Jamming LoRaWAN Over The Air Authentication

by

Baurzhan Orazbayev

Submitted to the School of Engineering and Digital Sciences
in partial fulfillment of the requirements for the degree of

Master of Computer Science

at the

NAZARBAYEV UNIVERSITY

Apr 2022

Author .....
School of Engineering and Digital Sciences
Apr 29, 2022

Certified by .....
Assistant Professor Dimitrios Zormpas
School of Engineering and Digital Sciences
Thesis Supervisor

Accepted by .....
Ph.D. Adnan Yazici
Department Chair, School of Engineering and Digital Sciences

Abstract

Nowadays Internet of Things is widely used in many applications, from industry to agriculture and smart cities. The cyber security of IoT technologies, such as the communication protocols, is a challenging task due to limitations the architecture, and the constrained nature of IoT devices in terms of energy and computation capabilities [14]. In the literature, hardware and software **jamming and anti-jamming** solutions have been developed or investigated [28].

In this thesis, the several jamming attacks and the physical layer vulnerabilities during the LoRa Over The Air Authentication (OTAA) will be discussed and compared in this paper. The focus will be on OTAA authentication attributes influenced by fixed or hopping channel jamming in the experimental test-bed.

Keywords: LoRAWAN, OTTA, Internet of things.

Contents

List of Figures

List of Tables

List of abbreviation

ABP	Activation by Personalization
CSS	Chirp Spread Spectrum
IIoT	Industrial Internet of Things
IoT	Internet of Things
LoRa	Long Range radio modulation technology
LoRaWAN	is a cloud-based MAC protocol based on LoRa
MAC	Medium Access Control
MCU	Microcontroller Unit
MIC	Message Integrity Code
MITM	Man in the Middle
OTAA	Over the Air Activation
RSSI	Received Signal Strength Indicator
SF	Spreading Factor

Chapter 1

Introduction

The Internet of Things (IoT) can continuously connect people and devices anywhere, using a network of different types of devices connected to transfer data seamlessly. The IoT devices communicate over the Internet, allowing businesses to obtain and use strategic information [20]. IoT solutions are widely used to monitor and control industrial, medical, logistics, home, and other applications (Figure 1-1 shows the use cases of IoT). IoT devices use embedded processors technologies that help minimize the sizes and diversify the field of application [5, 13, 29].

1.1 Background

IoT devices may suffer from various attacks, particularly jamming IoT devices attracts attackers' attention due to the potential risk of a feature failure.

Jamming is a deliberate attack that blocks or interferes with wireless communications by using stronger signals, degraded signal-to-noise ratio, or the same radio frequency range [31]. It can block nodes by emitting various blocking signals and aims to disrupt the performance of the IoT network. The IoT Gateway tries to detect or prevent jamming attacks using countermeasures, such as comparing information about the received strength of legitimate signals. However, the developed measures based on the obtained threat classifications cannot effectively protect the IoT Devices [15].

1.2 Motivation

In IoT architectures, the data is transferred through network and middleware devices to application servers and services, where this data is stored and processed. The critical problem is to provide a low power consumption while processing and transmitting data in an extended time [5, 19]. This constraint of IoT devices has created security concerns in handling and transporting the above data in all these steps. The main security problems of IoT devices are related to the following [15]:

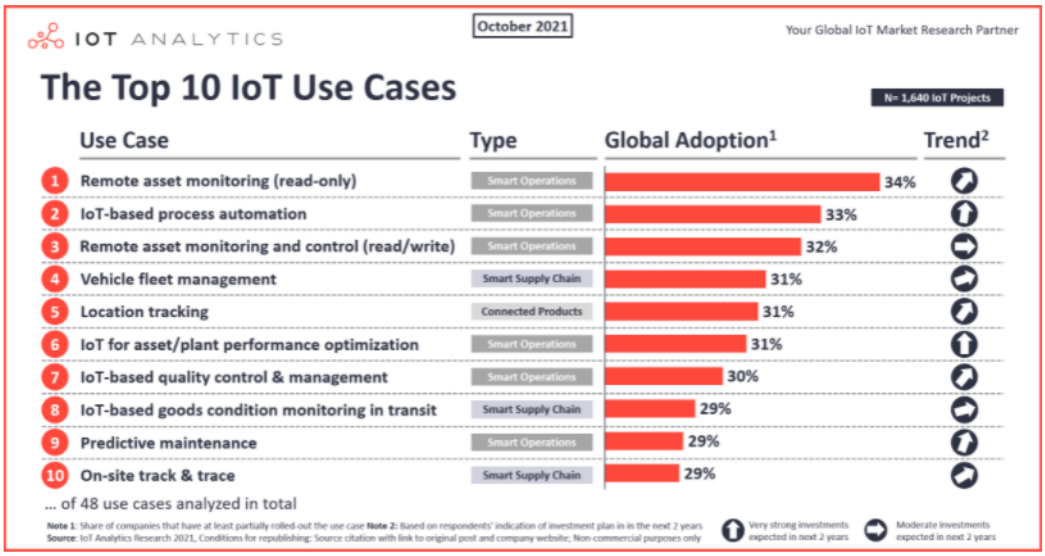

Figure 1-1: The top 10 IoT Use Cases [34]

1. Incorrect access control
2. Overly large attack surface
3. Outdated software
4. Lack of encryption
5. Application vulnerabilities
6. Lack of Trusted Execution Environment
7. Vendor security posture
8. Insufficient privacy protection
9. Intrusion ignorance
10. Insufficient physical security
11. User interaction

1.3 Problem statement

Jamming can affect various LoRa connection elements or procedures, and one of them is the OTAA authentication process. The impact of jamming on OTAA LoRaWAN will be assessed with the following requirements:

1. The microcontroller (MCU) must be small in size, economical, and energy-efficient.
2. MCU must communicate using LoRaWAN technology.
3. The experimental test-bed should be capable of evaluating OTAA authentication vulnerabilities using available hardware.

In this work, we are planning to use Pycom LoPy4, which provides a MicroPython environment with a debug board. Its size is 55mm x 20mm x 3.5mm, weight 7 g, and equipped with the Espressif 32-bit chipset. The device's current consumption during deep sleep is between 7uA and 10uA, depending on the configured wake monitoring sources [9]. These hardware characteristics make this device suitable for the requirements mentioned above.

The expected result is to identify the main shortcomings of OTAA authentication in jamming attacks, which will allow generating more effective security technologies for LoRaWAN.

1.4 Equipment constrains

The main requirements for IoT protocols implementation are the following [5, 23]:

1) Low memory usage

2) Low computational resources

3) Acceptable level of security and confidentiality

4) Economically effective

5) Easy to use

Various organizations and institutes are offering different security solutions. The leading solution is cryptography, and classical cryptography applications can be used in devices with excessive or sufficient performance but not in limited performance IoT models. Lightweight cryptography is a subfield of traditional cryptography provided for devices with limited resources and is proposed by various researchers [25].

The security solutions do not consist of only cryptographically secure implementations. Despite cryptography implementation in LoRa, some IoT LoRa versions are also vulnerable to jamming, replay, or man-in-the-middle attacks [4, 30].

1.4.1 Scope/Limitation

The selection of the LoRa module has been made according to the availability of the hardware. The IoT device information is available on the manufacturer's website [9]. The project aims to implement jamming attacks using the LoRa module and the Pycom Lopy4 microcontroller [9].

The use of single-channel jamming equipment limits the implementation of attacks.

1.5 Proposed approach

These experiments are aimed at investigating of Over-The-Air-Authentication of LoRaWAN. We believe that a broader knowledge of the vulnerabilities will help enhance authentication protocol implementations in the future.

The research investigates how secure the LoRaWAN OTAA mechanism is under jamming attacks low cost and size IoT devices.

1.6 Outline

The thesis is divided in:

- An overview of LoRaWAN and security solutions and technologies.

-The experimental method presents the selected components and the decision-making strategy for the safety decisions and the chosen design (microcontroller, LoRa radio module).

- The implementation part represents and tests the chosen scheme, the environments for the selected microcontroller, LoRa module, and security solution.

- Description of the achieved results of energy consumption measurement and security assessment.

- Discussion of the used methods that helped to understand the project results.

- The conclusion contains the results of the study and findings.

Chapter 2

LoRa and LoRaWAN

2.1 LoRa radio technologies

LoRa is an open-source energy-efficient radio technology, flexible, cost-effective technology, and works in an unlicensed frequency spectrum. This technology is used in smart parking, lighting, waste management services, civil construction, noise, air pollution, etc. [27,35].

2.1.1 LoRa chirp spectrum modulation and Carrier Frequency

There is Chirp Spread Spectrum(CSS) modulating used in LoRa. According to [16] the modulation scheme in CSS uses a linear frequency modulated chirp to represent message symbols. Due to its robustness to narrowband interference, constant envelope, and robustness to multipath fading and Doppler effect, CSS modulation has been adopted by LoRaWan. CSS also allowed LoRa to split the spectrum into different frequency channels [13,28].

LoRa uses different carrier frequencies (CF) for bands ranging from 137 to 1020 MHz in the standards of different countries (EU863-870 for Europe, etc.) [27]. The encoded bits are passed to a whitening block to avoid the transmission of a sequence of consecutive zeros/ones; then, the interleaving block is applied to the scrambled bits. The preamble sequence is combined with the processed bits, and the results are modulated with CSS at the carrier frequency(see Figure 2-1) [28].

2.1.2 Spreading Factor

The spreading factor (SF) determines:

• the amount of data encoded in one symbol. The information that a symbol of SF bits can be encoded in the range from 0 to 2^{SF-1}. For example, if SF is equal to 7, that can be encoded from 0 to 127 different values of one character;

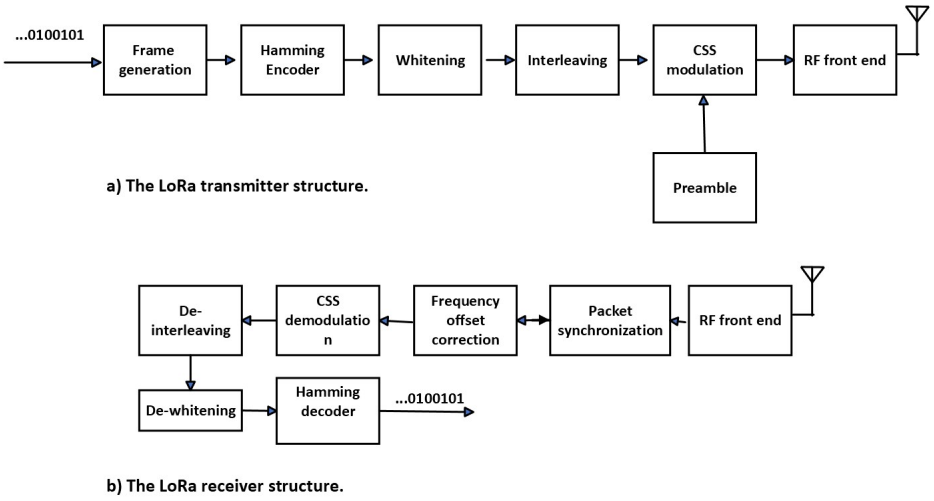

Figure 2-1: The schematic diagram of the LoRa transceiver [28]

• the duration of each chirp (Ts) and hence the airtime of the entire packet. A decrease in SF results in to decrease in the total airtime of the frame, but at the same time, a larger SF contributes to an increase in immunity to interference. The LoRa data rate (DR) depends on SF (in the case of BW = 125 kHz) ranging from SF = 7 and DR = 5.5 kbps to SF = 12 and DR = 0.29 kbps [26, 35]. The Ts can be calculated as:

$$\text{Ts} = \frac{2^{SF}}{BW}. \quad [13]$$

2.1.3 Bandwidth (BW)

According to Semtech company, BW is the chirp rate, which indicates the amount of chirp processed per second and designates the frequency band (e.g., BW = 125 kHz, then chirp frequency = 125000). The LoRa symbol comprises 2^{SF} chirps covering the whole channel, starting with a series of uplink chirps. LoRa offered 125, 250, and 500 kHz BW. LoRa data transmissions use the CSS modulation to support bit rates from 980 to 21900 bps and spreading factors (SF) from 6 to 12 [3, 11, 26, 28].

The LoRa transmission period ranges from hundreds of milliseconds to several seconds, influenced by the size of the payload and the spreading factor. It is an expansive window that provides ample opportunities for jamming attacks [1].

2.2 LoRaWAN

LoRaWAN is a Medium Access Control (MAC) protocol used to process data from low-power devices in WAN systems using LoRa radio media.

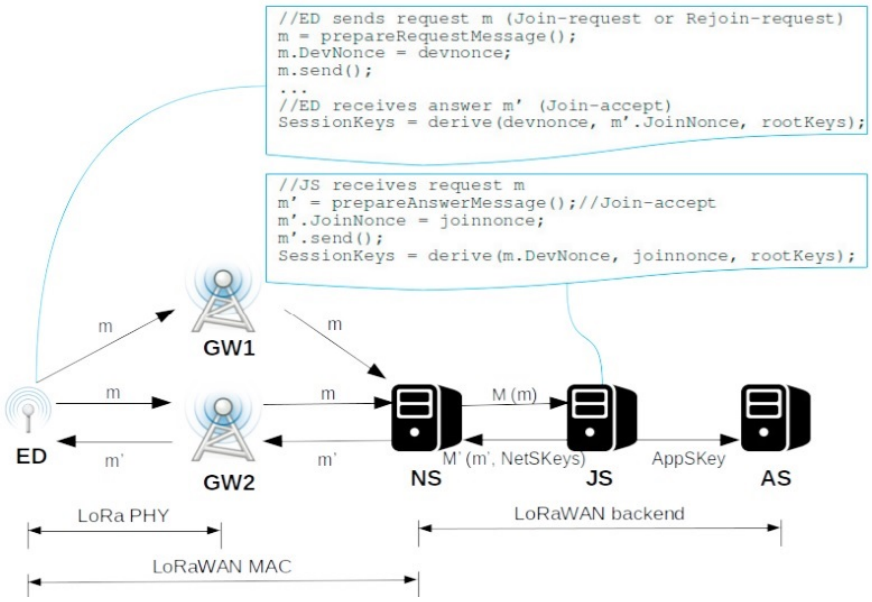

Figure 2-2: LoRaWAN's join procedure [12]

Communication in LoRaWAN can be achieved by using: uplink (from an end-node to a Network Server) and downlink (from a LoRaWAN Network Server to an end-device) packets.

The first byte of the LoRaWAN MAC frame is the MAC header (MHDR), where the three most significant bits define the message type (MType). LoRaWAN class A uses MType equal to zero if the sender did not request confirmation, and on the other side, MType equals one if the sender requested confirmation of this message [21].

The LoRaWAN architecture (see Figure 2-2) consists of the end-devices, gateways, Network, and Application servers. It can include the following:

End-devices are sensors or actuators that exchange chirp-modulated wireless messages with gateways.

Gateways - exchange information with end-devices and forward them to a network server without processing.

Network Server is a server for managing LoRaWAN.

Application server is a server that securely handles application information collected from end-devices.

The join server is a server that handles end-device join requests.

2.2.1 LoRaWAN authentication protocols

Two possible ways of authentication are available in LoRaWAN:

•ABP (Activation By Personalization), where a fixed DevAddr and session keys for a predefined

WAN are implemented in the end device and cannot be changed during the lifetime of this network [19].

•OTAA (Over The Air Activation), where the LoRa end-node generates a request to join LoRaWAN using root keys, which allows to assign end-device a DevAddr and generating session keys that change each time a new session is launched.

2.2.2 LoRaWAN security keys

MAC Payload Encryption (FRMPayload) of LoRaWAN uses the general algorithm described in Appendix B of IEEE 802.15.4 / 2006 [18], using the AES encryption with a key length of 128 bits [21].

Table 2.1: Key elements for the LoRaWAN security [32]

Element	**Description**
DevEUI (64 bit)	Unique ID of the end ED, installed during production. Announced only during the join procedure
DevAddress (32 bit)	The temporary address assigned by the network, valid on the current network, and consists of NwkAddr (network target device address) prefixed with NwkID (network identifier)
AppEUI (64 bit)	Unique ID of the Application server (renamed "JoinEUI" in v1.1).
AppKey (128 bit)	is the encryption key between the source of the message (behind the DevEUI) and the destination of the message (behind the AppEUI). This key must be unique for each ED.
AppSKey (128 bit)	Application Session Key, representing the application session key that is used to encrypt all payloads via AES 128-bit algorithm.
NwkSKey (128 bit)	The network session key represents the network session key used to compute a 32-bit cryptographic Message Integrity Check (MIC) signature via the AES 128-bit algorithm.

The LoRa protocol procedure involves the exchange of a join request (or re-join request) and an acceptance message between the end-device and the join server (see Figure 2-2). Join-accept requests, message processing, and session key generation take place on both parts [12].

After OTAA or ABP activation, the end-device information such as the device address (DevAddr), the network session key (NwkSKey), and the application session key (AppSKey) are kept in the end-device's non-volatile memory [21].

The join server will reject endpoint join requests if the DevNonce reset occurs while the JoinEUI is unchanged.

The NwkSKey is the network session key between the end-device and the network server. It is used to calculate and verify the message integrity code of frames and encrypt and decrypt MAC-only data frames' payload field. To facilitate roaming of end-devices between different network providers, LoRaWAN implements wireless activation where end-devices are not personalized with any network key, and the network session key specific to that end-device is obtained for encryption at the network

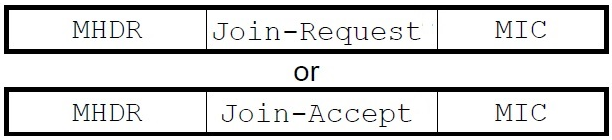

Figure 2-3: OTAA PHY Payload structure

layer.

The AppSKey (application session key) encrypts and decrypts the application payload field. Each endpoint device has a unique set of NwkSKey and AppSKey values, and their compromise does not compromise the security of other nodes' communications. Creating these keys must be such that the keys cannot be extracted from public data (the address of the end-device, server, or DevEUI) [7,21].

2.2.3 OTAA activation procedure

OTAA is one of the possible LoRa activation procedures in which the join procedure is performed whenever end-devices desire to join the network. It is done using a Class A working mode and can be done multiple times if a particular node has lost the session context information. The end-device has a globally unique identifier DevEUI(8 octets), an application identifier AppEUI (8 octets), and an AES-128 key (AppKey) [2, 4]. The LoRaWAN gateway keeps the receiver active until the downlink frame is demodulated after preamble detection [21], and this property can also be used for fixed or hopping interference.

The OTAA activation procedure consists of two MAC layer messages: a connection request sent by the host to the network server and a connection confirmation message sent back by the network server(see Figure 2-3). The join request message is a concatenation of JoinEUI (in version 1.1, AppEUI is renamed JoinEUI), DevEUI, and DevNonce authenticated with a 4-byte message integrity code (MIC) tag using AES in CMAC mode with AppKey; no encryption is performed. An end node initiates the join procedure by sending a join request frame, which consists of JoinEUI (8 octets), DevEUI (8 octets), and DevNonce (2 octets).

After the server has received the join request message, it recalculates the MIC and, if valid, sends the join message, as shown in Figure 2-4. The Join-Accept is authenticated with a 4-byte MIC tag using AES in CMAC mode and encrypted.

End-device temporary address DevAddr and session keys are assigned to the end-device during activation.

Gateway keeps track of the DevNonce values for each target device to avoid using it several times [2,4]. DevNonce is a 16-bit random number formed by N-read operations of the least significant bit of the RegRssiWideband register and the address 0x2c. In this register, the value of the power of the broadband (4 MHz) signal at the device's receiver, received every 1 ms, is stored. In addition,

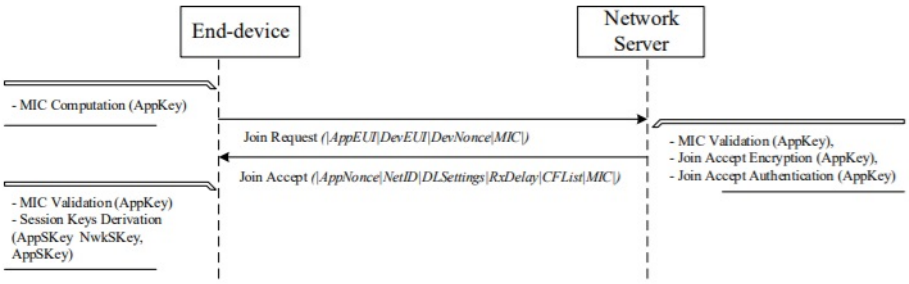

Figure 2-4: LoRaWAN Over the Air Activation [2, 4]

the LSB is constantly and randomly changing due to noise and radio channel behaviour such as reflection, fading, shadowing, and interference [33].

OTAA end-devices are not personalized with a network key, and when an end-device joins the network, a network layer session key specific to that end-device is generated. It allows devices to roam between different networks, and even then, application data cannot be read by the network provider [8].

Potentially any interruption of the OTAA procedure by using jamming can lead to end-device impossibility in the network. If the jamming interrupts the join message, the network will not know about the new end-device, in case of join confirmation, the end-device will not recognize the network parameters for work. So, we suppose that jamming the OTAA has to be investigated in an experimental test-bed.

Chapter 3

Previous researches

Compared to ZigBee and Bluetooth, LoRa can operate in the broader coverage area (5-15 km) and uses low complexity signal processing, low complexity MAC protocol, and consumes only 120-150 mW of transmission power. The device's battery lifetime can vary from 2 to 5 years [13, 28].

One potential gap in the LoRa specification is that when endpoints use ABP (Activation By Personalization), they operate with the same session keys for their entire lifespan (i.e., no key replacement possible). Therefore OTAA endpoints are recommended for higher security applications and be used in our experiments [12, 21].

Some authors [7, 12] have mentioned that a Join server is vital in the security key distribution chain; the network would be vulnerable without this server. To develop the functionality of Join Server, Chen et al. [7] proposed a Centralized Key Management (CKM) scheme that handles key generation/creation (a feature that is not available on the LoRaWAN Join server), update, backup/restore, and key revocation. The authors proposed the operation of generation and statistical check on the SCM, which would relieve the load on the end-devices.

LoRaWAN v1.1 specification does not describe the requirements for the key generation scheme and is limited only by general security requirements. However, the security of communication between end-devices largely depends on the pseudo-randomness of the generated keys; therefore, LoRaWAN includes the AES key generation. It is computationally complex to generate keys for constrained devices efficiently [7].

3.1 LoRaWAN jamming vulnerabilities

Physical access, key management, and lifecycle management are critical security concerns for the IoT. Root keys are integral to LoRaWAN security and must be protected from physical tampering on endpoints. If intruders break the device root keys, they can decrypt all previously-recorded application messages from IoT devices. Some authors have suggested using root keys only for the

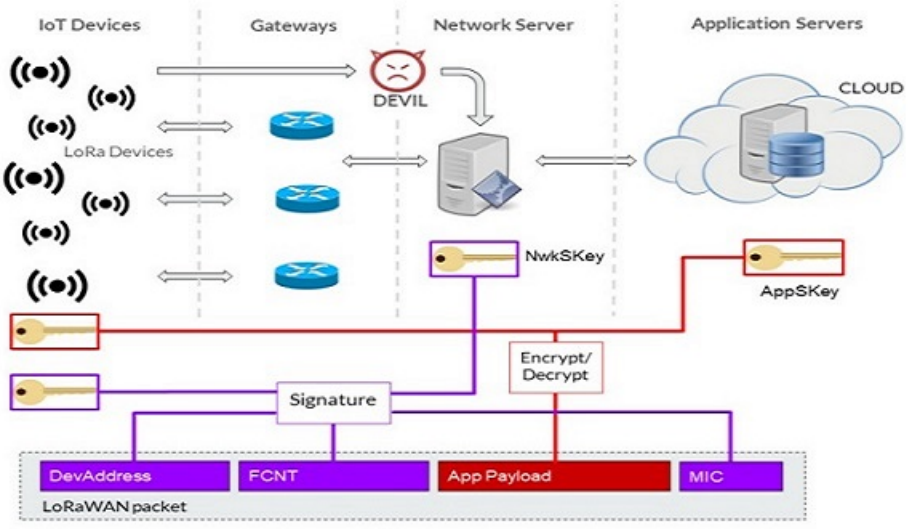

Figure 3-1: LoRaWAN network elements and DEVice Identification and privacy Leakage (DEVIL) [32]

initial collaborative procedure and then removing them from IoT devices. They have suggested using session keys from a previous session, which typically uses root keys [7, 12]. Dönmez and Nigussie offered the countermeasure from the replay attack by keeping track of DevNonce's last and RJcount (in case of v1.0 LoRa) last values in the Join Server, independently of the network server to prevent it from being compromised [12]. But if the join server loses the LastAppSKey, the device could not perform joins or rejoins procedures.

Spadaccino et al. [32] proposed a DEVIL solution(see Figure 3-1) to analyze the traffic exchanged between the endpoint and network server and generate alerts when the detected traffic is significantly different from the reference baseline. They showed that DEVIL could work with flexible network monitoring without relying on the presence of messages (requests to join) sent by end-devices. It is enough to receive a join request in one of the time windows to map the correct DevEUI to the end-device. As it has been demonstrated in experiments, DEVIL can deanonymize devices. The algorithm has a 93% accuracy in detecting all LoRaWAN addresses of a specific DevEUI, successfully restoring the latent mapping between DevAddr and its DevEUI.

Many vulnerabilities of IoT devices were excepted by LoRa cryptography implementation. For example, the endpoint attachment request is signed by AppKey. Thus, the attacker needs the AppKey to calculate the Message Integrity Check (MIC) for the join request, which is very difficult to obtain. To launch a DOS attack, an attacker always needs DevNonce [33].

However, LoRaWAN can suffer from jamming attacks, which can be quickly launched and can not be prevented. Wireless signals are usually jammed by attackers' irregular or sophisticated RF jamming signals, making it difficult for wireless devices to decode data packets. Also, LoRaWAN

operates on the unlicensed ISM bands and uses a pure ALOHA access scheme [11], making it easy to carry out a jamming attack [17].

Most MAC anti-jamming strategies as changing the communication frequency or channel hopping, can only mitigate the problem of consistent collisions [2]. The vulnerability of existing wireless networks can be explained by the lack of effective anti-interference mechanisms in practice, which underlines the critical necessity and fundamental problems in developing practical anti-jamming schemes [28].

Non-orthogonal signal interference can result in transmission failure, but LoRa has six orthogonal spreading factors (SF) to improve channel capacity and spectrum efficiency [17]. LoRa devices that send data simultaneously using specific frequencies and SF parameters can distort the signal of others. The LoRa gateways can receive simultaneous messages with different SF and similar power. Still, interference-influenced collisions occur when messages use the same SF (non-orthogonal signals interfere with each other) or are transmitted with significantly higher power than the legitimate device [2, 17].

Collision probability, in the case of the performance impact of channel-oblivious jammers, is highly dependent on transmit power, duty cycle, the jammers' geographical position, and the number of jammers. In the case where 25 jammers attack LoRaWAN, the probability of packet loss is 2.1 times higher when TX power = 20dBm than 14dBm, due to the lower SNR when the jammers have higher transmit power. The throughput is reduced by 99.8 % if the jammer is located near the end-device (local influence) [22].

3.2 Jamming attacks in LoRa networks

Research LoRa security issues have shown that LoRa PHY is vulnerable to attacks such as jamming and is directly conditional on the duration of the broadcast, which allows for selective and other types of jamming [24]. Traditional types of jamming [10] :

- Band Jamming (BJ) - jamming in the data signal bandwidth (B) and restricted by a fraction(p):

BJ = B * p, where p is the number between 0 and 1.

The Full Band Jamming can be reached when p equals one or Partial Band Jamming when p less 1.

-Tone Jamming (TJ) - combine several sine waveforms in the used bandwidth. TJ can be single tone jamming (in case of only one sine waveform) and multi-tone jamming (several sine waveforms).

LoRa is sensitive to jamming attacks, which can hold without join procedure [2]:

• Triggered jamming is an attack similar to reactive jamming. As soon as the jammer detects the preamble of the LoRaWAN device will be broadcast a jamming signal. Experiments show that the reception rate of packets by a LoRa device drops to 0.5 percent with this type of interference

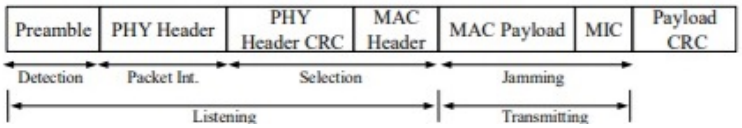

Figure 3-2: Selective jamming attack on packet transmissions [28]

attack.

• Selective Jamming: See Figure 3-2 is an attack in which the jammer sends a jamming signal after decoding the MAC header and endpoint address. This attack can block device communication in LoRaWAN without interfering with other devices on the network. Experiments show that the packet reception rate on the victim's LoRa device drops to 1.3 percent during a selective jamming attack.

• Reactive jamming [26, 28] is when the attacker can measure the power of the received signal and coordinate its jamming signal. The experiments show that for cases if the suppression signal is 3 dB stronger than the LoRa device signal, the device receiver cannot decode the received packets. The packet delivery rate drops to zero.

• Replay attack - the attacker listens to join connection procedure request signal and tampers with it on the LoRa gateway when sending connection request signals in LoRaWANat the PHY level [6]. Then attacker aborts the second connection request attempt and simultaneously sends a saved connection request signal captured in the first device's attempt. The authors claimed that the gateway tends to accept a join request signal tampered with by an attacker because it has never been used before. In this scenario, the LoRa device will no longer sync with its serving gateway because their used connection requests do not match.

For the jammer channel-oblivious cases, like constant or random jamming, the performance of the LoRa network drops significantly. For example, the throughput of all end-devices drops by 16.6 % when adding ten jammers with a duty cycle of 0.5 seconds (broad or non-selective impact) [22].

In channel-aware interference attacks, like triggered or selective jamming (see Figure 3-3, a jammer sends an interfering radio signal when it detects legitimate radio packets. Sometimes, channel-aware selective jamming blocks separate devices only without influencing the network.

Selective jamming can be combined with a Novel Wormhole Attack. Suppose the message can be recorded and prevented from reaching the gateway. If the gateway has not received a message with a higher sequence number, it can be played back later and displayed as a valid message. The above-described selective jamming attack using a single device cannot accomplish standalone since conventional radio transmitters cannot send and receive simultaneously. Hence, this dumb replay attack requires two devices: a sniffer and a jammer. The sniffer gets the messages and decides whether to inhibit the standard selective rejection. If the blocking decision is made, it sends a signal to the jamming device over a low latency link and immediately blocks the message. Unlike a selective

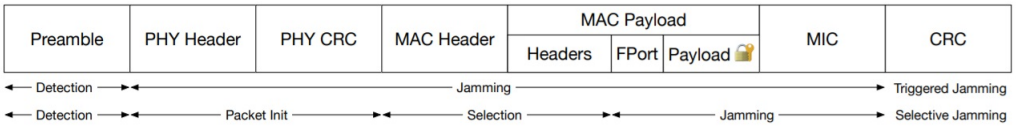

Figure 3-3: Timing of Triggered and Selective Jamming [2]

jamming attack, the scanner listens to the original transmission and stores it for later use in a new attack.

LoRaWAN networks usually have a star topology, with multiple gateways that relay messages between the end-device and the network and the join server. The gateways connect to the core via low latency wired links, while end-nodes use LoRa single-hop radio to connect to the gateways to transfer data to the network server. The end-node transmission will succeed if any gateways decode the received data. In this way, LoRaWAN data will be safe if the jammer's group cannot cover all end-node service gateways [17, 26].

3.3 Anti-jamming Techniques in LoRa networks

Danish et al. [33] proposed an interference detection mechanism in LoRaWAN using two different algorithms:

- Kullback-Leibler divergence (KLD) uses the probability distribution of the received signal without interference and the probability distribution of the received signal in a noisy attack. If the similarity between them is below a certain threshold, the presence of a jamming signal will be announced.

- Hamming distance (HD) scheme uses an algorithm to find the average Hamming distance between the received and training signals. In case of deviation from a certain threshold, the algorithm detects the presence of jamming.

The calculated characteristics show 98 and 88 percent interference detection accuracy for the KLD and HD.

LoRa CSS modulation makes LoRaWAN traffic reliable and more resistant to collisions. Features of LoRa radio protocol [2, 17, 26]:

- the LoRaWAN gateway receives both packets without loss when the packets are simultaneously transmitted over the same frequency channel but with different SF;

- packets are modulated with the same SF, resulting in collisions so that all packets will be lost except for the packet with the highest signal level at the gateway;

- the gateway will reject packets arriving at the gateway with the same signal level and SF.

Chapter 4

Methodology and implementation

In traditional jamming models, the attackers use frequency band interferers, but our testbed uses a device that can only transmit on one channel. In this work, the limitations of the experimental configuration with one potential jammer source are taken into account (see Figure 4-1) and implemented in two types of attacks: jamming in a fixed channel and jamming with channel hopping. The test-bed checks for a vulnerability in either the join-repeat or the join-accept frames.

The LoRa devices used in the experiments were Pycom platform modules: a base station acting as a the joining node, which is affected by an interfering signal (I) in the form of jammer signals generated by another Pycom device end-device acting as the jammer. Usually, when jamming LoRaWAN, the attacker tries to detect and decode the network information from the captured frame. It is assumed that the attacker knows the SF before the attack since the OTAA authentication frame is the first packet in the network. Interference signals have the same spreading factor (in experiment the SF=7) and frequency channels but transmitted with higher power. Each measurement is logged in the end-device and the number of re-authentication attempts (N) in the end-node show the jammer's influence. Additionally it is confirmed by the success or unsuccessful attempt of the OTAA authentication in the TTN (thethingnetwork). In the experiments, it was noticed that:

- in normal conditions (w/o the presence of the jammer), the authentication happened in one attempt (N=1);

- the most significant number of successful OTAA authentications occurred in less than fifteen attempts. So, $N < 15$ was taken as a successful connection attempt.

4.1 Experimental configuration

The end-device can transmit on any of the default channels at the available data rate, selecting frequency channels in a pseudo-random manner, making the system more resistant to interference. When an end-device requests an acknowledgement from the network but has not yet received it,

it sends a new uplink (retry or new frame) after a random time. The end-device must perform frequency hopping between retransmissions. The RETRANSMIT TIMEOUT delay is not required between unacknowledged uplinks or after receiving confirmation by the end-device [21]. Thus the jammer has to cover all possible channels in the LoRa spectrum range of OTAA authentication to succeed in blocking LoRa connections.

In this work, we implement and test fixed and hopping jamming cases using Pycom LoPy4 as an IoT device prototype and focus on LoRaWAN OTAA jamming using inexpensive and small devices.

Mainly, we evaluate the wireless activation connection mechanism OTAA and its vulnerabilities to several kinds of jamming attacks. The TTN (thethingsnetwork.org) cloud service is used as the network server, and a compatible LoRa gateway is also used (see Figure 4-1).

The experimental scheme is adapted for data analysis, and the internal gateway can show logs. The gateway connects over WiFi to TTN and is used as a rogue gateway required to capture and analyze LoRaWAN packets. Also, jammer equipment is used to jam the registration of the LoRa end-devices.

The SF is selected the same for all legitimate and jamming devices in the experiments.

To test the cause-and-effect relationships, we will conduct some experimental methodologies to evaluate the effects of jamming attacks.

The jamming attacks must satisfy at least the following requirements:

i) the time to react to the presence of traffic from devices in the air must be faster than their duration;

ii) the transmission power must be greater than the power of the legitimate messages (6dB higher than regular end-device [17,22]).

For our experiments to be successful, these mentioned above actions need to be coordinated, which can be difficult in some cases [2].

Table 4.1: EU863-870 ISM Band channel frequencies [8]

Channel Frequency (MHz)	**Bandwidth (kHz)**	**LoRa data rate**	**Bit rate**
868.10	125	DR0 – DR5	0.3 – 5 kbps
868.30	125	DR0 – DR5	0.3 – 5 kbps
868.50	125	DR0 – DR5	0.3 – 5 kbps

The jammers have the following capabilities:

-to work with any SF.

-can quickly change the channel frequency.

-to use a low-level configuration that allows logging of LoRa frames.

To test fixed channel jamming, we plan to use jamming devices with the possibility to operate work with the highest available transmit power [22].

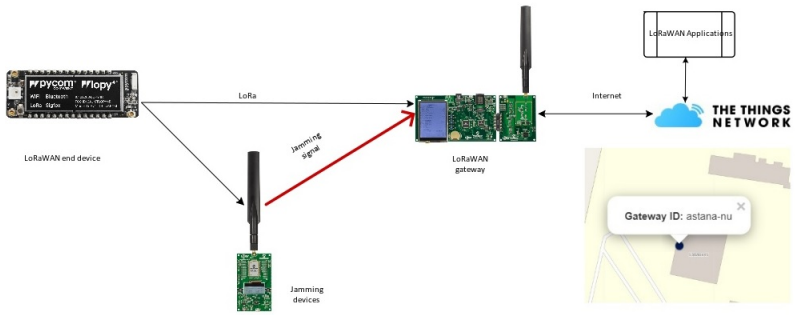

Figure 4-1: Jamming experiment

The end devices are programmed to generate a join request, and after a successful OTAA join procedure, the device reboots to clear the information in volatile memory. This procedure was repeated several times to collect enough statistical information.

The frequency channels settings differ for various regional settings. According to the regional settings of the LoRa Alliance technical committee, the EU863-870 range uses three default channels when bandwidth is equal 125 kHz (see Table 4.1), which are used to broadcast the join request message. The end-device randomly chooses one of them to send a join request message to the gateway [8]. We hypothesize that an attacker could exploit this as a vulnerability, and a single jammer could jam one of these lane channels to disrupt OTAA authentication. This hypothesis is investigated in the test-bed.

The default channels cannot be changed via NewChannelReq command, and manufacturers must guarantee the minimum standard set mentioned above. Manufacturers could increase the number of frequency channels but not decrease them [8]. After authentication, LoRaWAN can support no more than sixteen channels [13].

Table 4.2: EU863-870 Default Settings [8]

Attributes	**Rates**
RECEIVE DELAY1	1s
RECEIVE DELAY2	2s MUST be RECEIVE DELAY1 + 1s
JOIN ACCEPT DELAY1	5s
JOIN ACCEPT DELAY2	6s
MAX FCNT GAP	16384
ADR ACK LIMIT	64
ADR ACK DELAY	32
ACK TIMEOUT	2 +/- 1 s (random delay between 1 and 3s)

According Table 4.2, the join-accept signal confirmations can be received several seconds after join requests. The jammer needs to cover or has the possibility to interrupt this delay to succeed in jamming.

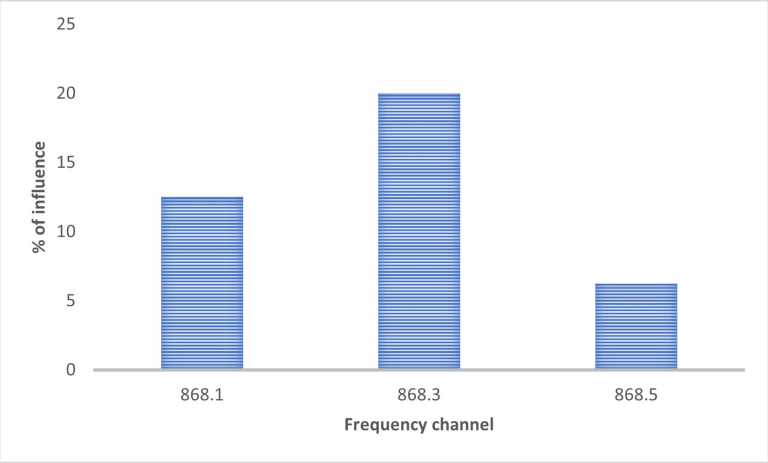

Figure 4-2: Fixed channel jamming

4.2 Fixed channel jamming

Fixed channel jamming uses only one of the three possible OTAA frequency channels. We used the same SF and frequency for the jammer as the joining node to simplify the experiments. According to the recommendations [4], our jammer was placed about one meter from the gateway to test the implementation(Figure 4-1). The end-device was located at different distances (from two to ten meters) from the gateway. According to the recommendations of [22], the power of the interfering signal should be at least six dBm higher than the power of a legitimate transmitter in case of nearby location.

The experiments tested all three default OTAA authentication channels separately. All three frequency channels, 868.1, 868.3, and 868.5 MHz, were tuned and tested under the same test environment (see Figure 4-2) one by one. In the results of fixed channel jamming we received that the influence on the 868.1 MHz channel was less than 12.5 percent, 868.3 20, and 868.5 6.25 percent.

Thus, the experiments in our test-bed demonstrate the efficiency of influence on the fixed channel jamming diverse from 6 to 20 percent. Successful attempts of interruption OTAA authentication were not detected due to the every connection were established after some($N<15$) attempts of authentication.

4.3 Channel hopping jamming

The next possible attack available in our jammer test-bed is the channel interleaving. As previously mentioned, the jammer transmits raw frames over the channel with a higher power. Due to hardware limitations, the jammer could not use simultaneous jamming on the three OTAA authentication channels. The attacker transmits a frame for a given SF on a specific channel and then moves to the next frequency channel and performs another transmission. Three OTAA authentica-

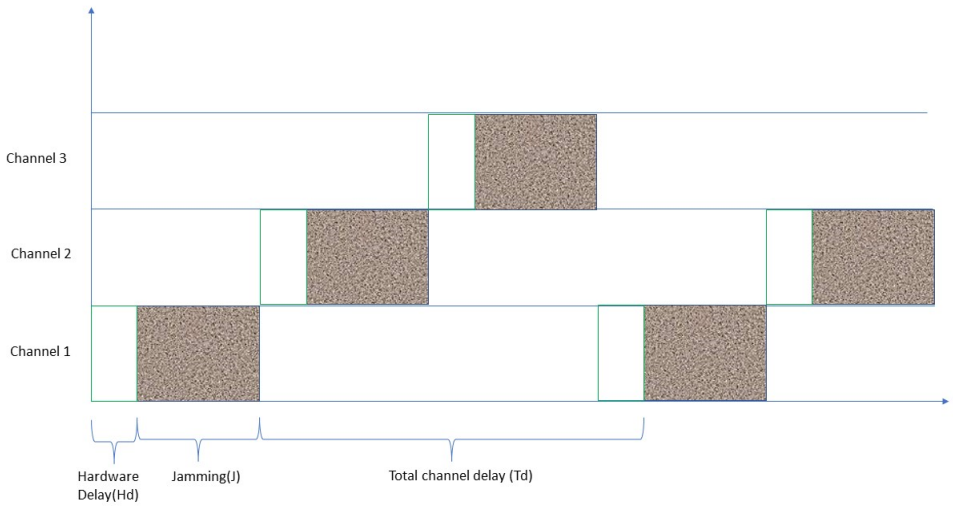

Figure 4-3: Channel hopping jamming

tion channels are available on each SF, and 36 possible combinations are available for LoRaWAN. For our SF combination, our jammer must interfere with all three default channels in a particular SF.

The attacker interleaves three OTAA channels in sequence (see Figure 4-3). The jammer interferes with the channel during the air period (J). It then switches to another channel with a hardware delay (Hd), which depends on the period when the device switches to another frequency. Thus, a legitimate device can send an authentication frame in three Hd and two J periods. Totally:

$$\mathrm{Td} = 2\mathrm{J} + 3\mathrm{Hd}\ (\mathrm{ms}).$$

According to the EU863-870 LoRaWAN v1.1 ISM channel frequency regional settings [8], three mandatory default LoRa channels where all network gateways must listen on 868.1, 868.3, and 868.5 MHz with a bandwidth of 125 kHz. So in test-bed's jammer device must interchange a minimum of three frequency channels.

The power of Pycom's device is limited to 14 dBm, so when testing, if a jammer transmits at that power, then a legitimate device can transmit between eight dBm or lower.

Jamming device can change interference periods (J), and different values are available for the device under test. Hardware delays (Hd) of Pycom devices do not exceed 11 ms.

In experiments we used four different payloads to influence to the air time of jamming signal (from 42 to 175 ms), in the experiment is showed that less airtime (J is equal 42) more efficient in case of hopping jamming.

As can be seen from the 4-4 figure, LoRa is quite resistant to such attacks since the success of the authentication process did not fall below 86 percent. However, channel hopping jamming proved

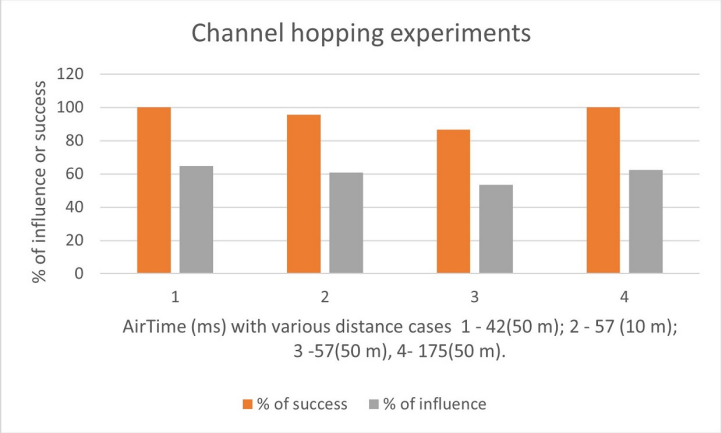

Figure 4-4: Channel hopping experimental jamming results

to be more effective than fixed channel jamming.

4.4 Results of experiments

In the test-bed we investigated the influence of jamming on OTAA authentication LoRa legitimate device.

The experimental results confirm the noise immunity of the LoRa technology. A transceiver used in these experiments could only operate in one frequency channel and not cover the possible entire range simultaneously. Therefore, we are trying to evaluate the impact of such a device on the OTAA authentication process, which has short airtime. In the LoRaWAN protocol, the JoinReq message is the first frame of a legitimate device. Even if this message is intercepted, OTAA authentication is completed, and the goal is not achieved. Thus, we used a simple jamming attack in these tests without capturing the header or the entire radio frame transmitted by the end-device. In the case of jamming only one fixed channel, the impact was minimal. However, the alternate jamming showed results above 53 percent impact (see Figure 4-4), which indicates that the OTAA authentication process can be intercepted by a single-channel jammer.

Figure 4-4 shows that the influence of hopping jamming varied from 53 to 65 percent. The result depends on the distance and airtime of jamming.

4.5 Experiment limitations

In the proposed experiments, the effect of one jammer on one terminal device was demonstrated. Undoubtedly, the efficiency of jamming all default LoRa channels will be higher if multiple jamming devices are used. In addition, the impact will increase in multi-end environments due to the possibility that three (or more) jamming end-devices are transmitting packets on default authentication

channels, which can be attacked.

Also, in this work, it was noted that attacks depend on the airtime and distance to the jammer frame - the more airtime for the jamming frame, the greater the chance of jamming success on the fixing channel. Therefore, examining the impact of several jamming and legal devices in factual conditions in future work is required.

Chapter 5

Conclusion

This work assessed the influence of OTAA LoRaWAN authentication of a jamming attack using a single channel jammer.

We investigated the behavior of the OTAA authentication process using off-the-shelf devices. In this work, it has been confirmed that individual jammers can be used to create collisions on gateways and can block or delay end-devices to join the network.

We suppose that an additional OTAA authentication channel can be used, which will help to reduce the attack's impact. Also, some interference detection mechanisms elaborate [33] can be implemented in OTAA.

Bibliography

[1] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, and Danny Hughes. Exploring the security vulnerabilities of lora. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, pages 1–6. IEEE, 2017. https://core.ac.uk/download/pdf/84932416.pdf.

[2] Emekcan Aras, Nicolas Small, Gowri Sankar Ramachandran, Stéphane Delbruel, Wouter Joosen, and Danny Hughes. Selective jamming of lorawan using commodity hardware. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous 2017, page 363–372, New York, NY, USA, 2017. Association for Computing Machinery. DOI:10.1145/3144457.3144478.

[3] Aloÿs Augustin, Jiazi Yi, Thomas Clausen, and William Mark Townsley. A study of lora: Long range & low power networks for the internet of things. *Sensors*, 16(9):1466, 2016. Retrieved from DOI:10.3390/s16091466.

[4] Ivan Marino Martinez Bolivar. *Jamming on LoRaWAN Networks: from modelling to detection.* PhD thesis, Institut National des Sciences Appliquées de Rennes, 2021. Retrieved from https://tel.archives-ouvertes.fr/tel-03196484/document.

[5] Ismail Butun. *Industrial IoT*, volume 1, pages XXI, 241. Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-42500-5.

[6] Ismail Butun, Nuno Pereira, and Mikael Gidlund. Analysis of lorawan v1.1 security: research paper. In *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, pages 1–6, 06 2018. DOI: 10.1145/3213299.3213304.

[7] Xingda Chen, Margaret Lech, and Liuping Wang. A complete key management scheme for lorawan v1. 1. *Sensors*, 21(9):2962, 2021.

[8] LoRa Alliance Technical Committee. Lorawan. regional parameters, November 2017.

[9] Lopy4, pycom, quadruple bearer micropython enabled dev board. Retrieved from https://pycom.io/product/lopy4/.

[10] Clement Demeslay, Roland Gautier, Anthony Fiche, and Gilles Burel. Band and tone jamming analysis and detection on lora signals. In *Workshop on Security and Protection Information SPI2021*, Jun 2021. Retrieved from arXiv preprint arXiv:2107.07782.2021.

[11] Zorbas Dimitrios, Abdelfadeel Khaled, Kotzanikolaou Panayiotis, and Pesch Dirk. TS-LoRa: Time-slotted LoRaWAN for the Industrial Internet of Things. *Computer Communications*, 153:1 – 10, 2020. Retrieved from DOI: https://doi.org/10.1016/j.comcom.2020.01.056.

[12] Tahsin Dönmez and Ethiopia Nigussie. Security of join procedure and its delegation in lorawan v1.1. *Procedia Computer Science*, 134:204–211, 01 2018. DOI:10.1016/j.procs.2018.07.202.

[13] Panagiotis Gkotsiopoulos, Dimitrios Zorbas, and Christos Douligeris. Performance Determinants in LoRa Networks: A Literature Review. *IEEE Communications Surveys Tutorials*, 23(3):1721–1758, 2021. Retrieved from DOI: 10.1109/COMST.2021.3090409.

[14] Nilupulee A. Gunathilake, William J. Buchanan, and Rameez Asif. Next generation lightweight cryptography for smart iot devices: : Implementation, challenges and applications. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 707–710, 2019. doi: 10.1109/WF-IoT.2019.8767250.

[15] Chen Haibo, Zhang Dalin, Chen Jinfu, Lin Wei, Shi Dengzhou, and Zhao Zian. An automatic vulnerability classification system for iot softwares. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, pages 1525–1529, 12 2020. Retrieved from: 10.1109/TRUSTCOM50675.2020.00208.

[16] Muhammad Hanif and Ha H Nguyen. Frequency-shift chirp spread spectrum communications with index modulation. *IEEE Internet of Things Journal*, 2021. Retrieved from https://arxiv.org/pdf/2102.04642.pdf.

[17] Chin-Ya Huang, Ching-Wei Lin, Ray-Guang Cheng, Shanchieh Jay Yang, and Shiann-Tsong Sheu. Experimental evaluation of jamming threat in lorawan. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–6. IEEE, 2019. DOI: 10.1109/VTC-Spring.2019.8746374.

[18] Low-Energy Critical Infrastructure and Monitoring LECIM Physical Layer. Ieee standard for low-rate wireless networks, 2020.

[19] Azhar Iqbal, Muhammad, Sajjad Hussain, Huanlai Xing, and Muhammad Ali Imran. *Internet of Things Security*, pages i–xix. River Publishers, 2018. Retrieved from doi:10.1002/9781119701460.fmatter.

[20] K. Kalkan. Sutsec: Sdn utilized trust based secure clustering in iot. *Computer Networks*, 178, 9 2020. doi://10.0.3.248/j.comnet.2020.107328.

[21] Lorawan® 1.0.4 specification package - lora alliance®, 10 2020.

[22] Ivan Martinez, Philippe Tanguy, and Fabienne Nouvel. On the performance evaluation of lorawan under jamming. In *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*, pages 141–145. IEEE, 2019. Retrieved from https://hal.archives-ouvertes.fr/hal-02301010/document.

[23] Turan Meltem, Sonmez, McKay Kerry, Chang Donghoon, Calik Cagdas, Bassham Lawrence, Kang Jinkeon, and Kelsey John. Status report on the second round of the nist lightweight cryptography standardization process. *National Institute of Standards and Technology*, 7 2021. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8369.pdf.

[24] Jung Moon, Soo and Wonjun Lee. Friendly jamming in lora physical layer using imperfect orthogonality of spreading factor. In *2022 International Conference on Information Networking (ICOIN)*, pages 423–428, 2022. DOI: 10.1109/ICOIN53446.2022.9687108.

[25] National Institute of Standards and Technology. Computer Security Division. Submission requirements and evaluation criteria for the lightweight cryptography standardization process. *National Institute of Standards and Technology*, August 2018. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight Cryptography/documents/final-lwc-submission-requirements-august2018.pdf.

[26] Toni Perković, Hrvoje Rudeš, Slaven Damjanović, and Antun Nakić. Low-cost implementation of reactive jammer on lorawan network. *Electronics*, 10(7):864, 2021. DOI: 10.3390/electronics10070864.

[27] Toni Perković and Dino Siriščević. Low-cost lorawan jammer. In *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–6, 2020. DOI: 10.23919/SpliTech49282.2020.9243739.

[28] Hossein Pirayesh and Huacheng Zeng. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *arXiv preprint arXiv:2101.00292*, 2021. Retrieved from http://arxiv.org/abs/2101.00292.

[29] Minerva Roberto, Biru Abyi, and Rotondi Domenico. Internet of things. In *Towards a definition of the Internet of Things*, 2015.

[30] Michael Santamaria and Alan Marchiori. Internet of things. In *Demystifying LoRa WAN Security and Capacity*, pages 1–7, 2019. doi: 10.1109/ITNAC46935.2019.9077997.

[31] Vineeta Soni, Samriddhi Koolwal, Sahiti Balantrapu, Devershi Pallavi Bhatt, and Narendra Singh Yadav. Security requirements in internet of things: Challenges and methods. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, pages 600–604, 2021. DOI: 10.1109/ISPCC53510.2021.9609355.

[32] Pietro Spadaccino, Domenico Garlisi, Francesca Cuomo, Giorgio Pillon, and Patrizio Pisani. Discovery privacy threats via device de-anonymization in lorawan. In *2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet)*, pages 1–8, 2021. DOI: 10.1109/MedComNet52149.2021.9501247.

[33] Danish Syed, Muhammad, Nasir Arfa, Qureshi Hassaan, Khaliq, Ashfaq Ayesha, Binte, Mumtaz Shahid, and Rodriguez Jonathan. Network intrusion detection system for jamming attack in lorawan join procedure. *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, 2018. Retrieved from : DOI: 10.1109/ICC.2018.8422721.

[34] The top 10 iot use cases. Retrieved from https://iot-analytics.com/top-10-iot-use-cases/.

[35] Dimitrios Zorbas and Xenofon Fafoutis. Time-slotted lora networks: Design considerations, implementations, and perspectives. *IEEE Internet of Things Magazine*, 4(1):84–89, 2021. Retrieved from DOI:10.1109/IOTM.0001.2000072.