applied sciences

MDPI

Article

Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem

Nuno Torres [1], Pedro Pinto [1,2,3] and Sérgio Ivan Lopes [1,4,*]

[1] ADiT—Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal; nunotorres@ipvc.pt (N.T.); pedropinto@estg.ipvc.pt (P.P.)
[2] Instituto Universitário da Maia, 4475-690 Maia, Portugal
[3] INESC TEC, 4200-465 Porto, Portugal
[4] IT—Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
* Correspondence: sil@estg.ipvc.pt

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. Due to its low-cost and high availability (regional/city level scale), this type of network has been widely used in several IoT applications, such as Smart Metering, Smart Grids, Smart Buildings, Intelligent Transportation Systems (ITS), SCADA Systems. By using LPWAN technologies, the IoT devices are less dependent on common and existing infrastructure, can operate using small, inexpensive, and long-lasting batteries (up to 10 years), and can be easily deployed within wide areas, typically above 2 km in urban zones. The starting point of this work was an overview of the security vulnerabilities that exist in LPWANs, followed by a literature review with the main goal of substantiating an attack vector analysis specifically designed for the IoT ecosystem. This methodological approach resulted in three main contributions: (i) a systematic review regarding cybersecurity in LPWANs with a focus on vulnerabilities, threats, and typical defense strategies; (ii) a state-of-the-art review on the most prominent results that have been found in the systematic review, with focus on the last three years; (iii) a security analysis on the recent attack vectors regarding IoT applications using LPWANs. Results have shown that LPWANs communication technologies contain security vulnerabilities that can lead to irreversible harm in critical and non-critical IoT application domains. Also, the conception and implementation of up-to-date defenses are relevant to protect systems, networks, and data.

Keywords: LPWAN; IoT; security; attacks; responses; attack vectors; LoRa; NB-IoT; Sigfox

Citation: Torres, N.; Pinto, P.; Lopes, S.L. Security Vulnerabilities in LPWANs: An Attack Vector Analysis for the IoT Ecosystem. *Appl. Sci.* **2021**, *11*, 3176. https://doi.org/10.3390/app11073176

Academic Editor: Eui-Nam Huh

Received: 6 March 2021
Accepted: 29 March 2021
Published: 2 April 2021

1. Introduction

The Internet of Things (IoT) 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.

Reducing the computational cost 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) [1] or Wake-Up-Radio (WUR) [2,3], 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 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 Low Power Wide Area Networks (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 [4,5] on a single battery charge and perform long-range wireless communication at a regional/city level. Figure 1 depicts a set of IoT devices used in multiple application scenarios, for example, authentication using RFID [6], to a bike with a tracking device, using a LoRa network [7,8]. 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.

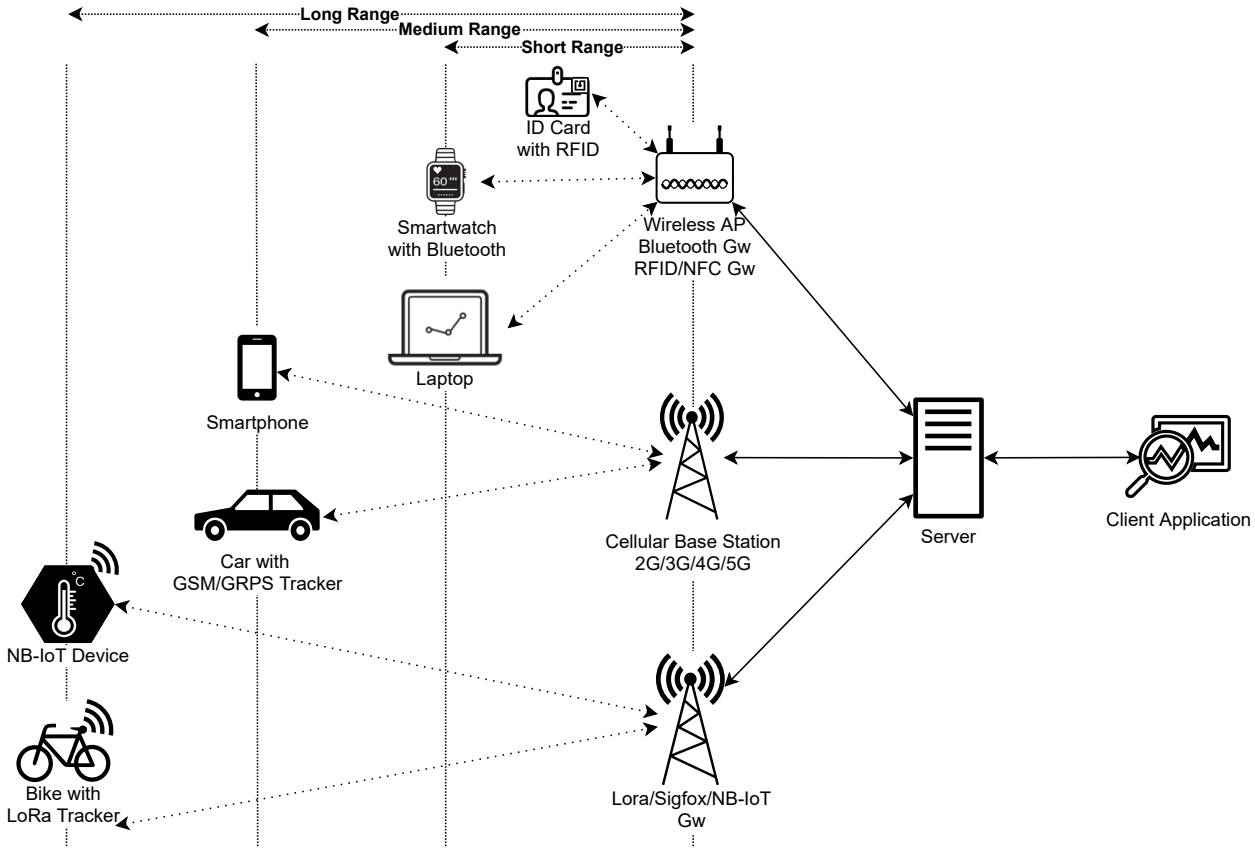


Figure 1. Communication Technologies in IoT applications by range.

When compared with other technologies, cf. Figure 2, LPWANs present higher cost-benefit and higher power/bandwidth efficiency for long-range communications, which results in less infrastructure/hardware needs. 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 [9].

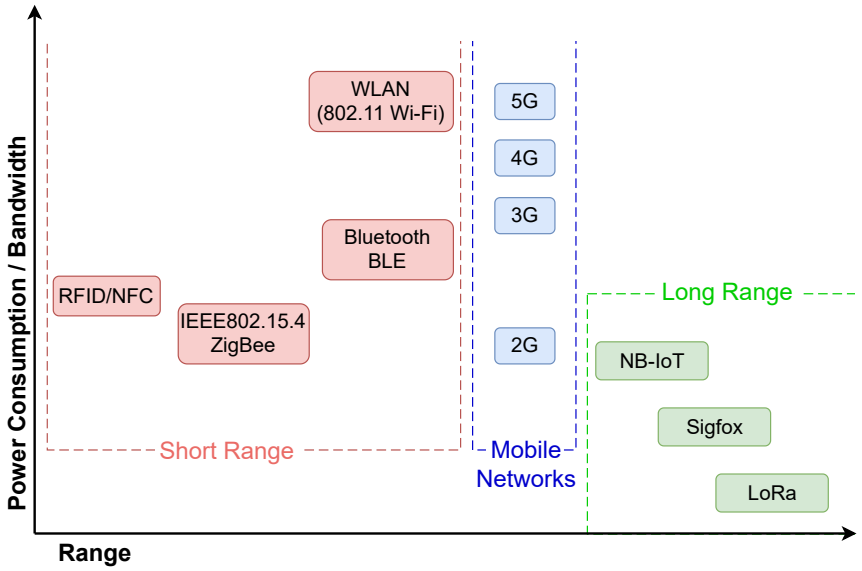


Figure 2. Power/Bandwidth vs. Range in wireless communication Technologies. Adapted from [10].

Mobile networks like 3G and LTE deliver high-speed Internet access [11]. This type of communication is characterized by a high battery drain and flaws in coverage which, according to [12], does not prove to be suitable for the IoT ecosystem. Consequently, cellular networks are not handy for M2M or local network communication [13].

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 [14]. However, Zigbee operates on private networks [15–17], and has not been designed for long-range communications—only for small-scale projects (10–75 m) [18]—but rather to implement mesh networks. In its turn, mesh networks suffer from many factors, such as limited network coverage and high response time [19].

Narrowband IoT (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 [20]. It can be operated in LTE or GSM under licensed frequency bands [21], which is a major drawback, due to the use of licensed spectrum, which increases considerably the operational cost (LTE frequency band for example, the price is over 500 million euro per MHz [22]).

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 [23–25]. 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 [26]. 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 [27]. To make 5G-IoT less expensive over time, some solutions like large-scale manufacturing and common platforms optimization have been recommended [26].

LPWANs have been widely used in several IoT applications as the main communication technology [28]. 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 [29], smart security [30], smart agriculture [31] and smart health [32]. 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) [32]. 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 we aim 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) [33]. 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 [33]. Moreover, LPWAN technologies use, in general, symmetric-key cryptography in which, the end devices and the network, share the same secret key [28].

The main goal of this work is to provide a general overview of which LPWAN technologies are most used today, as well as, to address the core security gaps found in this type of technologies. After identifying its core vulnerabilities, defense strategies are put forward for each specific attack vector, to mitigate the risks that are directly related to each vector. Afterward, a general model for the IoT ecosystem is presented, making it possible to map the security vulnerabilities previously identified, and thus, making it easier to identify the critical attack vectors that can be exploited by malicious users.

This paper provides a security analysis to the attack vectors regarding generic IoT application, given by the evolution (in the last 10 years) of the security issues regarding LPWANs and explore the most relevant state-of-the-art works (from the last three years) that address this topic. To attain this goal, the research methodology was divided into these three steps:

1. Systematic review regarding security in LPWANs with focus on main vulnerabilities, common threats and typical responses, adopted since 2010.
2. State-of-the-art review that focuses on the most prominent results found in the systematic review.
3. Attack Vectors Analysis for a generic IoT application that can be explored in the context of IoT applications using LPWAN.

Based on the results obtained with the systematic review, it was observed that the LPWAN technologies that have been more used and studied, are LoRaWAN and NB-IoT, respectively. After researching LPWAN-related works, relevant vulnerabilities, threats, attack types, and possible defenses were identified and presented in detail. This research has been undertaken to discover strategies to protect, mitigate or even eliminate these security weaknesses. In addition, a set of six attack vectors were identified and related to the security flaws addressed in the state-of-the-art review. Each attack vector was analyzed according to its impact on different application scenarios, which are more likely to be affected by malicious interactions.

The remainder of this document is organized as follows—Section 2 introduces and describes the systematic review methodology and presents its results; Section 3 presents the state-of-the-art review as well as its results; Section 4 defines and presents the analysis on the attack vectors in LPWAN-based IoT applications; Section 5 puts forward a discussion regarding the security analysis; Lastly, in Section 6, the main conclusions are cited.

2. Systematic Review

To perform the systematic review, the PRISMA checklist [34] 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 review is expected to answer each of these questions:

- **Q1**—Given the technologies LoRa, Sigfox, LPWAN, and 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 review follows a defined process, to structure and organize the entire research. A diagram of the systematic process is presented in Figure 3, which identifies all the phases, from the questions to the results.

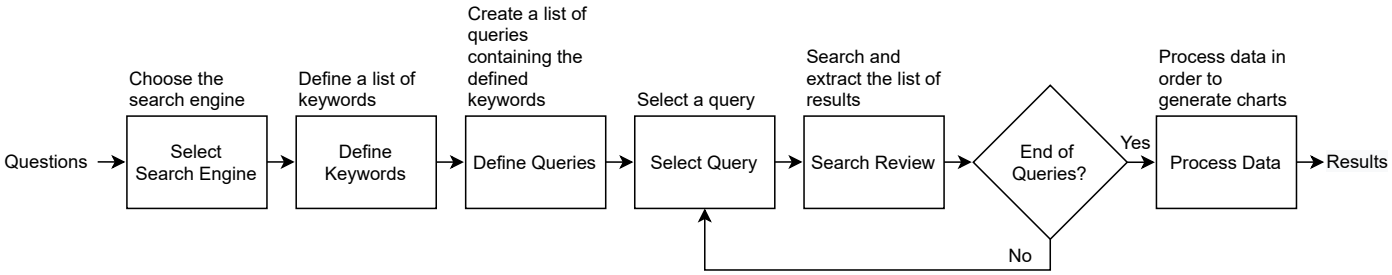


Figure 3. Systematic Process Diagram.

After defining the questions, cf. Section 2, the selection of the search engine was performed. In this work, we opted for the IEEEXplore database, since, when compared to other types of search engines (Google Scholar, Scopus, Arxiv, MDPI, DOAJ), was the one that demonstrated greater capacity and being user-friendly when using relatively elaborated queries (with 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 1.

Table 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 4.

Security Queries		
title contains		metadata contains
lora OR sigfox OR lpwan OR nb-iot	AND	-
		attack
		defense
		exploit
		security
		privacy
		vulnerabilities

Tech Queries		
metadata contains		title contains
attack OR defense OR exploit OR security OR privacy OR vulnerabilities	AND	lora
		sigfox
		lpwan
		nb-iot

Smart Queries				
metadata contains				
lora OR sigfox OR lpwan OR nb-iot	AND	attack OR defense OR exploit OR security OR privacy OR vulnerabilities	AND	-
				smart
				smart campus
				smart environment
				smart monitoring

Figure 4. Queries defined for each category ("Security", "Tech" and "Smart").

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

- 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.

Table 2. Inclusion and Exclusion criteria for this systematic review.

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 5. 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 [35] and NB-IoT [18], 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 5. Systematic review 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, we had *NB-IoT* with 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. Lastlly, *smart campus* presented only 2 papers, with 1 in 2017 and another in 2019.

3. State-of-the-Art Review

IoT technologies have grown over the past years increasing the quality of human life in different application domains, namely, everyday applications (smart home, smart transportation, smart education, smart cities), economy applications (mining fields, oil and gas fields, productivity in factories), health care and security applications [36–39].

The existing IoT connectivity standards, for example, in IEEE 802.15.1 and IEEE 802.15.4 have been generally used, but their short communication range has been announced as the main drawback [40]. Alternatively, cellular networks that allow a wide connectivity range present cost and complexity as their main drawback. Thus, LPWAN has granted a viable option to the diversified shortcomings of these standards.

With LPWAN use cases growing [41], it is crucial to assess the security mechanisms of these technologies. Multiple LPWAN technologies are available using different frequencies and transmission mechanisms, however, all of these types of communications have their own set of resources and security mechanisms for authenticity, confidentiality, and data integrity [42]. Even with the valuable characteristics that LPWAN technologies present, security and privacy issues still the biggest challenge for their large-scale implementation [40]. Due to their heterogeneity, ubiquity, and easy accessibility to devices in the network, LPWANs vulnerabilities continue to increase, leading to new threats and types of intrusions [39]. Security is a major concern in the IoT ecosystem, where LPWAN communication technologies play a crucial role. These types of technologies increase the attackers' range of action due to their long-range connection and high transmission time. Each device connected to the network is a possible vulnerable point where each type of technology uses its security mechanisms to establish secure communications [43].

In this section, the main vulnerabilities, threats, attacks, and defense strategies to these gaps in LPWAN networks will be presented, through a state-of-the-art review.

3.1. 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 [44].

IoT frameworks depend on system hardware equipment and system software, and both have design and configuration defects frequently [45]. Equipment vulnerabilities are exceptionally hard to identify, due to hardware compatibility and interoperability issues, that are difficult to fix [45]. Software weaknesses are present in operating systems, application software, and control software such as communication protocols and device drivers. There are derived circumstances that can lead to software design flaws, namely, human factors and software complexity [46]. 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 [44].

LoRaWan [47] 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 [48]. 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.

A critical factor in the NB-IoT protocol is the lack of computing power in the devices, which limits the use of cryptographic algorithms on the device, which limits the use of public and private keys when operating. If the Diffie Hellman [49] exchange update key is used, the overall exchange process cannot be authenticated and is vulnerable to Man-inthe-Middle (MitM) attacks. Moreover, the IoT device has limited storage resources, being only able to store small size group keys. If a specific key is not updated over time, using always the same key makes the communications vulnerable to ciphertext-only attacks [50].

3.2. Threats

Threats can be defined as actions intended to explore security flaws in a system [51]. Threats derive from essentially primary sources such as human and nature [52,53]. 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 [54] or external [55] 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 [45]. 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.

3.3. Security

Security is one of the main requirements in real-world IoT deployments [56]. 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 [57]. 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 are not supported with the ability to update the firmware/software (i.e., typically

cable-based or over-the-air updates), turning them extremely exposed and vulnerable to eventual exploits and attacks [58]. Security must protect services, devices, information, and data, not only during communication but also data storage [45].

To protect privacy, it must be ensured that communication and collected data met the following requirements, as defined in [59–61]:

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.

3.4. 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 [62]. 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 [45]. 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 [45]. The attackers can make use of these weaknesses to gain access to the systems, swipe sensitive data, and acquire confidential information for later manipulation [63]. Malicious entities can also harm the devices and stop the functionality of the services [62]. In this document, attacks will be classified into five distinct categories, cf. Table 3.

Table 3. Types of possible attacks. Adapted from [62].

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 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.

3.4.1. 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 [47]. Besides, physical access by malicious entities may compromise the security keys and other data [43]. 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 [64]. 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 [65].
- **Social Engineering:** This attack aims to manipulate individuals to divulge confidential and sensitive data [66] 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 [67].
- **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 [68].
- **Environment:** Changing the air temperature (e.g., with a hairdryer). This could trigger an alarm because the values measured by the temperature sensor had dramatically been changed. Using a light cigarette next to a smoke sensor, that could trigger an alarm, c.f. Figure 6.

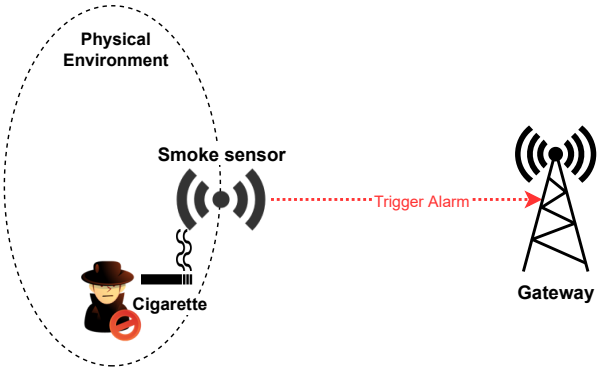


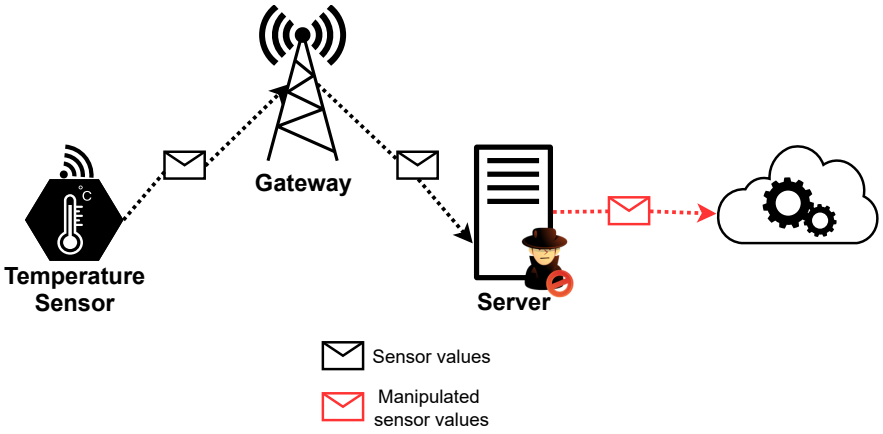
Figure 6. Example of physical-related attack.

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 counter value in between resets [69]. Hardware Security Module (HSM) should be implemented. It 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. If no HSM is used, 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 [64].

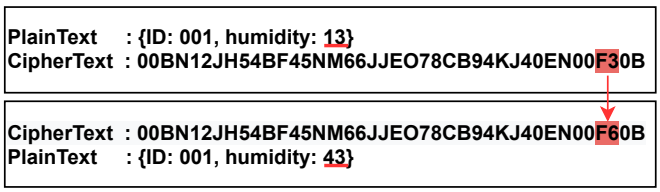
3.4.2. Bit-Flipping Attack

Bit-Flipping is a common encryption attack, cf. Figure 7, which focuses on obtaining the cipher keys during communications. In LoRaWAN, different research studies have identified a security vulnerability that can lead to a bit flipping attack [70]. 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 captures traffic, the application server cannot detect if the message is from the attacker or the network server [71]. The network server in practice is usually fixed by a network operator, and because of the infrastructure, the network server is not able to eavesdrop on the application data. The application server in practice usually belongs to application owners. The application server and the

network server work together in the process of join procedure and traffic control [72]. LoRaWAN messages are both encrypted and provided with a message integrity check. The cryptographic message integrity code on the payload data and header information is checked and terminated by the infrastructure provider, while the payload encryption using the AppSKey is undone by the application provider [69]. Uplink messages are encrypted and then signed. After the network server receives the messages, it uses the NwkSKey to control the signature. Encrypted messages are received on a network server and then processed on the application server. 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 data cannot be checked for integrity and authenticity [69]. If an attacker gains access to a network server, he can eavesdrop on the communication between the network and the application server, which can potentially result in a bit flipping attack [71]. 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 7. An attacker can modify specific fields, just by modulating bits in the same positions of the ciphertext [70]. With this, it is only necessary to change certain fields of the ciphertext, for later when deciphered, the plaintext will be manipulated, cf. Figure 7b).



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



(**b**) Sensor data manipulation.

Figure 7. Bit-Flipping attack example with manipulated sensor data. Adapted from [70].

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 termination of the message integrity code in the system architecture [69]. A secure transmission method between the network server and the application server should be selected and utilized. Since the protocol allows providers to choose the transmission method between two servers, there are numerous decisions, for example, 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 [72].

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 [69]. 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 author [72] suggests that it is necessary for the application server to also check the MIC with NwkSKey to ensure that the message is not modified during the communication between the two servers. NwkSKey is owned by the network server, which in practice, is operated by the network administrator. It would be better if the application server could also have NwkSKey, to be able to calculate the MIC to check the signature.

3.4.3. Jamming Attack

The jamming attack is one of the most serious problems for IoT security [76]. 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 [64]. 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 8, because LoRa transmissions at the same frequency and spreading factor can interfere with each other [48]. This is possible by using commercial-off-the-self LoRa hardware [47].

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 [47], about 99% of LoRa transmissions are damaged by this jamming technique. Typically, this approach uses low-cost devices (Arduino Leonardo [77] board and a Semtech LoRa radio module [78] 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 [64].

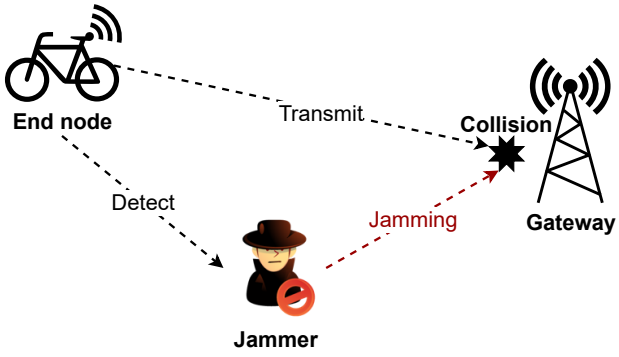


Figure 8. Example of jamming attack. Adapted from [79].

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 [43]. Jamming detection mechanisms can also be useful, for example, changing the used frequency channels [64]. Some low-level techniques [80] 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 [64], 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 Spreading Factors (SFs) require higher dB differentials between the jammer and target message. However higher spreading factor transmissions afford more time for the jammer 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 [80] 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.

3.4.4. Replay Attack

A replay attack is an attack on security protocol, 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 [47]. 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 [62].

For example in replay attack for Activation by Personalization (ABP) activated devices in LoRaWAN, cf. Figure 9, 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. The DoS period relies on selecting a rehashed message [71]. For development devices, which often use ABP activation to join networks, it is necessary to consider that this method has security flaws [47]. For ABP enabled terminal devices are utilized static keys, this way after a reset, the keys continue the same as before, they do not change and may be used in future sessions [81]. 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. As expressed beforehand, the keys are static and the counter values are not utilized securely. For this situation, an attacker can choose and resend messages before the reset, and the server cannot figure if these messages are from this session or the session before the recovery [71]. The LoRaWAN 1.0 protocol states [82] 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 [69]. For this situation, the attacker can use messages from the last session with the high values counters and repeat them in the current session. Whether or not the end device is activated by ABP or Over The Air Authentication (OTAA), it is possible to perform a replay attack [71]. In addition to manually resetting counters on the two sides, the counter overflow is another method of reset. When the counter value reaches its maximum value, the counter is reset and restarts from 0. With 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 [71]. This goes for both ABP and OTAA. 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 [69].

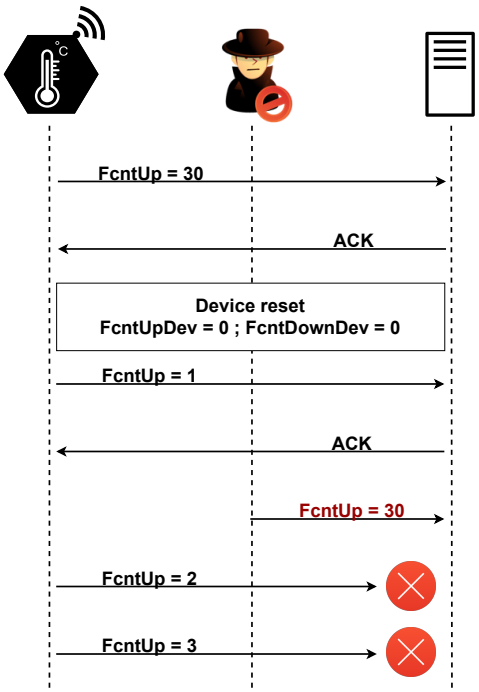


Figure 9. ABP device exploiting the Replay Attack. Adapted from [79].

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 [69]. 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 [43]. 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 [72]. 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, however, the counter values are reused, session keys will prevent the server from accepting malicious messages. With that, this attack will not be possible. 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. According to LoRaWAN specification 1.0.2, after the device activation or the reset, the frame counters on the end-device and the frame counters on the network server for that end-device are reset to zero [69].

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 [72].

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 [72].

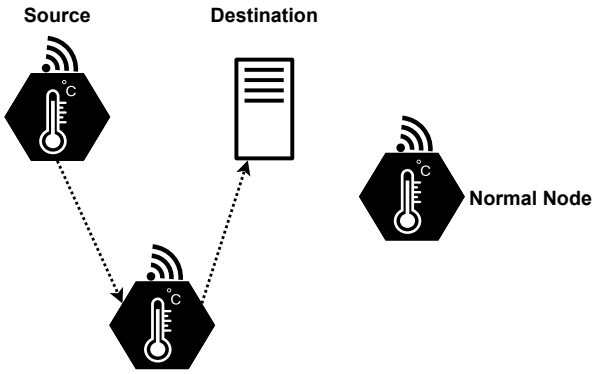
To protect against replay attacks in Sigfox communications, a 12-bit Sequence Number (SN) is used and transmitted with every uplink frame and protected by a specific Message Authentication Code (MAC). If the actual received Sigfox frame contains a lower SN than the latest received frame, the actual frame 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 [64].

3.4.5. Wormhole Attack

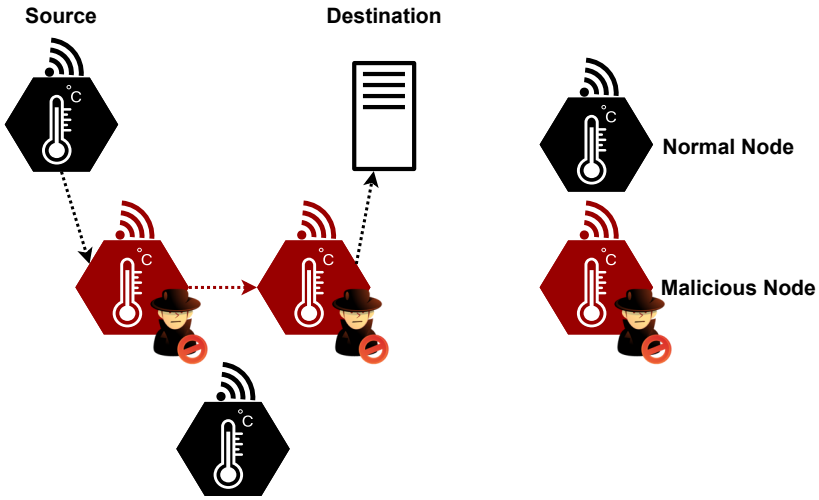
A wormhole is an out-of-band connection between two IoT devices, cf. Figure 10, using wired or wireless links. Wormholes can be used to forward packets faster than via typical paths. A wormhole could not be breach security, for example, a wormhole can be used to forward critical messages where high throughput 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 [56].

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 [47]. 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 [43]. 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 [80]. Since there is no time-related information in LoRaWAN messages [47], wormhole attacks can become a serious security breach and are very difficult to detect particularly when the wormhole is systematically switched on and off [56].



(**a**) Normal Network.



(**b**) Network with wormholes.

Figure 10. 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 [80].

A general mechanism, called packet leashes could be used for detecting and defending against wormhole attacks [43]. 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].

3.4.6. 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 [67], 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 11, 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].

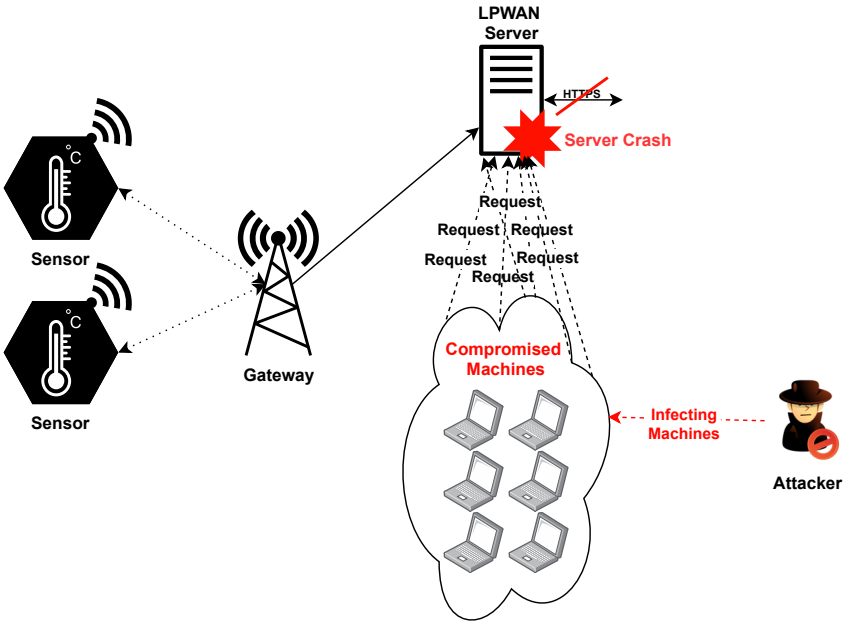


Figure 11. Distributed Denial of Service Attack.

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

ally, 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 [42].

4. Attack Vectors in the IoT Ecosystem

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 [92,93]. This type of device can improve the execution of our 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 [94]. The main activities stage of an IoT application includes data acquisition, data processing, data storage, and data transmission [11].

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 [95]. 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 12, 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 [96–101], Sigfox [102–104] and NB-IoT [50,64,105]. 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.

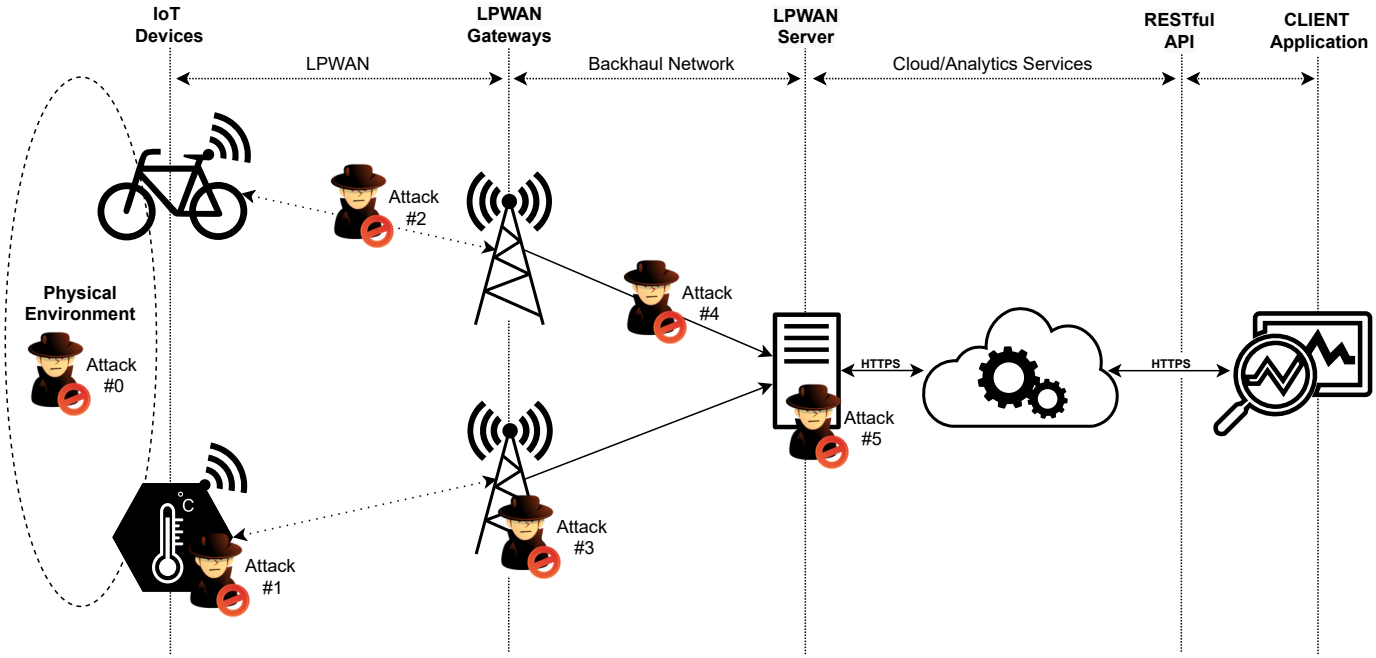


Figure 12. Definition of Attack Vectors in Low Power Wide Area Networks (LPWAN)-based Internet of Things (IoT) applications.

As described in Figure 12, 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 4 compiles and maps the attacks identified in Section 3 to the attack vectors depicted in Figure 12, respectively, with focus on the physical environment, where IoT devices are deployed, and in the LPWAN and backhaul networks.

Table 4. Attack Vectors and their characterization according to Figure 12.

Attack Vector	Description	Attack	Attack Type (Table 3)	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 3.4.1)	Physical	[43,47,62,64,72]
#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 3.4.5)	Software Physical	[56,62,80,83,85]
#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 3.4.3)	Network	[43,47,64,76,80]
#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 3.4.1)	Physical	[43,47,62,64,72]
#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 3.4.4)	Network	[43,62,64,69,71,72,80,81]
#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 3.4.2) Denial-of-Service (Section 3.4.6)	Software Data Privacy Network Encryption	[42,67,69–73,86–91]

5. Discussion

In the systematic review, it is possible to verify that all the defined keywords and the approach used to compile the results, cf. Figure 5, make this analysis more simple and intuitive. From the results obtained, it is possible to observe that the LPWAN protocols with most related-works are LoRaWAN and NB-IoT.

The technology that ranked higher was LoRaWAN, due to its higher penetration in academia.

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 our 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, ends up restricting 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 example, that the "smart campus" environment is still under the process of developing and implementation on new application contexts that make use of the type of LPWAN technologies. In our perspective, this may be because 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.

In this research, it was possible 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 mechanisms such as handover roaming [106] of the end devices such that the Network Server can act according to different roles specified, and a new security architecture which includes the Join Server which allows the end devices to connect to the network [73].

Since Sigfox devices are not IP-addressable, the likelihood of being attacked is reduced, since there is no OTAA mechanism, such as in the LoRaWAN protocol. In Sigfox communications, a user can decide whether to encrypt the message using the encryption solutions provided by its proprietary infrastructure, or by using their encryption methods if necessary [43].

After conducting the research regarding 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 obtain a vision of the critical zones 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 as well as 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 application 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.

The technology that obtained most of the attention from academia, 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, we found it pertinent 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 realize that the identified vulnerabilities, can be achieved in several application contexts where distinct users are involved in various tasks performed throughout their daily activities.

6. Conclusions

This work presents an overview of the evolution of LPWAN communication technologies over the past 10 years. It also identifies some types of security breaches arising from the use of these communication technologies, as well as defense mechanisms and techniques to mitigate them. 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 this research, it was possible to conclude that LPWANs technologies had a spontaneous growth over the past years, as well as 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 review 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.

Author Contributions: Conceptualization, S.I.L.; Methodology, S.I.L., P.P.; Investigation, N.T., P.P. and S.I.L.; Writing—Original Draft Preparation, N.T.; Writing—Review & Editing, S.I.L., P.P.; Supervision, S.I.L. and P.P.; Project Administration, S.I.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is a result of the project TECH—Technology, Environment, Creativity and Health, Norte-01-0145-FEDER-000043, supported by Norte Portugal Regional Operational Program (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Wada, R.; Yamasaki, N. Fast Interrupt Handling Scheme by Using Interrupt Wake-Up Mechanism. In Proceedings of the 2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW), Nagasaki, Japan, 26–29 November 2019; pp. 109–114. [CrossRef]
2. McCormick, D.K. *IEEE Technology Report on Wake-Up Radio: An Application, Market, and Technology Impact Analysis of Low-Power/Low-Latency 802.11 Wireless LAN Interfaces*; 802.11ba Battery Life Improvement: IEEE Technology Report on Wake-Up Radio; IEEE: Piscataway, NJ, USA, 2017; pp. 1–56. [CrossRef]
3. Frøytlog, A.; Cenkeramaddi, L.R. Design and Implementation of an Ultra-Low Power Wake-up Radio for Wireless IoT Devices. In Proceedings of the 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 16–19 December 2018; pp. 1–4. [CrossRef]
4. Iqbal, M.; Abdullah, A.Y.M.; Shabnam, F. An Application Based Comparative Study of LPWAN Technologies for IoT Environment. In Proceedings of the 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 5–7 June 2020; pp. 1857–1860. [CrossRef]
5. Lavric, A.; Popa, V. Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey. In Proceedings of the 2017 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 13–14 July 2017; pp. 1–5. [CrossRef]
6. Pereira, H.; Carreira, R.; Pinto, P.; Lopes, S.I. Hacking the RFID-based Authentication System of a University Campus on a Budget. In Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 24–27 June 2020; pp. 1–5. [CrossRef]
7. Martins, P.; Lopes, S.I.; Rosado da Cruz, A.M.; Curado, A. Towards a Smart & Sustainable Campus: An Application-Oriented Architecture to Streamline Digitization and Strengthen Sustainability in Academia. *Sustainability* **2021**, *13*, 3189. [CrossRef]
8. Martins, P.; Lopes, S.I.; Curado, A. Designing a FIWARE-based Smart Campus with IoT Edge-enabled Intelligence. In *Advances in Intelligent Systems and Computing, AISC 1367, Proceedings of the 9th World Conference on Information Systems and Technologies, WorldCist'21, Terceira Island, Azores, Portugal, 30–31 March 2021*; Rocha, Á., Adeli, H., Dzemyda, G., Moreira, F., Ramalho Correia, A.M., Eds.; Trends and Applications in Information Systems and Technologies; Springer: Cham, Switzerland, 2021; pp. 1–13. [CrossRef]
9. Lopes, S.I.; Cruz, A.M.; Moreira, P.M.; Abreu, C.; Silva, J.P.; Lopes, N.; Vieira, J.M.N.; Curado, A. On the design of a Human-in-the-Loop Cyber-Physical System for online monitoring and active mitigation of indoor Radon gas concentration. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; pp. 1–8. [CrossRef]
10. Pereira, F.; Correia, R.; Pinho, P.; Lopes, S.; Carvalho, N. Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment. *Sensors* **2020**, *20*, 6420. [CrossRef]
11. Samie, F.; Bauer, L.; Henkel, J. IoT technologies for embedded computing: A survey. In Proceedings of the 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Pittsburgh, PA, USA, 2–7 October 2016; pp. 1–10.
12. Leverage. LPWAN Witepaper. Available online: https://www.leverege.com/research-papers/lpwan-white-paper (accessed on 20 November 2020).
13. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 685–690. [CrossRef]
14. Zhang, M.; Hu, Q. A hybrid network smart home based on Zigbee and smart plugs. In Proceedings of the 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, India, 11–13 November 2017; pp. 389–392. [CrossRef]
15. Samuel, S.S.I. A review of connectivity challenges in IoT-smart home. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–4. [CrossRef]
16. Moridi, M.A.; Kawamura, Y.; Sharifzadeh, M.; Chanda, E.K.; Wagner, M.; Okawa, H. Performance analysis of ZigBee network topologies for underground space monitoring and communication systems. *Tunn. Undergr. Space Technol.* **2018**, *71*, 201–209. [CrossRef]
17. Hidayat, T.; Mahardiko, R.; Sianturi Tigor, F.D. Method of Systematic Literature Review for Internet of Things in ZigBee Smart Agriculture. In Proceedings of the 2020 8th International Conference on Information and Communication Technology (ICoICT), Yogyakarta, Indonesia, 24–26 June 2020; pp. 1–4. [CrossRef]
18. Ayoub, W.; Samhat, A.E.; Nouvel, F.; Mroue, M.; Prévotet, J. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1561–1581. [CrossRef]
19. Sun, J.; Zhang, X. Study of ZigBee Wireless Mesh Networks. In Proceedings of the 2009 Ninth International Conference on Hybrid Intelligent Systems, Shenyang, China, 12–14 August 2009; Volume 2, pp. 264–267. [CrossRef]
20. Zayas, A.D.; Merino, P. The 3GPP NB-IoT system architecture for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 277–282. [CrossRef]
21. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 197–202. [CrossRef]
22. Sinha, R.S.; Wei, Y.; Hwang, S.H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* **2017**, *3*, 14–21. [CrossRef]

23. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
24. Agiwal, M.; Roy, A.; Saxena, N. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
25. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
26. Moongilan, D. 5G Internet of Things (IOT) Near and Far-Fields and Regulatory Compliance Intricacies. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 894–898. [CrossRef]
27. Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet Things J.* **2020**, *7*, 16–32. [CrossRef]
28. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873. [CrossRef]
29. Suciu, G.; Anwar, M.; Ganaside, A.; Scheianu, A. IoT time critical applications for environmental early warning. In Proceedings of the 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Romania, 29 June–1 July 2017; pp. 1–4. [CrossRef]
30. Bjelcevic, S.; Jemson, J.; Karusala, N.; Purcell, D. LAMBS: Light and Motion Based Safety. Available online: https://andyhub.com/wordpress/wp-content/uploads/LAMBSFinalReport.pdf (accessed on 25 November 2020).
31. Stočes, M.; Vaněk, J.; Masner, J.; Pavlík, J. Internet of Things (IoT) in Agriculture-Selected Aspects. *AGRIS On-Line Pap. Econ. Inform.* **2016**, *8*, 83–88. [CrossRef]
32. Buyukakkaslar, M.T.; Erturk, M.A.; Aydin, M.A.; Vollero, L. LoRaWAN as an e-Health Communication Technology. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 4–8 July 2017; Volume 2, pp. 310–313. [CrossRef]
33. Margelis, G.; Piechocki, R.; Kaleshi, D.; Thomas, P. Low Throughput Networks for the IoT: Lessons learned from industrial implementations. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 181–186. [CrossRef]
34. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; The PRISMA Group. PRISMA 2009 Checklist. Available online: http://www.prisma-statement.org/documents/PRISMA%202009%20checklist.pdf (accessed on 2 December 2020).
35. Alliance, L. LoRaWAN—What is it?—A Technical Overview of LoRa and LoRaWAN. Available online: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf (accessed on 20 November 2020).
36. Radoglou Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
37. Zeadally, S.; Das, A.K.; Sklavos, N. Cryptographic technologies and protocol standards for Internet of Things. *Internet Things* **2019**, 100075. [CrossRef]
38. Biggs, P.; Garrity, J.; LaSalle, C.; Polomska, A.; Pepper, R.; Hulse, M.; Madigan, M.C.; Borno, R; ITU; Cisco. Harnessing the Internet of Things for Global Development. Available online: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf (accessed on 28 December 2020).
39. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
40. Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. *Sensors* **2020**, *20*, 5800. [CrossRef] [PubMed]
41. Newman, D. Return On IoT: Dealing With The IoT Skills Gap. Available online: https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=7f4661167091#27017efb7091 (accessed on 28 December 2020).
42. Pathak, G.; Gutierrez, J.; Rehman, S.U. Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions. *Electronics* **2020**, *9*, 1195. [CrossRef]
43. Chacko, S.; Job, M.D. Security mechanisms and Vulnerabilities in LPWAN. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*, 012027. [CrossRef]
44. Kizza, J.M. *AGuide to Computer Network Security*; Springer: London, UK, 2013. [CrossRef]
45. Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
46. Bertino, E. Data Security and Privacy in the IoT. In Proceedings of the 19th International Conference on Extending Database Technology (EDBT), Bordeaux, France, 15–18 March 2016. [CrossRef]
47. Aras, E.; Ramachandran, G.S.; Lawrence, P.; Hughes, D. Exploring the Security Vulnerabilities of LoRa. In Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 21–23 June 2017; pp. 1–6. [CrossRef]
48. Reynders, B.; Meert, W.; Pollin, S. Range and coexistence analysis of long range unlicensed communication. In Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016; pp. 1–6. [CrossRef]
49. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
50. Cao, J.; Yu, P.; Ma, M.; Gao, W. Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. *IEEE Internet Things J.* **2019**, *6*, 1561–1575. [CrossRef]

51. Brauch, H.G.; Spring, Ú.O.; Mesjasz, C.; Grin, J.; Kameri-Mbote, P.; Chourou, B.; Dunay, P.; Birkmann, J. *Coping with Global Environmental Change, Disasters and Security*; Springer: Berlin/Heidelberg, Germany, 2011. [CrossRef]
52. Dahbur, K.; Mohammad, B.; Tarakji, A. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2nd International Conference on Intelligent Semantic Web-Services and Applications, ISWSA 2011, Amman, Jordan, 18–20 April 2011; p. 12. [CrossRef]
53. Rainer, R.K.; Prince, B.; Splettstoesser-Hogeterp, I.; Sanchez-Rodriguez, C.; Ebrahimi, S. *Introduction to Information Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2020.
54. Duncan, A.J.; Creese, S.; Goldsmith, M. Insider Attacks in Cloud Computing. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 857–862. [CrossRef]
55. Baybutt, P. Assessing risks from threats to process plants: Threat and vulnerability analysis. *Process Saf. Prog.* **2002**, *21*, 269–275. [CrossRef]
56. Wallgren, L.; Raza, S.; Voigt, T. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *Int. J. Distrib. Sens. Netw.* **2013**, *2013*, 11. [CrossRef]
57. Hayajneh, A.A.; Bhuiyan, Z.A.; Mcandrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]
58. Dhanjani, N. *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*; O'Reilly Media, Inc.: Newton, MA, USA, 2015.
59. Leloglu, E. A Review of Security Concerns in Internet of Things. *J. Comput. Commun.* **2017**, *5*, 121–136. [CrossRef]
60. Nguyen, K.T.; Laurent, M.; Oualha, N. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Netw.* **2015**, *32*, 17–31. [CrossRef]
61. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341. [CrossRef]
62. Ikrissi, G.; Mazri, T. A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS. In Proceedings of the 2020 5th International Conference on Smart City Applications, Virtual Safranbolu, Turkey, 7–8 October 2020. [CrossRef]
63. Rehman, S.U.; Manickam, S. A Study of Smart Home Environment and it's Security Threats. *Int. J. Reliab. Qual. Saf. Eng.* **2016**, *23*, 1640005. [CrossRef]
64. Coman, F.L.; Malarski, K.M.; Petersen, M.N.; Ruepp, S. Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6. [CrossRef]
65. AlDairi, A.; Tawalbeh, L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. [CrossRef]
66. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
67. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187. [CrossRef]
68. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37. [CrossRef]
69. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security Vulnerabilities in LoRaWAN. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 17–20 April 2018; pp. 129–140. [CrossRef]
70. Lee, J.; Hwang, D.; Park, J.; Kim, K.H. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017; pp. 549–551. [CrossRef]
71. Skorpil, V.; Oujezsky, V.; Palenik, L. Internet of Things Security Overview and Practical Demonstration. In Proceedings of the 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Moscow, Russia, 5–9 November 2018; pp. 1–7. [CrossRef]
72. Yang, X. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Master's Thesis, Delft University of Technology, Delft, The Netherlands, 2017.
73. Thomas, J.; Cherian, S.; Chandran, S.; Pavithran, V. Man in the Middle Attack Mitigation in LoRaWAN. In Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–28 February 2020; pp. 353–358. [CrossRef]
74. Paterson, K.G.; Yau A.K.L. Cryptography in Theory and Practice: The Case of Encryption in IPsec. In *Advances in Cryptology–EUROCRYPT 2006. EUROCRYPT 2006*; Vaudenay, S., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4004. [CrossRef]
75. Lipmaa, H.; Rogaway, P.; Wagner, D. Comments to NIST Concerning AES Modes of Operations: CTR-Mode Encryption. In Proceedings of the Symmetric Key Block Cipher Modes of Operation Workshop, Baltimore, MD, USA, 18 October 2000.
76. Labib, M.; Ha, S.; Saad, W.; Reed, J.H. A Colonel Blotto Game for Anti-Jamming in the Internet of Things. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
77. Arduino Store. Arduino Leonardo with Headers. Available online: https://www.arduino.cc/en/Main/ArduinoBoardLeonardo (accessed on 4 January 2021).

78. Semtech. Semtech SX1276. Available online: https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276 (accessed on 4 January 2021).
79. Huang, C.; Lin, C.; Cheng, R.; Yang, S.J.; Sheu, S. Experimental Evaluation of Jamming Threat in LoRaWAN. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–6. [CrossRef]
80. Aras, E.; Small, N.; Ramachandran, G.S.; Delbruel, S.; Joosen, W.; Hughes, D. Selective Jamming of LoRaWAN using Commodity Hardware. In Proceedings of the MobiQuitous 2017, Melbourne, Australia, 7–10 November 2017. [CrossRef]
81. Bernardinetti, G.; Mancini, F.; Bianchi, G. Disconnection Attacks Against LoRaWAN 1.0.X ABP Devices. In Proceedings of the 2020 Mediterranean Communication and Computer Networking Conference (MedComNet), Arona, Italy, 17–19 June 2020; pp. 1–8. [CrossRef]
82. Inc, L.A. LoRaWAN Specification v1.0. Available online: https://lora-alliance.org/sites/default/files/2018-05/2015_-_lorawan_specification_1r0_611_1.pdf (accessed on 7 January 2021).
83. Hu, Y.; Perrig, A.; Johnson, D.B. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of the IEEE INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), San Francisco, CA, USA, 30 March–3 April 2003; Volume 3, pp. 1976–1986. [CrossRef]
84. Nagrath, P.; Gupta, B. Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. In Proceedings of the 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011; Volume 6, pp. 245–250. [CrossRef]
85. Bhushan, B.; Sahoo, G. Detection and defense mechanisms against wormhole attacks in wireless sensor networks. In Proceedings of the 2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall), Dehradun, India, 15–16 September 2017; pp. 1–5. [CrossRef]
86. Liang, L.; Zheng, K.; Sheng, Q.; Huang, X. A Denial of Service Attack Method for an IoT System. In Proceedings of the 2016 8th International Conference on Information Technology in Medicine and Education (ITME), Fuzhou, China, 23–25 December 2016; pp. 360–364. [CrossRef]
87. Anirudh, M.; Thileeban, S.A.; Nallathambi, D.J. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017; pp. 1–4. [CrossRef]
88. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
89. Shurman, M.M.; Khrais, R.M.; Yateem, A.A. IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS. In Proceedings of the 2019 International Arab Conference on Information Technology (ACIT), Al Ain, United Arab Emirates, 3–5 December 2019; pp. 252–254. [CrossRef]
90. Ravi, N.; Shalinie, S.M. Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture. *IEEE Internet Things J.* **2020**, *7*, 3559–3570. [CrossRef]
91. Luo, X.; Yan, Q.; Wang, M.; Huang, W. Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT. In Proceedings of the 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 26–28 October 2019; pp. 392–395. [CrossRef]
92. Bandyopadhyay, D.; Sen, J. Internet of Things: Applications and Challenges in Technology and Standardization. *Wirel. Pers. Commun.* **2011**, *58*, 49–69. [CrossRef]
93. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
94. Cardenas, A.; Kth, H.S.; Conti, M.; Tippenhauer, N.O. Cyber-Physical Systems Security Knowledge Area (Draft for Comment). Available online: https://www.cybok.org/ (accessed on 13 November 2020).
95. Sequeiros, J.A.B.F.; Chimuco, F.T.; Samaila, M.G.; Freire, M.M.; Inácio, P.R.M. Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design. *ACM Comput. Surv.* **2020**, *53*. [CrossRef]
96. Qu, Z.; Cao, H.; Cheng, Y.; Wu, S.; Zhang, G. A LoRaWAN-Based Network Architecture for LEO Satellite Internet of Things. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW), Yilan, Taiwan, 20–22 May 2019; pp. 1–2. [CrossRef]
97. Barro, P.A.; Zennaro, M.; Pietrosemoli, E. TLTN—The local things network: On the design of a LoRaWAN gateway with autonomous servers for disconnected communities. In Proceedings of the 2019 Wireless Days (WD), Manchester, UK, 24–26 April 2019; pp. 1–4. [CrossRef]
98. Dimitrov, S.M.; Tokmakov, D.M. Integrating data from heterogeneous wireless sensor networks based on LoraWan and ZigBee sensor nodes. In Proceedings of the 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020; pp. 1–4. [CrossRef]
99. Lopes S.I.; Pereira F.; Vieira J.M.N.; Carvalho N.B.; Curado A. Design of Compact LoRa Devices for Smart Building Applications. In *Green Energy and Networking. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Proceedings of the 5th EAI International Conference, GreeNets 2018, Guimarães, Portugal, 21–23 November 2018*; Afonso, J., Monteiro, V., Pinto, J., Eds.; Springer: Cham, Switzerland, 2019; Volume 269, pp. 1–12. [CrossRef]

100. Lopes, S.I.; Moreira, P.M.; Cruz, A.M.; Martins, P.; Pereira, F.; Curado, A. RnMonitor: A WebGIS-based platform for expedite in situ deployment of IoT edge devices and effective Radon Risk Management. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019; pp. 451–457. [CrossRef]
101. Pereira, F.; Lopes, S.I.; Carvalho, N.B.; Curado, A. RnProbe: A LoRa-Enabled IoT Edge Device for Integrated Radon Risk Management. *IEEE Access* **2020**, *8*, 203488–203502. [CrossRef]
102. Chung, Y.; Ahn, J.Y.; Du Huh, J. Experiments of A LPWAN Tracking(TR) Platform Based on Sigfox Test Network. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018; pp. 1373–1376. [CrossRef]
103. Lavric, A.; Petrariu, A.I.; Popa, V. SigFox Communication Protocol: The New Era of IoT? In Proceedings of the 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI), Lisbon, Portugal, 29–30 August 2019; pp. 1–4. [CrossRef]
104. Lavric, A.; Petrariu, A.I.; Popa, V. Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions. *IEEE Access* **2019**, *7*, 35816–35825. [CrossRef]
105. Yu, P.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. Quantum-Resistance Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–7. [CrossRef]
106. Eldefrawy, M.; Butun, I.; Pereira, N.; Gidlund, M. Formal security analysis of LoRaWAN. *Comput. Netw.* **2019**, *148*, 328–339. [CrossRef]