turns offline and cannot communicate with LoRa server.

In Replay Attack between devices, since the devices communicate between them and

the packets do not need to go through the LoRa gateway, the security of the communications is not fully present. If the packets do not pass through the gateway, the security is not guaranteed because none of the activation methods are being used. When capturing some packets and re-transmitting them, the receiver device thinks that they are from a legitimate device. It is always possible to perform this kind of attack due to the lack of security in the transmissions between devices.

To perform a Replay Attack in ABP mode it is necessary to have access to a device where the reset button could be triggered. Turning the energy off and on can also force a reset from the device in the LoRa network server. When a reset occurs by a device, the frame counters transmitted are also reset, and every time a frame counter has a value of 0, this packet can always be transmitted without forcing a reset into the device again because the LoRa gateway and server will assume this packet as a real reset. With that, the first frame can be captured after doing a hard reset on the device, and after that, these packets can always be transmitted with the HackRF One and the LoRa gateway will assume them as legitimate signals from the device.

In Jamming Attack it is necessary to be close to the target gateway. This time high noise signals were produced near the gateway. This led to a stop in the communications due to the high noise transmission. When Jamming is accomplished it could be verified and assumed that is also possible to perform the Denial of Service Attack because the device stops all the communications with the LoRa network.

As mentioned before, the only attack that was not successful was the Replay Attack in OTAA mode. This activation method is the most secure and recommended activation method for end devices due to the fact that devices perform a join procedure with the network, during which a dynamic device address is assigned and security keys are negotiated with the device [115]. When a device performs a network join request, a DevAddr is attributed and sent to the device. With that, it is not possible to have the same device with different DevAddr, so the gateway will discard this uplinks.

5.4 Summary

After identifying the attack vectors referring to the BIRA Bicycle application context, it was pertinent to carry out a series of tests that mirrored a real situation, where the possible attacks previously presented could be exploited. It was presented a detailed description of the experimental setup defined to perform the operations that rely on different types of software, hardware, virtual machines and a laptop. All the implementation of the vulnerabilities exploited were also described. Six types of attacks were chosen, at different points of the attack vectors mentioned before. From the six explored attacks, only one of them was not successful exploited (Replay Attack in OTAA mode). The results of these tests demonstrate that in this type of applications that communicate through LoRAWAN networks, a set of vulnerabilities can be, or are present, and could lead to irreversible damage not only to the application's operation, but also to the system in which it operates.

Chapter 6

Discussion

Within the results obtained in the systematic overview, it is possible to observe that LoRaWAN and NB-IoT were the technologies with most related-works. Between this two technologies, LoRaWAN had more results. However, this does not guarantee that these are the most used protocols in LPWAN, but rather, the protocols that have been more used in research and development, due to their higher maturity and openness to researchers in academia. The major limitation of this approach is the fact that only the IEEEXplore database was used, which despite being the most suitable in terms of using elaborated queries to the research, can eventually restrict this research. Furthermore, the application domains in which more results were also obtained, it was in the context of "smart monitoring" that resulted in 60% of the responses (among the contexts "smart campus", "smart environment", "smart monitoring"). This may reveal, for instance, that the "smart campus" environments are still under the process of developing and implementation on new application contexts that make use of the type of LPWAN technologies. One possibility is that smart campus environments have a high number of users daily pending, and eventually, devices connected to the network, which may originate a wide spectrum of possible threats to this type of network.

This research also allowed to identify the most relevant types of attacks, vulnerabilities, threats, and possible defenses regarding LPWAN technologies. Some of the attacks were identified individually, giving a detailed description of how they can be exploited and carried out. After identifying the main focal points of the identified attacks, the research was carried out to find possible solutions to protect, mitigate or even eliminate these security

weaknesses. Moreover, it was crucial to relate the attacks and vulnerabilities analyzed in the State-of-the-Art review, with these types of technologies, creating a connection in this document. Most of the described attacks are present in LoRa technology. In total, five different types of attacks were identified, which exploit certain vulnerabilities found in this sort of technology. Furthermore, some responses that could be adopted have also been identified to mitigate these threats. One of the main solutions is to update the LoRaWAN protocol to its latest version 1.1, which already has some security improvements compared to its older versions. LoRaWAN v1.1, officially released in October 2017, has been a big upgrade to the specification of the protocol. Concerning the entire network architecture, LoRaWAN v1.1 presents a new server called Join Server, which is introduced to manage the OTAA procedure [116].

After presenting some security vulnerabilities in LPWAN, a set of attack vectors for a generic IoT application was introduced, which presents common security flaws that may arise in a general application case. In this work, the focus was on the LPWAN and Backhaul communication zones, although the Bit-Flipping attack can be performed between the network server and the application server. With the elaboration of each attack vector, it is possible to know where a possible attacker can initiate a malicious action. These attack vectors are related to the state-of-the-art review done previously, so it is possible to identify vulnerabilities and the respective defense strategies, to implement changes to mitigate or avoid these security breaches. One of the weaknesses of the current set of attack vectors can be the fact that the entire communication path between the IoT devices and the client application, has not been fully explored. Security flaws may exist on the server side, or even in the client application. Six different scenarios of possible malicious interactions were presented and mapped with the identified attacks described in the state-of-the-art review. However, all the scenarios developed have a brief description, as well as possible attacks that can be carried out with a set of references that justify them. It is possible to create a link between the set of attack vectors analyzed and the state-of-the-art review.

From the obtained results, the technology that obtained most of the attention regarding security, was the LoRaWAN protocol. This can be observed by the fact that the majority of the attacks identified and described during this study focus on the LoRaWAN technology,

with fewer works related to other LPWAN technologies, such as NB-IoT and Sigfox. With the vulnerabilities described and the types of attacks identified, it was relevant to propose an attack vector analysis to systematize and map these security flaws to the IoT ecosystem, whose main goal was to depict the most vulnerable points that must be considered, when designing IoT applications that rely on LPWAN technologies.

With the development of the defined attack vectors, it is possible to obtain a visual notion that demonstrates in which part of the communications, the possible attackers will be able to perform their malicious intentions. This makes it easier to identify where some improvements and security suggestions may arise in LPWAN-based IoT applications. With this type of approach, it was possible to verify that the identified attack vectors, can be present in several application contexts where distinct users are involved during their daily activities.

The proposed BIRA Bicycle Application system has some specific issues that should be addressed. Firstly, the tracking system should respect the privacy of each user and provide anonymized and general data to the IPVC application managers. Secondly, coverage may also present limitations, mainly if the bikes are used in rural areas on the outskirts of the city. As shown in Figure 4.2, practically the entire city center of Viana do Castelo is covered by LoRaWAN connection. If the user decides to take a longer route, LoRaWAN connectivity may not be guaranteed, failing to communicate his GPS position. Thirdly, the integration of the tracking device on the bicycle needs to be improved. In the designed prototype, a box was adapted for the device and placed under the bicycle seat. It is recommended the development of a capsule that better protects the equipment, more visually appealing, and also easier to adapt to the bicycle. For electric bicycles, one of the solutions for charging the GPS tracker device would be to adapt the device to the electric motor to consume the bicycle's battery. For the conventional bicycles, the device's case needs to be adapted with a mini-USB port output, to be able to charge the device through USB in a conventional power outlet. The proof-of-concept presents an average consumption of 131mA, which means that when using a Li-Ion TR 18650 3.7V battery cell, with a capacity of 9900mAh, an autonomy of 75 hours can be reached. Moreover, upgrades to the device firmware could be introduced to reduce the computational cost and, with this, reduce the devices energy. This can be achieved by selecting ultra-low-

power microprocessors and by using event-triggered programming techniques, such as WoI, and by forcing the microprocessor into an ultra-low-power "sleep" state, until a WoI event occurs. This approach can considerably reduce the overall CPU execution time and contribute to more efficient power management of the IoT device, consuming less energy and reaching higher autonomy.

Lastly, regarding security, the main vulnerabilities in this type of application can be categorized into two types, physical and network attacks. Physical attacks can be performed on the IoT devices deployed on bicycles and they can include damaging the antenna causing it to malfunction, tampering, or even theft. It is difficult to prevent this type of attack since the device is typically exposed and visible. The LoRaWAN communication bandwidth is small and relies on low-power for data transmission. Network attacks like jamming are possible and the hardware used for it can rely on cheap SDRs, which can be configured to transmit powerful malicious signals in the LoRaWAN bands, which may cause denial-of-service due to communication failure. It is also possible to manipulate GPS signals and transmit them over the SDR peripheral an trick the application server with fake GPS positions. Another possible threat is the replay attack. This type of attack takes advantage of the implemented security mechanism, by re-sending or repeating a legitimate data packet, and consists of tricking the device by using handshake messages or old data from the network. Data captured by a malicious actor may be duplicated and replayed to access services that are only available to authenticated users. However, these replay attacks can be detected and blocked in the application layer using the FCNT, cf. Figure 4.6.

Chapter 7

Conclusion

IoT applications may be deployed using LPWAN networks and devices. These LPWAN devices and networks are vulnerable to attacks and, in the context of critical scenarios and applications, it is relevant to review the security risks or vulnerabilities, before to deployment stage.

This work presents the results of a systematic review regarding the evolution of LPWAN communication technologies over the past 10 years. In this context, it also identified security breaches, defense mechanisms and techniques to mitigate attacks. Finally, a set of attack vectors are described and analyzed in the context of LPWAN-based IoT applications. The attacks are mapped in the security vulnerabilities identified in the previous state-of-the-art review.

Based on the review performed, it was possible to conclude that LPWANs technologies had a growth over the past years and discovered and exploited security flaws. It is also possible to verify that most of the results obtained were about LoRa and NB-IoT technologies. Then a state-of-the-art review that focused on the most prominent results that have been found in the systematic overview was conducted on possible threats, vulnerabilities, attacks, and the designated responses to mitigate these weaknesses in this type of technology. Lastly, a set of attack vectors for a generic IoT application was elaborated and analyzed, presenting some possible security breaches that may arise. These security weaknesses were mapped with the security flaws that have been found during the state-of-the-art review. This analysis and results demonstrate that LPWANs contain security vulnerabilities that can be exploited by malicious entities.

A real life scenario was setup to explore a set of attacks. The BIRA Bicycle Application was developed, where the connectivity is ensured by low-cost and secure bi-directional communications with coverage at a regional level, with a focus on the city center of Viana do Castelo. It also uses a low-cost GPS chipset tracker, with state-of-the-art examples for the programmed firmware.

After exploring the Attack Vectors in this application context can be concluded that the existing vulnerabilities could lead to irreversible damage to the application and also to the users, depending on which type of activation method is used in the communications between the devices and the LoRa server. It is suggested to use OTAA mode since it was the only method where the implemented attacks were not successful. Protecting against physical related attacks is also very important, because everyone could execute them, both to the LoRa gateway and the IoT devices.

Future work may include to propose mitigation strategies and the correction of the explored vulnerabilities. Further tests can also be conducted to disclose novel attacks.

Regarding the BIRA Bicycle application, the future work could include the development of a dashboard and a mobile application where regular users can manage their mobility using their devices such as smartphones or tablets. Also, the device box can be further improved to better secure the physical access to the device.

References

[1] Hittu Garg and Mayank Dave. "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware". In: *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. 2019, pp. 1–6. DOI: 10.1109/IoT-SIU.2019.8777334.

[2] "Introduction to IoT — What is LPWAN". In: URL: https://www.leverege.com/iot-ebook/iot-lpwan (visited on 07/29/2020).

[3] Smilty Chacko and Mr. Deepu Job. "Security mechanisms and Vulnerabilities in LPWAN". In: *IOP Conference Series: Materials Science and Engineering* 396 (Aug. 2018), p. 012027. DOI: 10.1088/1757-899x/396/1/012027.

[4] D. Kellstedt et al. "Evaluation of free-floating bike-share on a university campus using a multi-method approach". In: *Preventive Medicine Reports* 16 (2019), p. 100981. ISSN: 2211-3355. DOI: 10.1016/j.pmedr.2019.100981.

[5] A. de Nazelle et al. "Improving health through policies that promote active travel: A review of evidence to support integrated health impact assessment". In: *Environment International* 37.4 (2011), pp. 766–777. ISSN: 0160-4120. DOI: 10.1016/j.envint.2011.02.003.

[6] J. Pucher, J. Dill, and S. Handy. "Infrastructure, programs, and policies to increase bicycling: An international review". In: *Preventive Medicine* 50 (2010), S106–S125. ISSN: 0091-7435. DOI: 10.1016/j.ypmed.2009.07.028.

[7] D. Croce et al. "Performance of LoRa for Bike-Sharing Systems". In: *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*. 2019, pp. 1–6. DOI: 10.23919/EETA.2019.8804519.

[8] N. K. Khadem et al. “Bike Station Suitability on University Campus Using Origin–Destination Matrix—A Morgan State University Case Study”. In: *Urban Science* 3.3 (2019). ISSN: 2413-8851. DOI: 10.3390/urbansci3030074.

[9] M. Longo, C. A. Hossain, and M. Roscia. “Smart mobility for green university campus”. In: *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. Dec. 2013, pp. 1–6. DOI: 10.1109/APPEEC.2013.6837298.

[10] H. H. Teng et al. *Feasibility study of a campus-based bikesharing program at UNLV*. Tech. rep. Mineta National Transit Research Consortium, 2017.

[11] D. H. Kim et al. “Design and implementation of object tracking system based on LoRa”. In: *2017 International Conference on Information Networking (ICOIN)*. 2017, pp. 463–467. DOI: 10.1109/ICOIN.2017.7899535.

[12] PRISMA TRANSPARENT REPORTING of SYSTEMATIC REVIEWS and META-ANALYSES. *PRISMA 2009 Checklist*. 2009. URL: http://www.prisma-statement.org/documents/PRISMA%5C%202009%5C%20checklist.pdf (visited on 12/02/2020).

[13] LoRa Alliance. *LoRaWAN - What is it? - A technical overview of LoRa and LoRaWAN*. URL: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf (visited on 11/20/2020).

[14] W. Ayoub et al. “Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility”. In: *IEEE Communications Surveys Tutorials* 21.2 (2019), pp. 1561–1581. DOI: 10.1109/COMST.2018.2877382.

[15] César Cerrudo and Esteban Martinez. *LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them*. 2020. URL: https://act-on.ioactive.com/acton/attachment/34793/f-87b45f5f-f181-44fc-82a8-8e53c501dc4e/1/-/-/-/-/LoRaWAN%5C%20Networks%5C%20Susceptible%5C%20to%5C%20Hacking.pdf (visited on 07/29/2020).

[16] E. G. Sierra and G. A. Ramirez Arroyave. “Low cost SDR spectrum analyzer and analog radio receiver using GNU radio, raspberry Pi2 and SDR-RTL dongle”. In:

2015 7th IEEE Latin-American Conference on Communications (LATINCOM). 2015, pp. 1–6. DOI: 10.1109/LATINCOM.2015.7430125.

[17] André L. G. Reis et al. "Software defined radio on digital communications: A new teaching tool". In: *WAMICON 2012 IEEE Wireless Microwave Technology Conference*. 2012, pp. 1–8. DOI: 10.1109/WAMICON.2012.6208436.

[18] GNURadio. *About GNU Radio*. 2021. URL: https://www.gnuradio.org/about/ (visited on 10/13/2021).

[19] Khyati Vachhani and Rao Arvind Mallari. "Experimental study on wide band FM receiver using GNURadio and RTL-SDR". In: *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2015, pp. 1810–1814. DOI: 10.1109/ICACCI.2015.7275878.

[20] Eric Blossom. *GNU Radio: Tools for Exploring the Radio Frequency Spectrum*. 2004. URL: https://www.linuxjournal.com/article/7319 (visited on 10/21/2021).

[21] R. Wada and N. Yamasaki. "Fast Interrupt Handling Scheme by Using Interrupt Wake-Up Mechanism". In: *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*. 2019, pp. 109–114. DOI: 10.1109/CANDARW.2019.00027.

[22] D. K. McCormick. "IEEE Technology Report on Wake-Up Radio: An Application, Market, and Technology Impact Analysis of Low-Power/Low-Latency 802.11 Wireless LAN Interfaces". In: *802.11ba Battery Life Improvement: IEEE Technology Report on Wake-Up Radio* (2017), pp. 1–56. DOI: 10.1109/IEEESTD.2017.8055459.

[23] A. Frøytlog and L. R. Cenkeramaddi. "Design and Implementation of an Ultra-Low Power Wake-up Radio for Wireless IoT Devices". In: *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. 2018, pp. 1–4. DOI: 10.1109/ANTS.2018.8710086.

[24] M. Iqbal, A. Y. M. Abdullah, and F. Shabnam. "An Application Based Comparative Study of LPWAN Technologies for IoT Environment". In: *2020 IEEE Region 10 Symposium (TENSYMP)*. 2020, pp. 1857–1860. DOI: 10.1109/TENSYMP50017.2020.9230597.

[25] A. Lavric and V. Popa. “Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey”. In: *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*. 2017, pp. 1–5. DOI: 10.1109/ISSCS.2017.8034915.

[26] H. Pereira et al. “Hacking the RFID-based Authentication System of a University Campus on a Budget”. In: *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. 2020, pp. 1–5. DOI: 10.23919/CISTI49556.2020.9140943.

[27] Pedro Martins et al. “Towards a Smart & Sustainable Campus: An Application-Oriented Architecture to Streamline Digitization and Strengthen Sustainability in Academia”. In: *Sustainability* 13.6 (2021). ISSN: 2071-1050. DOI: 10.3390/su13063189.

[28] Pedro Martins, Sérgio Ivan Lopes, and António Curado. “Designing a FIWARE-based Smart Campus with IoT Edge-enabled Intelligence”. In: *In: A Rocha et al (Eds): WorldCIST 2021, Advances in Intelligent Systems and Computing, AISC 1367*. 2021, pp. 1–13. DOI: 10.1007/978-3-030-72660-7_53.

[29] F. Pereira et al. “Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment”. In: *Sensors* 20.6420 (2020). DOI: 10.3390/s20226420.

[30] S. I. Lopes et al. “On the design of a Human-in-the-Loop Cyber-Physical System for online monitoring and active mitigation of indoor Radon gas concentration”. In: *2018 IEEE International Smart Cities Conference (ISC2)*. 2018, pp. 1–8. DOI: 10.1109/ISC2.2018.8656777.

[31] F. Samie, L. Bauer, and J. Henkel. “IoT technologies for embedded computing: A survey”. In: *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*. 2016, pp. 1–10.

[32] M. Zhang and Q. Hu. “A hybrid network smart home based on Zigbee and smart plugs”. In: *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*. 2017, pp. 389–392. DOI: 10.1109/CSNT.2017.8418572.

[33] S. S. I. Samuel. "A review of connectivity challenges in IoT-smart home". In: *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*. 2016, pp. 1–4. DOI: 10.1109/ICBDSC.2016.7460395.

[34] Mohammad Ali Moridi et al. "Performance analysis of ZigBee network topologies for underground space monitoring and communication systems". In: *Tunnelling and Underground Space Technology* 71 (2018), pp. 201–209. ISSN: 0886-7798. DOI: https://doi.org/10.1016/j.tust.2017.08.018.

[35] T. Hidayat, R. Mahardiko, and F. D. Sianturi Tigor. "Method of Systematic Literature Review for Internet of Things in ZigBee Smart Agriculture". In: *2020 8th International Conference on Information and Communication Technology (ICoICT)*. 2020, pp. 1–4. DOI: 10.1109/ICoICT49345.2020.9166195.

[36] J. Sun and X. Zhang. "Study of ZigBee Wireless Mesh Networks". In: *2009 Ninth International Conference on Hybrid Intelligent Systems*. Vol. 2. 2009, pp. 264–267. DOI: 10.1109/HIS.2009.164.

[37] A. D. Zayas and P. Merino. "The 3GPP NB-IoT system architecture for the Internet of Things". In: *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2017, pp. 277–282. DOI: 10.1109/ICCW.2017.7962670.

[38] K. Mekki et al. "Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT". In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2018, pp. 197–202. DOI: 10.1109/PERCOMW.2018.8480255.

[39] J. Lin et al. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications". In: *IEEE Internet of Things Journal* 4.5 (2017), pp. 1125–1142. DOI: 10.1109/JIOT.2017.2683200.

[40] M. Agiwal, A. Roy, and N. Saxena. "Next Generation 5G Wireless Networks: A Comprehensive Survey". In: *IEEE Communications Surveys Tutorials* 18.3 (2016), pp. 1617–1655. DOI: 10.1109/COMST.2016.2532458.

[41] M. R. Palattella et al. “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models”. In: *IEEE Journal on Selected Areas in Communications* 34.3 (2016), pp. 510–527. DOI: 10.1109/JSAC.2016.2525418.

[42] D. Moongilan. “5G Internet of Things (IOT) Near and Far-Fields and Regulatory Compliance Intricacies”. In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. 2019, pp. 894–898. DOI: 10.1109/WF-IoT.2019.8767334.

[43] L. Chettri and R. Bera. “A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems”. In: *IEEE Internet of Things Journal* 7.1 (2020), pp. 16–32. DOI: 10.1109/JIOT.2019.2948888.

[44] U. Raza, P. Kulkarni, and M. Sooriyabandara. “Low Power Wide Area Networks: An Overview”. In: *IEEE Communications Surveys Tutorials* 19.2 (2017), pp. 855–873. DOI: 10.1109/COMST.2017.2652320.

[45] G. Suciu et al. “IoT time critical applications for environmental early warning”. In: *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. 2017, pp. 1–4. DOI: 10.1109/ECAI.2017.8166451.

[46] Stefan Bjelcevic et al. “LAMBS: Light and Motion Based Safety”. In: (2015). URL: https://andyhub.com/wordpress/wp-content/uploads/LAMBSFinalReport.pdf.

[47] Michal Stočes et al. “Internet of Things (IoT) in Agriculture-Selected Aspects”. In: *AGRIS on-line Papers in Economics and Informatics*. 8th ser. 665-2016-45107 (2016), p. 6. DOI: 10.22004/ag.econ.233969.

[48] M. T. Buyukakkaslar et al. “LoRaWAN as an e-Health Communication Technology”. In: *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 2. 2017, pp. 310–313. DOI: 10.1109/COMPSAC.2017.162.

[49] G. Margelis et al. “Low Throughput Networks for the IoT: Lessons learned from industrial implementations”. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. 2015, pp. 181–186. DOI: 10.1109/WF-IoT.2015.7389049.

[50] Nitesh Dhanjani. *Abusing the internet of things: blackouts, freakouts, and stakeouts.* ” O’Reilly Media, Inc.”, 2015.

[51] Mohamed Abomhara and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks". In: *Journal of Cyber Security and Mobility* 4 (2015), pp. 65–88. DOI: https://doi.org/10.13052/jcsm2245-1439.414.

[52] Engin Leloglu. "A Review of Security Concerns in Internet of Things". In: *Journal of Computer and Communications* 5 (2017), pp. 121–136. ISSN: 2327-5219. DOI: 10.4236/jcc.2017.51010.

[53] Kim Thuat Nguyen, Maryline Laurent, and Nouha Oualha. "Survey on secure communication protocols for the Internet of Things". In: *Ad Hoc Networks* 32 (2015). Internet of Things security and privacy: design methods and optimization, pp. 17–31. ISSN: 1570-8705. DOI: https://doi.org/10.1016/j.adhoc.2015.01.006.

[54] R. Mahmoud et al. "Internet of things (IoT) security: Current status, challenges and prospective measures". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. 2015, pp. 336–341. DOI: 10.1109/ICITST.2015.7412116.

[55] Joseph Migga Kizza. *A Guide to Computer Network Security*. Springer-Verlag London, 2013. ISBN: 978-1-4471-4543-1. DOI: 10.1007/978-1-4471-4543-1.

[56] Elisa Bertino. "Data Security and Privacy in the IoT". In: *19th International Conference on Extending Database Technology, Bordeaux, France, March 15-16, Proceedings*. 2016, pp. 1–3. ISBN: 9783893180707. DOI: 10.5441/002/edbt.2016.02.

[57] E. Aras et al. "Exploring the Security Vulnerabilities of LoRa". In: *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. 2017, pp. 1–6. DOI: 10.1109/CYBConf.2017.7985777.

[58] B. Reynders, W. Meert, and S. Pollin. "Range and coexistence analysis of long range unlicensed communication". In: *2016 23rd International Conference on Telecommunications (ICT)*. 2016, pp. 1–6. DOI: 10.1109/ICT.2016.7500415.

[59] J. Cao et al. "Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network". In: *IEEE Internet of Things Journal* 6.2 (2019), pp. 1561–1575. DOI: 10.1109/JIOT.2018.2846803.

[60] Hans Günter Brauch et al. *Coping with Global Environmental Change, Disasters and Security*. Springer, Berlin, Heidelberg, 2011. ISBN: 978-3-642-17775-0. DOI: https://doi.org/10.1007/978-3-642-17776-7.

[61] Kamal Dahbur, Bassil Mohammad, and Ahmad Bisher Tarakji. "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing". In: *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*. ISWSA '11. Amman, Jordan: Association for Computing Machinery, 2011. ISBN: 9781450304740. DOI: 10.1145/1980822.1980834.

[62] R. Kelly Rainer et al. *Introduction to Information Systems*. John Wiley & Sons, 2020, 2020. ISBN: 978-1118779644.

[63] G. Ikrissi and T. Mazri. "A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS". In: *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* XLIV-4/W3-2020 (2020), pp. 255–261. DOI: 10.5194/isprs-archives-XLIV-4-W3-2020-255-2020.

[64] Shafiq Ul Rehman and Selvakumar Manickam. "A Study of Smart Home Environment and it's Security Threats". In: *International Journal of Reliability, Quality and Safety Engineering 23* (2016). DOI: https://doi.org/10.1142/S0218539316400052.

[65] F. L. Coman et al. "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT". In: *2019 Global IoT Summit (GIoTS)*. 2019, pp. 1–6. DOI: 10.1109/GIOTS.2019.8766430.

[66] Anwaar AlDairi and Lo'ai Tawalbeh. "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies". In: *Procedia Computer Science* 109 (2017), pp. 1086–1091. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2017.05.391.

[67] Fatima Salahdine and Naima Kaabouch. "Social Engineering Attacks: A Survey". In: *Future Internet* 11.4 (2019). ISSN: 1999-5903. DOI: 10.3390/fi11040089.

[68] I. Andrea, C. Chrysostomou, and G. Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges". In: *2015 IEEE Symposium on Computers and Communication (ISCC)*. 2015, pp. 180–187. DOI: 10.1109/ISCC.2015.7405513.

[69] J. Deogirikar and A. Vidhate. "Security attacks in IoT: A survey". In: *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. 2017, pp. 32–37. DOI: 10.1109/I-SMAC.2017.8058363.

[70] X. Yang et al. "Security Vulnerabilities in LoRaWAN". In: *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. 2018, pp. 129–140. DOI: 10.1109/IoTDI.2018.00022.

[71] JungWoon Lee et al. "Risk analysis and countermeasure for bit-flipping attack in LoRaWAN". In: *2017 International Conference on Information Networking (ICOIN)*. 2017, pp. 549–551. DOI: 10.1109/ICOIN.2017.7899554.

[72] V. Skorpil, V. Oujezsky, and L. Palenik. "Internet of Things Security Overview and Practical Demonstration". In: *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. 2018, pp. 1–7. DOI: 10.1109/ICUMT.2018.8631198.

[73] J. Thomas et al. "Man in the Middle Attack Mitigation in LoRaWAN". In: *2020 International Conference on Inventive Computation Technologies (ICICT)*. 2020, pp. 353–358. DOI: 10.1109/ICICT48043.2020.9112391.

[74] K.G. Paterson and Arnold Yau. "Cryptography in Theory and Practice: The Case of Encryption in IPsec". In: vol. 2005. Jan. 2005, p. 416. DOI: 10.1007/11761679_2.

[75] Helger Lipmaa, Phillip Rogaway, and David Wagner. "CTR-Mode Encryption". In: (May 2001).

[76] Xueying Yang. *LoRaWAN: Vulnerability Analysis and Practical Exploitation*. 2017. URL: https://repository.tudelft.nl/islandora/object/uuid:87730790-6166-4424-9d82-8fe815733f1e?collection=education (visited on 09/30/2021).

[77] M. Labib et al. "A Colonel Blotto Game for Anti-Jamming in the Internet of Things". In: *2015 IEEE Global Communications Conference (GLOBECOM)*. 2015, pp. 1–6. DOI: 10.1109/GLOCOM.2015.7417437.

[78] Arduino. *ARDUINO LEONARDO WITH HEADERS*. URL: https://www.arduino.cc/en/Main/ArduinoBoardLeonardo (visited on 01/04/2021).

[79] Semtech. *Semtech SX1276*. URL: https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276 (visited on 01/04/2021).

[80] C. Huang et al. "Experimental Evaluation of Jamming Threat in LoRaWAN". In: *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. 2019, pp. 1–6. DOI: 10.1109/VTCSpring.2019.8746374.

[81] Emekcan Aras et al. "Selective Jamming of LoRaWAN using Commodity Hardware". In: (2017). DOI: 10.1145/3144457.3144478.

[82] Linus Wallgren, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-Based Internet of Things". In: *International Journal of Distributed Sensor Networks* 2013 (2013), p. 11. DOI: 10.1155/2013/794326.

[83] Y. -. Hu, A. Perrig, and D. B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks". In: *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*. Vol. 3. 2003, 1976–1986 vol.3. DOI: 10.1109/INFCOM.2003.1209219.

[84] P. Nagrath and B. Gupta. "Wormhole attacks in wireless adhoc networks and their counter measurements: A survey". In: *2011 3rd International Conference on Electronics Computer Technology*. Vol. 6. 2011, pp. 245–250. DOI: 10.1109/ICECTECH.2011.5942091.

[85] B. Bhushan and G. Sahoo. "Detection and defense mechanisms against wormhole attacks in wireless sensor networks". In: *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*. 2017, pp. 1–5. DOI: 10.1109/ICACCAF.2017.8344730.

[86] L. Liang et al. "A Denial of Service Attack Method for an IoT System". In: *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*. 2016, pp. 360–364. DOI: 10.1109/ITME.2016.0087.

[87] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi. "Use of honeypots for mitigating DoS attacks targeted on IoT networks". In: *2017 International Conference*

on Computer, Communication and Signal Processing (ICCCSP). 2017, pp. 1–4. DOI: 10.1109/ICCCSP.2017.7944057.

[88] L. Xiao et al. "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" In: *IEEE Signal Processing Magazine* 35.5 (2018), pp. 41–49. DOI: 10.1109/MSP.2018.2825478.

[89] M. M. Shurman, R. M. Khrais, and A. A. Yateem. "IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS". In: *2019 International Arab Conference on Information Technology (ACIT)*. 2019, pp. 252–254. DOI: 10.1109/ACIT47987.2019.8991097.

[90] N. Ravi and S. M. Shalinie. "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture". In: *IEEE Internet of Things Journal* 7.4 (2020), pp. 3559–3570. DOI: 10.1109/JIOT.2020.2973176.

[91] X. Luo et al. "Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT". In: *2019 Computing, Communications and IoT Applications (ComComAp)*. 2019, pp. 392–395. DOI: 10.1109/ComComAp46287.2019.9018775.

[92] Gaurav Pathak, Jairo Gutierrez, and Saeed Ur Rehman. "Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions". In: *Electronics* 9.8 (July 2020), p. 1195. ISSN: 2079-9292. DOI: 10.3390/electronics9081195.

[93] Debasis Bandyopadhyay and Jaydip Sen. "Internet of Things: Applications and Challenges in Technology and Standardization". In: *Wireless Personal Communications* 58 (May 2011), pp. 49–69. DOI: 10.1007/s11277-011-0288-5.

[94] Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The Internet of Things: A survey". In: *Computer Networks* 54.15 (2010), pp. 2787–2805. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2010.05.010.

[95] Alvaro Cardenas et al. *CYBER-PHYSICAL SYSTEMS SECURITY KNOWLEDGE AREA (DRAFT FOR COMMENT)*. URL: https://www.cybok.org/ (visited on 11/13/2020).

[96] João B. F. Sequeiros et al. “Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design”. In: *ACM Comput. Surv.* 53.2 (Mar. 2020). ISSN: 0360-0300. DOI: 10.1145/3376123.

[97] Z. Qu et al. “A LoRaWAN-Based Network Architecture for LEO Satellite Internet of Things”. In: *2019 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*. 2019, pp. 1–2. DOI: 10.1109/ICCE-TW46550.2019.8991826.

[98] P. A. Barro, M. Zennaro, and E. Pietrosemoli. “TLTN – The local things network: on the design of a LoRaWAN gateway with autonomous servers for disconnected communities”. In: *2019 Wireless Days (WD)*. 2019, pp. 1–4. DOI: 10.1109/WD.2019.8734239.

[99] S. M. Dimitrov and D. M. Tokmakov. “Integrating data from heterogeneous wireless sensor networks based on LoraWan and ZigBee sensor nodes”. In: *2020 XXIX International Scientific Conference Electronics (ET)*. 2020, pp. 1–4. DOI: 10.1109/ET50336.2020.9238256.

[100] Lopes S.I., Pereira F., Vieira J.M.N., Carvalho N.B., Curado A. “In: Afonso J., Monteiro V., Pinto J. (eds) Green Energy and Networking. GreeNets 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering”. In: *2020 XXIX International Scientific Conference Electronics (ET)*. Vol. 269. 2019, pp. 1–12. DOI: 10.1007/978-3-030-12950-7_12.

[101] S. I. Lopes et al. “RnMonitor: a WebGIS-based platform for expedite in situ deployment of IoT edge devices and effective Radon Risk Management”. In: *2019 IEEE International Smart Cities Conference (ISC2)*. Oct. 2019, pp. 451–457. DOI: 10.1109/ISC246665.2019.9071789.

[102] F. Pereira et al. “RnProbe: A LoRa-Enabled IoT Edge Device for Integrated Radon Risk Management”. In: *IEEE Access* 8 (2020), pp. 203488–203502. DOI: 10.1109/ACCESS.2020.3036980.

[103] Y. Chung, J. Y. Ahn, and J. Du Huh. “Experiments of A LPWAN Tracking(TR) Platform Based on Sigfox Test Network”. In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. 2018, pp. 1373–1376. DOI: 10.1109/ICTC.2018.8539697.

[104] A. Lavric, A. I. Petrariu, and V. Popa. "SigFox Communication Protocol: The New Era of IoT?" In: *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*. 2019, pp. 1–4. DOI: 10.1109/ISSI47111.2019.9043727.

[105] A. Lavric, A. I. Petrariu, and V. Popa. "Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions". In: *IEEE Access* 7 (2019), pp. 35816–35825. DOI: 10.1109/ACCESS.2019.2903157.

[106] P. Yu et al. "Quantum-Resistance Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks". In: *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. 2019, pp. 1–7. DOI: 10.1109/WCNC.2019.8885686.

[107] G. Bernardinetti, F. Mancini, and G. Bianchi. "Disconnection Attacks Against LoRaWAN 1.0.X ABP Devices". In: *2020 Mediterranean Communication and Computer Networking Conference*. 2020, pp. 1–8. DOI: 10.1109/MedComNet49392.2020.9191495.

[108] *Projeto U-bike Portugal*. pt. URL: https://www.u-bike.pt/ (visited on 02/20/2021).

[109] P. Martins, S. I. Lopes, and A. Curado. "Designing a FIWARE-based Smart Campus with IoT Edge-enabled Intelligence". In: *Á. Rocha et al. (Eds.): WorldCIST 2021, Advances in Intelligent Systems and Computing, AISC 1367, pp. 1–13* (2021). DOI: 10.1007/978-3-030-72660-7_53.

[110] *What is the difference between OTAA and ABP Devices - End Devices (Nodes) - The Things Network*. URL: https://www.thethingsnetwork.org/forum/t/what-is-the-difference-between-otaa-and-abp-devices/2723 (visited on 03/11/2021).

[111] *LoRaWAN FAQ*. URL: https://lora-alliance.org/wp-content/uploads/2020/11/la_faq_security_0220_v1.2_0.pdf (visited on 03/11/2021).

[112] GREAT SCOTT GADGETS. *HackRF One*. 2021. URL: https://greatscottgadgets.com/hackrf/one/ (visited on 10/13/2021).

[113] McAfee. *What is GPS spoofing?* 2020. URL: https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing/ (visited on 10/30/2021).

[114] NASA. *NASA's Archive of Space Geodesy Data*. 2021. URL: https://cddis.nasa.gov/archive/gnss/data/daily/ (visited on 07/22/2021).

[115] The Thing Network. *LoRaWAN - End Devices Activation*. 2021. URL: https://www.thethingsnetwork.org/docs/devices/bestpractices/ (visited on 10/30/2021).

[116] Mohamed Eldefrawy et al. "Formal security analysis of LoRaWAN". In: *Computer Networks* 148 (2019), pp. 328–339. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2018.11.017.

Appendices

Appendix A

SASYR 2021 Poster

Symposium of Applied Science for Young Researchers

EXPLORING SECURITY VULNERABILITIES IN LPWANS: THE IPVC BIRA BICYCLE CASE

Nuno Torres [1*], Pedro Pinto [1], Sérgio Ivan Lopes [1]
*nunotorres@ipvc.pt
[1]ADiT-Lab, Instituto Politécnico de Viana do Castelo, 4900-348 Viana do Castelo, Portugal

ABSTRACT

Due to its pervasive nature, the Internet of Things (IoT) is demanding for Low Power Wide Area Network (LPWAN) since wirelessly connected devices need battery-efficient and long-range communications. By using LPWAN technologies the devices can operate using small, inexpensive, and long-lasting batteries (up to 10 years), and can be easily deployed within wide areas (over 2 km in urban zones).
The BIRA bicycle is an initiative of Instituto Politécnico de Viana do Castelo (IPVC) that aims to promote bicycle usage on campus, by encouraging the adoption of more sustainable mobility habits within the institution.
This work is divided in two steps. The first one, is a systematic review on the security vulnerabilities that exist in LPWANs, followed by a literature review with the main goals of substantiating an attack vector analysis specifically designed for the IoT ecosystem.
The second one, is a proposal for a secure LoRa-based tracking system for the BIRA bicycle. The system consists of BIRA bicycles equipped with low-cost GPS trackers. The collected data is transmitted using a LoRaWAN infrastructure to an application server, which is responsible for storing and serving the client application with several contextual information.
The proposed system is a viable low-cost solution for tracking bicycles and users' habits at a campus or city level.

BIRA

BIRA is an initiative of Instituto Politécnico de Viana do Castelo.

1. Aims to promote bicycle usage on campus.
2. Composed by electric and conventional bicycles.
3. Available to IPVC students and staff.

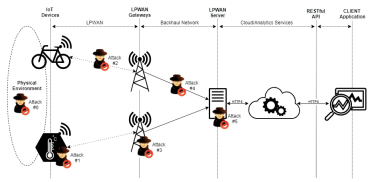
RESULTS

LPWAN Literature Review and Attack Vector Analysis

- LPWAN protocols with most related-works were LoRaWAN and NB-IoT.
- Only the IEEEXplore database was used.
- The application domain with more results was Smart Monitoring with 60%.

Types of possible attacks explored:

1. Physical Attacks (#0, #1, #3).
2. Software Attacks (#1, #5).
3. Encryption Attacks (#5).
4. Data Privacy Attacks (#5).
5. Network Attacks (#2, #4, #5).



Generic attack vectors proposed for LPWAN-based IoT applications [1].

LoRaWAN

Is a LPWAN protocol distinguished by:

- Low-cost.
- Low-power consumption.
- High operational redundancy and scalability.
- Secure bi-directional communications.

Proposed Architecture

- BIRA bicycles equipped with low-cost GPS trackers.
- The collected data is transmitted over LoRaWAN.
- The application server stores and serves the client application with location, route, speed, and battery level.

BIRA bicycle equipped with LoRa GPS tracking device and application frontend [2].

Security Mechanisms

1. Mutual Authentication.
2. Integrity Protection.
3. Confidentiality.

LoRaWAN packet protection mechanism [2].

CONCLUSIONS AND FUTURE WORK

- LPWANs contain security vulnerabilities that can lead to irreversible harm.
- Conception and implementation of up-to-date defenses are relevant to protect systems, networks, and data.
- The proposed system is a viable low-cost solution at a campus or city level.

FUTURE TASKS:

1. Define an experimental setup.
2. Hack the LoRaWAN RF physical layer with Software Defined Radio (SDR) techniques.
   - GPS Jamming and Spoofing.
   - Replay Attacks.
   - Selective Jamming.

RESULTING PUBLICATIONS

[1] **N. Torres**, P. Pinto, S. I. Lopes, "Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem". Appl. Sci. 2021, 11, 3176, DOI: 10.3390/app11073176.

[2] **N. Torres**, P. Martins, P. Pinto and S. I. Lopes, "Smart \& Sustainable Mobility on Campus: A secure IoT tracking system for the BIRA Bicycle", CISTI'2021 – 16th Iberian Conference on Information Systems and Technologies, 23-26 June, Chaves, Portugal.

ipb Instituto Politécnico de Bragança · IPCA Instituto Politécnico do Cávado e do Ave · ipvc Instituto Politécnico de Viana do Castelo · CeDRI Research Centre in Digitalization and Intelligent Robotics · 2Ai Applied Artificial Intelligence Laboratory · ADiT-LAB Applied Digital Transformation Laboratory

Figure A.1: Poster presented at SASYR, in 07/07/2021.