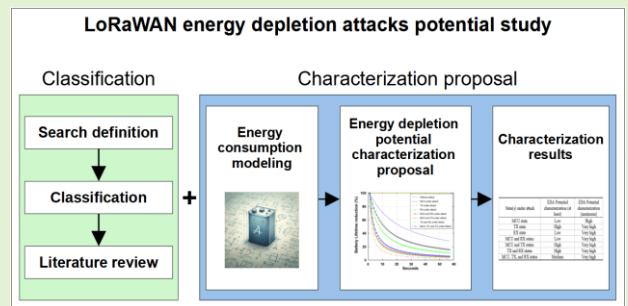


# Classification and characterization of LoRaWAN energy depletion attacks: A Review

André Proto, USP, Charles C. Miers, UDESC, and Tereza. C. M. B. Carvalho, USP

**Abstract**— Long Range Wide Area Network (LoRaWAN) is an Internet of Things (IoT) technology widely adopted by industrial, agriculture, and academic sectors. Despite its capability to provide low-power devices with extended battery life, secure communication, and cost-effectiveness, LoRaWAN has attracted significant attention due to its security concerns. A specific type of attack targeting sensors has emerged within this context, known as energy depletion attacks (EDAs). It aims to deplete the battery of sensors until they become unavailable, posing a potential threat to IoT networks and increasing infrastructure maintenance costs. A notable characteristic of EDAs is their tendency to stem from other types of attacks, such as flooding or jamming. Indeed, many attacks can elevate the energy consumption of an end device and deplete its battery. However, there is a research gap regarding the characterization of the potential impact of these attacks on a sensor's energy. This paper presents a novel characterization of EDAs in LoRaWAN networks using an emulation-based approach, providing insights for improving IoT security. Thus, our paper offers a classification of the most significant attacks associated with LoRaWAN, provides a summary of the current state-of-the-art energy consumption models, introduces a characterization of their potential to deplete the sensor's energy, and presents a comparative tabulation of the attacks in terms of their energy depletion potential. In addition, we provide a literature review of current defenses against EDAs in LoRaWAN, highlight the security gap concerning EDAs in LoRaWAN, and outline the open challenges for future research in this area.



**Index Terms**— LoRaWAN, energy depletion attacks, energy consumption model, characterization, DoS

## I. INTRODUCTION

THE Long Range Wide Area Network (LoRaWAN) is an emerging technology designed for efficiently communicating with Internet of Things (IoT) sensors across extensive distances while using minimal energy resources. LoRaWAN, an open-source technology, plays a pivotal role in the Low Power Wide Area Network (LPWAN) realm. LPWANs are foundational for connecting a wide range of battery-operated devices, facilitating seamless communication in the rapidly expanding IoT landscape. According to a report by Beecham Research [1], researchers view LPWAN as the key technology for mass-volume IoT applications, predicting it will constitute over 80% of IoT applications by 2026. The report further forecasts that LoRaWAN will be utilized by over 148.4 million IoT devices by 2027, representing over 25% of all LPWAN devices globally (excluding China).

LoRaWAN distinguishes itself by facilitating long-range

communication with minimal power consumption, making it an ideal solution for various applications. Whether deployed in smart cities, agricultural settings, or industrial environments, LoRaWAN provides a cost-effective, energy-efficient, and scalable platform for connecting diverse IoT devices. The protocol implements a star topology for communication, which allows sensors to communicate directly with a gateway, thereby streamlining the exchange of information. The star topology approach offers the advantages of simplifying communication, allowing extended battery life, and lowering device costs. Moreover, LoRaWAN offers wide communication ranges, compatibility with heterogeneous devices, and scalability to accommodate a growing number of connected devices.

With the substantial and swift expansion of LoRaWAN, industrial and academic research circles have paid attention to its security. Researchers have reported several types of attacks, such as jamming, bit flipping, eavesdropping, ACK spoofing, firmware manipulation, replay attacks, and others [2], [3]. Certain attacks, such as an Energy Depletion Attack (EDA), have the potential to deplete the energy of end devices until they become unavailable [4], [5]. An EDA can compromise a group of sensors, resulting in the unavailability of a portion or the entire network and escalating maintenance costs. In this case, the disruption of a LoRaWAN network could halt industrial processes, leading to production line errors that result in material losses [6]. Additionally, it could compromise agricultural monitoring in smart agriculture,

Manuscript received on 13 June 2024. Revised on 16 November 2024. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001 and Fundação de Apoio à Pesquisa do Estado de São Paulo (FAPESP) Grant Number: 2018/23097-3.

A. Proto and Tereza C. M. B. Carvalho are with Escola Politécnica de University of São Paulo (USP), São Paulo, Brazil (e-mail: andre.proto@usp.br, tereza.carvalho@usp.br).

Charles C. Miers is with Graduate Program in Applied Computing of Santa Catarina State University (UDESC), Santa Catarina, Brazil (e-mail: charles.miers@udesc.br).

where EDAs could lead to missed data from soil moisture sensors, affecting crop irrigation decisions and resulting in a severe economic loss [7], [8]. In addition, EDA can compromise battery-powered IoT healthcare devices [9], potentially disrupting patient monitoring and risking their lives.

EDAs have been recognized in Wireless Sensor Networks (WSNs) [10], [11]. Some of the known EDAs in WSNs include: denial-of-sleep, in which an attacker sends fake requests or control packages to keep a node awake [12]; flooding attack, in which an attacker increases the requests for packet transmission by a node using Denial-of-Service (DoS) techniques, demanding significantly more energy [13]; jamming attack, in which the attacker aims to disrupt IoT network communications by creating interference and cause packet collisions [14]; and, firmware modification, in which an attacker deploys malicious codes in a node to alter its behavior [15].

In the context of LoRaWAN, EDAs have been addressed recently, as it is a relatively new technology. Although the EDAs in LoRaWAN follow the same principles as EDAs for WSNs, they sometimes need to explore different vulnerabilities due to the unique characteristics of LoRaWAN. Some examples of attacks include jamming attacks, in which an attacker generates noise in the communication frequency when a communication is initiated, forcing the end devices to retransmit the packets and, consequently, waste more energy [5]. Another example is the sinkhole attack, in which an attacker compromises the transmission or reception of packets like acknowledgment packets, compelling sensors to retransmit their packets [3]. Other attacks, known as silent or ghost attacks [16], [17], can deplete the energy of sensors without generating network traffic, making their detection a challenging task. These attacks usually compromise an end device by exploiting a firmware or API vulnerability.

Often, the primary objective of the attacks listed above is not to deplete the sensor's battery. For example, jamming and sinkhole are originally DoS attacks, and an attacker might simply be trying to make network resources unavailable. Other DoS attacks, like replay and beacon synchronization, may also deplete the energy of sensors, although they have not yet been studied for this specific scope. Consequently, it is imperative to undertake a comprehensive study of these attacks to understand their behavior in the energy consumption of end devices and to establish robust countermeasures.

We aim to present an extensive study of attacks in LoRaWAN and their relationship to energy depletion. To achieve this, we classified the most relevant attacks in LoRaWAN based on literature surveys and proposed a method to characterize some of these attacks according to their energy depletion capacities. In summary, our paper presents:

- A literature review and a classification of the most relevant attacks in LoRaWAN.
- A summary of the most relevant state-of-the-art in energy consumption models for LoRaWAN.
- A method to characterize certain types of attacks based on their potential to deplete the energy of end devices.
- A comparison of some LoRaWAN attacks, focusing on the end device resources affected by each attack and

their potential to deplete energy.

- A literature review about the current defenses against EDAs in LoRaWAN, discussions about open challenges and future directions for this scope.

Our proposal is innovative because it explores a classification of LoRaWAN attacks with a focus on EDAs, presents a literature review of energy consumption models, and is the first paper to propose a survey that characterizes LoRaWAN attacks based on their energy depletion potential. Furthermore, this study can assist other researchers in addressing current gaps in this field.

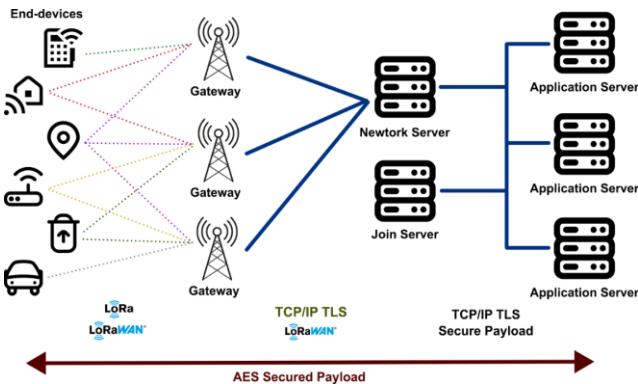
This paper is organized as follows: Section II introduces the concepts of LoRaWAN and discusses related security concerns. Section III presents a literature review of EDAs, describing the keywords for searching and classifying LoRaWAN attacks based on their aims. Section IV provides a summary of the state-of-the-art energy consumption modeling of end devices, introduces our method for characterizing the energy depletion potential of attacks, and discusses the results of this characterization. Section V presents and discusses the current defenses against LoRaWAN attacks with the potential to deplete the energy of end devices. Finally, Section VI presents our conclusions and identifies research gaps for future exploration.

## II. LORAWAN CONCEPTS AND ARCHITECTURE

The journey of LoRaWAN began in 2012 when Semtech acquired and patented the LoRa, a modulation technology developed for the physical layer [18]. Semtech created LoRa to operate on a sub-GHz frequency using Chirp Spread Spectrum (CSS) modulation, a technology widely used for sonar in the maritime industry and radar in aviation. Semtech also created the proprietary MAC protocol called LoRaMAC, which specifies the message formats and security layers for a true networking protocol. Later, in 2015, the LoRa Alliance was founded, and the LoRaWAN networking protocol was published.

LoRa technology usually operates at 915 MHz, 868 MHz, 433 MHz, or 430 MHz, depending on the region and regulations, providing communication up to 20 km outdoors [19]. A LoRa radio offers various configuration options to align with the application's requirements. One such option is the Spreading Factor (SF), which refers to the speed at which the signal frequency changes across the bandwidth and can be set between 7 and 12 [20]. This parameter controls the chirp rate and thus controls the speed of data transmission. Lower SF means faster chirps and, therefore, a higher transmission. Conversely, higher SFs lead to a lower data rate but provide greater communication range due to increased receiver sensitivity, however, with an increase in energy consumption. Another feature is the Adaptive Data Rate (ADR), a mechanism to control the following transmission parameters: SF, bandwidth, and transmission power [20]. Ochoa et al. [21] evaluated SF and other parameters in LoRa networks, showing that the suitable values depend on the environment.

LoRaWAN now implements several standards to support the MAC and network layer. To date, the LoRa Alliance has released several versions of LoRaWAN, the most recent being 1.0.4 (released in 2020) and 1.1 (released in 2017) [22].



**Fig. 1.** LoRaWAN architecture example in LoRaWAN 1.1. The end device communicates directly with gateways, forming a star topology. The network server manages the network by implementing security and control processes, the application server provides the applications that are used in the LoRaWAN network, and the join server manages the process used to add end devices to the network.

Essentially, LoRaWAN is a long-range star architecture in which the end devices communicate directly to the gateways, simplifying the communication process as illustrated in Fig. 1 [23]. Other components of this architecture include the network server and application server. The network server manages the network, filters redundant received packets, performs ADR, etc., while the application server implements and stores the application. In addition, the Join Server manages the over-the-air activation process used to add end devices to the network.

The standard defines three classes of end devices as follows:

### 1) Class A

This is the most energy-efficient class and must be supported by all devices. The downlink is available only after the end device transmits an information, when two receive windows are opened for a specific time [24].

### 2) Class B

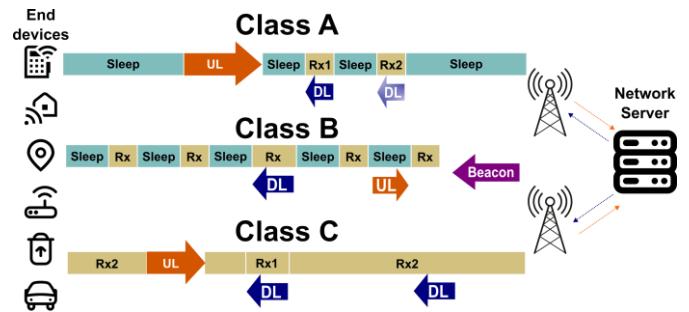
This class provides energy efficiency with latency-controlled downlink. The communication is divided into slots, and there is a requirement to open receive windows at fixed time intervals [24].

### 3) Class C

This class is recommended for devices which can afford to listen continuously. That means the network server can initiate the communication, avoiding latency for downlink communication [24].

**Fig. 2** depicts the difference between the Class A, B and C receive windows, in which downlink and uplink are represented as DL and UL respectively. LoRaWAN defines that the transmission slot scheduled by the end devices is based on its own communication. It needs a small variation based on a random time basis, as an ALOHA-type of protocol.

Concerning the energy efficiency of LoRaWAN, the existing literature predicts a battery lifetime of around 10 years for a battery-powered end device [25], [26]. These studies highlight that transmission activity is the primary contributor to the energy consumption of a device. Sherazi et al. [27] conducted a study on the energy efficiency of



**Fig. 2.** Comparison of receive windows for LoRaWAN communications in Class A, B, and C. Class A is the most energy efficient but has the largest downlink latency. Class B provides slot times, controlled by beacons, to allow the network server to transmit requests in fixed time periods. Class C allows end devices to listen to a connection continuously.

LoRaWAN that examined the average battery life of end devices, considering different transmission powers. The results presented by Sherazi et al. [27] indicated a battery life between 1 to 8 years for a sensing interval between 60 to 300 seconds and transmission power between -13dBm and -20dBm. This demonstrates that both transmission power and sensing interval affect the battery life of an end device, which are the primary targets for a successful EDA.

### A. LoRaWAN Security Concerns

LoRaWAN technology has addressed several security concerns since its first version [28]. Over the years, the LoRa Alliance has improved, as documented throughout the releases [24]. All LoRaWAN security is designed to adhere to principles such as low power consumption, low implementation complexity, low cost, and high scalability. The end devices and the LoRaWAN network establish mutual authentication as part of the network join procedure. There are two ways to authenticate an end device: Activation by Personalization (ABP) and Over-the-Air Activation (OTAA). ABP is a simplified commissioning process in which IDs and keys are personalized at fabrication. Although the devices become immediately functional upon powering up, they are tied to a specific network. OTAA implements a join procedure in which devices autonomously generate essential provisioning parameters. A device can store multiple "identities" to switch networks dynamically and securely, making it the preferred authentication method. LoRaWAN devices establish secure 128-bit AES connections for both end-to-end data with the application server and transportation data with the network server. Each payload is encrypted by AES with Counter mode (AES-CTR) and carries a frame counter and a Message Integrity Code (MIC) computed with AES Cipher-based Message Authentication Code (AES-CMAC) [28].

In Over-the-Air Activation (OTAA), a join server can be introduced to manage the join procedure of an end device. The join server contains the information required to process uplink *join-request* frames and generate downlink *join-accept* frames [20]. It generates the network and application session encryption key derivations and communicates the network session key (NwkSkey) of the new device to the network server, and the application session key (AppSKey) to the corresponding application server [29]. LoRaWAN 1.1

introduces the Join server to enhance the Join process. The Join process provides new keys like NwkSEncKey, SNwkSIntKey, and FNwkSIntKey, which are used for MAC command encryption and for checking message integrity [30]. This method ensures that neither the gateway nor the network server can read the user data. Fig. 3 illustrates secure communication among the end devices and network and application servers.

Despite efforts to provide a security protocol, some researchers have identified vulnerabilities that need to be addressed. Kuntke et al. in [7] presented an extensive survey about security issues of LoRaWAN in agricultural IoT scenarios, divided by physical attacks, message replay, eavesdropping, jamming attacks, spoofing attacks, and others. Alizadeh and Bidgoly [31] discussed the bit-flipping attack and proposed a deep-learning mechanism to detect it. Ruotsalainen et al. [32] reviewed physical layer-based attacks in LoRaWAN. Moraes and Conceição [33] conducted a systematic review of Security in LoRaWAN, providing a set of possible vulnerabilities and several papers that approach each.

None of the papers previously described have explored a study that illustrates the potential of LoRaWAN attacks to deplete the energy of end devices, as proposed in this paper.

### III. EXPLORING AND CLASSIFYING LORAWAN ATTACKS

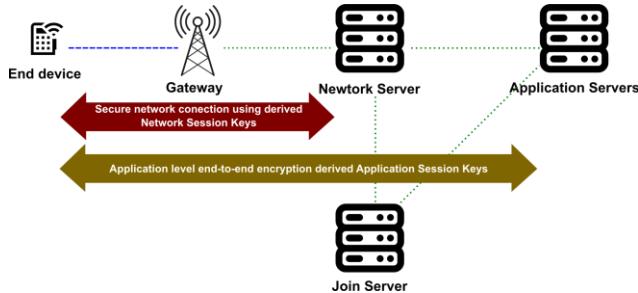
This section presents a literature review and classifies the most well-known attacks in LoRaWAN technology based on their shared aims. Several papers have classified these attacks based on various aspects such as type of technique, scope (end devices, gateway or network server), OSI layer, among others [3], [7], [32]. We summarize the main aspects of these classifications, leaving the details to the referenced papers.

#### A. Literature review search process

Initially, we conducted a search process to find the most relevant papers about the LoRaWAN attacks. The search process sought out reviews, surveys, systematic reviews, and similar works that review and classify attacks in LoRaWAN. This process unfolded in four steps:

##### 1) Search Query Definition

This step defines a search query based on the keywords *LoRa*, *LoRaWAN*, *LPWAN*, *security*, *attack*, *energy depletion*, and *battery exhaustion*. The proposed query is:



**Fig. 3.** Secure transmission of LoRaWAN. End devices communicate with Servers using different Session Keys [29]. The Network Server manages the entire network, dynamically controls transmission parameters to optimize network performance. The Join Server manages the OTAA process for end devices to be added to the network. The Application Servers are responsible for securely handling, managing and interpreting sensor application data.

(*LoRaWAN OR LoRa OR LPWAN*) AND (*security OR attack OR ((energy OR battery)* AND (*depletion OR exhaustion*)).

##### 2) Search Application

This step excludes duplicates and the following filters: the papers must be about surveys or literature reviews; the paper must be published between 2017 and 2024.

##### 3) Refine process

This step analyses the title, abstract and keywords to check if they contain the requested words defined before.

##### 4) Manual analysis

This step analyzes the full content papers, extracts and tabulates the attack definitions.

**TABLE I** presents the proposed search queries adjusted according to the database and the search process results among the steps. We conduct the search process in three databases: *IEEEExplore*, *ScienceDirect*, and *Web of Science*. During the process, steps 1 and 2 selected 57 papers. After step 3, our search process selected 27 papers. Finally, manual analysis in step 4 excluded 9 more papers that did not provide attack information in their content, resulting in 18 review papers that provide information and details about attacks in LoRaWAN.

#### B. Classification of LoRaWAN attacks

Our analysis summarizes 31 attacks in LoRaWAN discussed in the 18 selected papers. For a better discussion, this analysis classified the attacks into categories representing the common primary objectives of the attacks. The categories are defined as follows: DoS, Man-in-the-middle, Hijacking, Data corruption, Spoofing, and Multiple/Others. The subsequent list provides a summary of the categories and each one of the classified attacks. Fig. 4 illustrates the taxonomy resulting from the classification.

##### 1) Denial-of-Service attacks

Denial-of-Service (DoS) attacks aim to compromise a

**TABLE I**  
SEARCH PROCESS AND ITS RESULTS

Database	Search query	Qty (2)	Qty (3)	Qty (4)
IEEEExplore	( <i>LoRaWAN OR LoRa OR LPWAN</i> ) AND ( <i>security OR attack OR "energy depletion" OR "energy exhaustion" OR "battery depletion" OR "battery exhaustion</i> ) AND ( <i>survey OR "literature review" OR "comprehensive analysis" OR "comprehensive study"</i> )	36	16	10
ScienceDirect	( <i>LoRaWAN OR LoRa OR LPWAN</i> ) AND ( <i>security OR attack OR ((energy OR battery)</i> AND ( <i>depletion OR exhaustion</i> ))	3	3	3
Web of Science	(Topics): <i>lorawan security or lorawan attack or lora security or lora attack or lorawan energy depletion or lorawan energy exhaustion or lorawan battery depletion or lorawan battery exhaustion</i> (Document Types): Review Article	18	8	5

Databases request customizations in search query. The Qty (x), x={2,3,4} columns refers to quantities of papers resulted after steps 2, 3, and 4.

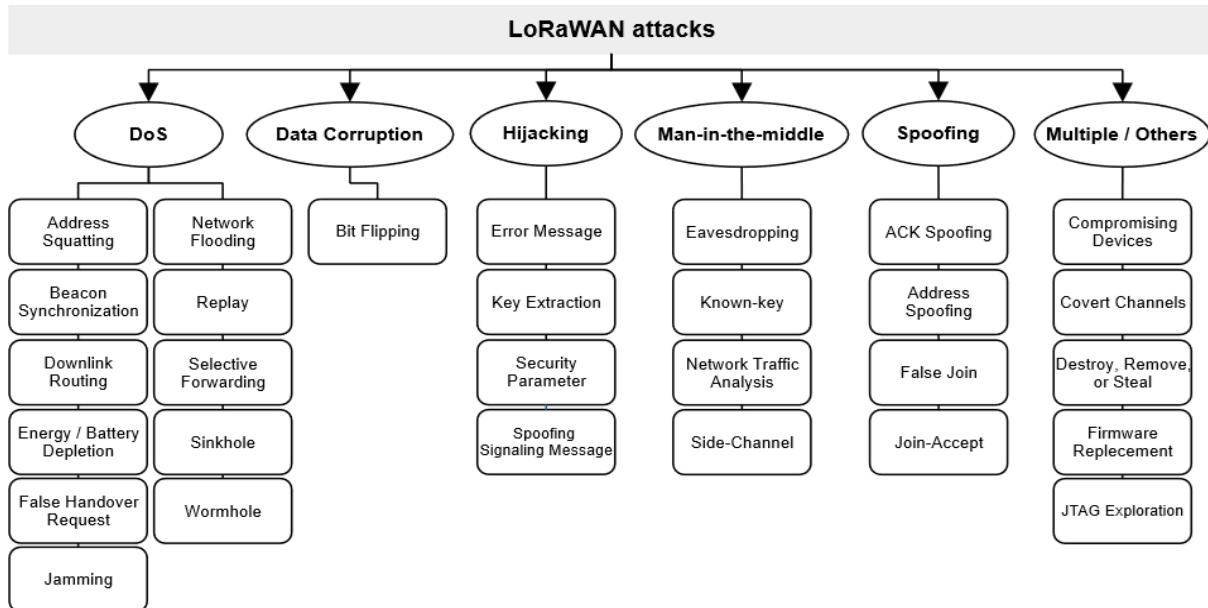


Fig. 4. A taxonomy for LoRaWAN attacks, whereas we defined categories that represent the type of attacks.

resource of sensors or an entire IoT network until it becomes unavailable. Such resources can be network, processing, or energy related. Several research studies have associated DoS attacks with different aspects, most of which are related to the network resources [34]–[40]. The following attacks have been appropriately classified as DoS:

- Address squatting: It prevents an end device from obtaining its genuine address [40]. This issue arises when an attacker predicts the address generation algorithm and subsequently claims ownership of a valid address.
- Beacon Synchronization: It broadcasts a malicious beacon with a high signal strength [2], [39], [41], [42] in a scenario in which a gateway sends beacon frames. The end devices receive the beacon and process it during the reception window, opening several unconfirmed receive windows, which can increase the likelihood of collisions between transmitted packets.
- Downlink routing: It occurs in a scenario with two or more gateways. An attacker eavesdrops on the transmission channel and replays an uplink message sent by an end device to a different network through a compromised gateway [2]. The Network Server validates the replayed packet and updates the downlink routing path to the gateway.
- Energy/Battery Depletion: It is predominantly characterized in the literature as an attempt by an attacker to force an end device to increase its transmission or retransmission, generate downlink packets, and overflow the reception stage. All these actions aim to deplete the energy of battery-powered end devices [32], [39].
- False handover request: It occurs when numerous end devices move towards the boundary of their home network coverage, triggering the mobility management process. At this point, the end devices move back towards the coverage of their home network, leading to a false handover request and consequently degrading performance on the network server [40].
- Jamming: It involves transmitting a radio signal at the

same frequency as an ongoing radio transmission to disrupt it [2], [32], [35], [36], [39], [42]–[44]. The literature enumerate four types of jamming: Constant Jammer, Deceptive Jammer, Random Jammer, and Reactive Jammer [2]. This attack is often used by others to achieve their objectives, such as the EDAs.

- Network flooding: In this attack, a compromised end-device is used to flood the network with packets, compromising the network's availability [2], [35].
- Replay: It involves an attacker intercepting the data transmitted in the network and then repeating or delaying it. This action enables the attacker to masquerade as a legitimate participant in the network [2], [34], [35], [37]–[39], [41], [42], [44], [45]. With several variants, replay attacks can be leveraged by other types of attacks to achieve their objectives.
- Selective forwarding: In this type of attack, an attacker compromises a gateway and selectively forwards packets, leading to network instability or unavailability [2].
- Sinkhole: This attack occurs in a scenario with multiple gateways. The attacker compromises a gateway, forces the end devices to use it for routing, and then drops the messages [2], [35].
- Wormhole: In this attack, the attacker positions a reactive jammer near a gateway. This compromises selected transmissions, emulating packet losses [32], [35], [39], [42], [44].

## 2) Data corruption attacks

This category aims to corrupt data transmitted by an end device or gateway, changing the payload. The only attack classified in this category is described below:

- Bit Flipping: It allows an attacker to alter a specific field in the ciphertext without decrypting it [2], [39], [41], [42], [45], [46]. It explores certain encryption modes in which both the plaintext and the ciphertext share the same bit order. In such cases, the attacker can manipulate the bits

in the ciphertext at the same position as in the plaintext.

### 3) Hijacking attacks

This category contains attacks related to hijacking connection sessions between end devices and gateway or network servers. In this literature review, the following attacks with this objective have been identified:

- Error message: It occurs when the mobility process started by an end device is interrupted without a signaling message indicating that the process must be canceled [40]. This allows an attacker to hijack the session that should be established between the visited network and an end device.
- Key Extraction: In this type of attack, an attacker is able to extract the *AppKey* from an end device, for example, by exploiting a vulnerability and using it to hijack the device [32], [34], [39].
- Security Parameter: An attacker with physical access to the end device can steal the reused keys [2], [42].
- Spoofing Signaling Message: Signaling messages contain commands to control communication and are used in the mobility management process. If an attacker succeeds in spoofing this message, it can assign the identity of an end node that wants to finish it. Thus, the attacker can take control over the end device session [40].

### 4) Man-in-the-middle attacks

The attacks that aim to listen and capture network communications secretly are considered main-in-the-middle (MITM) attacks. We identified in LoRaWAN literature the following attacks related to MITM:

- Eavesdropping: In this type of attack, the attacker captures a large amount of transmitted information and attempts to extract important information, such as the *AppKey* [32], [34]–[36], [41], [44], [45], [47]. Moreover, LoRaWAN uses AES-128 in counter mode to ensure message confidentiality. In ABP activation mode, the network and application keys are static, and only the counters are updated. However, when the counter overflows, its value will be reset, and consequently, the same keystream will be produced [2]. An attacker can exploit these behaviors to recover plaintext.
- Known-key: Any attack where the *AppKey* was discovered by the attacker, allowing the decryption of messages, can be considered a known-key attack [34].
- Network traffic analysis: An attacker with access to the LoRaWAN network can analyze the network traffic to trace patterns of communication and use such information for malicious purposes [2], [42], [44].
- Side-Channel attacks: In the OTAA phase, a single *AppKey*, which is not updated, is used throughout to compute the session keys. Although the session keys can be updated, the *AppKey* remains static [34]. Thus, an attacker that intercepted the *AppKey* employing side-channel attack techniques, such as timing information or electromagnetic leaks, can eavesdrop on the network.

### 5) Spoofing attacks

This category has attacks related to spoofing messages of end devices, gateways, and servers. The aim is to replace selected messages without hijack sessions. In this analysis, the following attacks have been classified as spoofing:

- ACK Spoofing: An attacker compromises a gateway and prevents certain messages from being transmitted and received [2], [39]. In this scenario, the compromised gateway blocks the ACK from reaching the end device. As a result, the end device sends another message to the network server, but this message is also blocked. The gateway then uses the last blocked ACK to deceive the end device into believing its message has been received.
- Address Spoofing: It is similar to the Address Squatting attack, but in this case, the attacker not only steals the address but also sends messages to other nodes that appear to come from the genuine node [40].
- False Join: The attacker spoofs packets that contain some parameters used by the join-procedure to simulate a false join in the network [2].
- Join-Accept: It occurs when an end device joins the network using OTAA and sends an uplink packet with application data within the security context [2], [41], [42]. An attacker can replay a join-accept message from the network server to the end device before it receives the authenticated confirmation from the network server.

### 6) Multiple / Others attacks

This category includes all other LoRaWAN attacks that cannot be classified under any other category described before or those which can be classified under multiple categories. They are described below:

- Compromising Devices: An attacker can compromise end devices by exploiting security vulnerabilities. For example, an attacker can expose the Universal Asynchronous Receiver/Transmitter (UART) serial lines between the Microcontroller Unit (MCU) and LoRa radio module [35], [39]. Using a special chip, it can interrupt, capture, and manipulate all the transactions between them, compromising the device.
- Covert Channels: It is a method to transmit sensitive information, such as secret keys, using a transmission medium that is often not intended for communication purposes [32]. In the case of LoRaWAN, an attacker can conceal a communication channel built on top of LoRa signaling. The key component of this method involves embedding amplitude modulation into a physical LoRa payload [48].
- Destroy, Remove, or Steal: Attackers with physical access to an end device can destroy, remove, or steal them. They can also attempt to extract the root keys implemented in end devices during fabrication or before deployment [2].
- Firmware Replacement: An attacker typically exploits a vulnerability in the firmware update process, such as over-the-air (OTA) updates, to implement malicious firmware [2], [49].
- JTAG Exploration: When an attacker, with access to physical end devices, accesses the JTAG interface. This

interface is used as a backdoor entry to access and exploit devices, leading to product malfunction and data modification [50].

#### IV. ENERGY DEPLETION POTENTIAL CHARACTERIZATION

The literature review reveals that attackers use diverse attacks to gain access to end devices and to execute malicious actions, such as to stress a device resource. In this context, it becomes crucial to understand the potential of certain attacks to deplete the energy of the end devices. To address this demand, this thesis proposes a characterization method to identify such potential.

Before discussing the method for characterizing this potential, Subsection IV-A provides a literature review of energy consumption modeling, which serves as the basis for this proposal. Subsequently, Subsection IV-B presents the proposed method for characterizing LoRaWAN attacks based on their potential to deplete the energy from end devices. Finally, Subsection IV-C encapsulates the results of this characterization.

##### A. Energy consumption modeling of end devices

Several papers have explored such subjects and provided good explanations about energy consumption of IoT devices [20], [25], [26], [49]–[57]. An end device can usually be in one of the following states:

- MCU State: The device is processing something.
- TX State: The device is sending something over the network.
- RX State: The device is actively listening or receiving data from the window.
- Sleep State: The device is in low-power mode.

Despite simplifying the states of end devices, analyzing their energy consumption has proven to be quite complex [26], [54]. This complexity arises from the various possible scenarios of IoT deployment, in which factors such as the number of end devices, transmission frequency, noise frequency, and others can vary. Furthermore, Singh, Puluckul, and Weyn [26] presented several substates of energy consumption in end-device activities. They classified the total energy expenditure of an end device as the sum of the energy spent in sleep mode ( $E_S$ ) and the energy spent in active mode ( $E_A$ ). Consequently, they outlined the following states of energy consumption in an LPWAN end device: *Device wakeup* (warming up the micro-controller and initializing the end device); *Sensor processing* (fetching the sensor value, which includes reading, parsing, and time activity); *Data processing* (processing the data and preparing package frame); *Transceiver pre-processing* (transmitting the packet to transceiver which includes activating radio for transmission mode); *Radio transmission* (using radio for packet transmission); *Wait/RX* (energy spent during the receive window); and *post processing* (energy spent to stop all the aforementioned activity) [26].

In another study, Casals et al. [54] defined eleven states of a Class A LoRaWAN end device, as presented in TABLE II. The states correspond to each step of the end device task,

**TABLE II**  
STATES AND VARIABLES OF ENERGY FOR LORAWAN TRANSMISSION [54]

State number	Description	Time spent in state	Current drawn
1	Wake up	$T_{wu}$	$I_{wu}$
2	Radio preparation	$T_{pre}$	$I_{pre}$
3	Transmission	$T_{tx}$	$I_{tx}$
4	Wait 1 <sup>st</sup> window	$T_{w1w}$	$I_{w1w}$
5	1 <sup>st</sup> receive window	$T_{rx1w}$	$I_{rx1w}$
6	Wait 2 <sup>nd</sup> window	$T_{w2w}$	$I_{w2w}$
7	2 <sup>nd</sup> receive window	$T_{rx2w}$	$I_{rx2w}$
8	Radio off	$T_{off}$	$I_{off}$
9	Postprocessing	$T_{post}$	$I_{post}$
10	Turn off sequence	$T_{seq}$	$I_{seq}$
11	Sleep	$T_{sleep}$	$I_{sleep}$

End devices spends a variable of time in each one of states, and every state has its own current drawn. The presented states belong to Class A LoRaWAN devices.

including wake up, radio preparation, transmission, 1st and 2nd receive window, radio off, postprocessing, turn off sequence, and sleep. Each state has its own time duration, which must be considered when calculating the current consumption. Thus, the authors proposed in (1) a calculation of the current consumption profile  $I_{avg\_unACK}$  of an end device in a LoRaWAN unacknowledged transmission. The  $T_{Notif}$  value represents the time between two consecutive periodic message transmissions performed by the end device,  $T_i$  and  $I_i$  are the time spent and the current drawn of a state  $i$ , respectively. Equation (2) was proposed to calculate the current consumption profile  $I_{avg\_ACK}$  of an end device during a LoRaWAN acknowledged transmission. The  $I_{act}$  and  $T_{act}$  values are the current drawn and time spent in any active states, whereas  $I_{sleep}$  value refers to the current drawn in sleep state. In this case, the ACK packet can be received in either the 1st or 2nd receive window, necessitating the inclusion of a probabilistic variable to calculate  $I_{act}$ . This is calculated using (3), in which  $MAX\_RETR$  denotes the maximum number of message retransmissions,  $E[I_k]$  represents the expected current consumption of an end device when it has performed  $k$  data message retransmissions, and  $p_k$  indicates the probability that the end device performs such retransmissions. Lastly, the authors calculated the lifetime  $T_{lifetime}$  of an end device using (4), as for both unacknowledged and acknowledged transmissions ( $I_{avg}$ ) [51], [54]. Here,  $C_{battery}$  represents the battery capacity expressed in mAh.

$$I_{avg\_unACK} = \frac{1}{T_{Notif}} \cdot \sum_{i=1}^{N_{states}} T_i \cdot I_i \quad (1)$$

$$I_{avg\_ACK} = \frac{I_{act} \cdot T_{act} + I_{sleep} \cdot (T_{Notif} - T_{act})}{T_{Notif}} \quad (2)$$

$$I_{act} = \sum_{k=0}^{MAX\_RETR} E[I_k] \cdot p_k \quad (3)$$

$$T_{lifetime} = \frac{C_{battery}}{I_{avg}} \quad (4)$$

**TABLE III**  
MAIN CURRENT DRAWN DETAILS FOR SLEEP, TX AND RX STATES ON  
LoRa/LORAWAN TRANSCIEVERS [54]

Transceiver	Sleep	TX	RX
Semtech SX1272	0.1 $\mu$ A (max. 1 $\mu$ A)	Min.: 18 mA Max.: 125 mA	10.5 or 11.2 mA
Semtech SX1276	0.2 $\mu$ A (max. 1 $\mu$ A)	Min.: 20 mA Max.: 120 mA	10.8, 11.5 or 12.0 mA
HopeRF HM-TRLR-LF/HFS	2 $\mu$ A (min. 1.2 $\mu$ A, max. 3 $\mu$ A)	Min.: 35 mA Max.: 120 mA	16 mA (min. 15 mA, max. 18 mA)
Microchip RN2483	Up to 100-150 $\mu$ A	Min.: 17.3 mA Max.: 38.9 mA	14.2 mA

The energy consumption reference given by microcontroller datasheets for Sleep, TX and RX states.

In the same paper, Casals et al. presented a summary of the expected energy consumption of four LoRa/LoRaWAN transceivers, as shown in TABLE III, based on their datasheets [54]. Typically, every IoT sensor consumes most of its energy in TX state, followed by the RX state to a lesser extent. However, the data compiled in TABLE III indicates that the RX state can contribute significantly to the expected energy consumption of an end device, depending on the scenario. For example, Semtech SX1272 transceiver has a minimum of 18mA in the TX state and a maximum of 11.2mA in the RX state. Consider a scenario in which the IoT application requires low transmission but high reception data from servers, the RX state would be responsible for the highest energy consumption over the lifetime of the sensor. According to TABLE III, other transceivers may exhibit this behavior if they consume the minimum energy in the TX state and the maximum in the RX state. Furthermore, in the same scenario, any EDA that amplifies the RX activity in an end device will significantly alter its expected energy consumption. Consequently, this could potentially shorten the battery life of the end device.

In another study, Kuaban et al. in [56] conducted an extensive study on modeling EDAs for battery-powered IoT devices. In addition to describing the lifetime prediction equation similar to (4), the authors presented equations to calculate the probability of the amount of energy present in the battery at time  $t$  in (5) and the probability that the battery is empty at time  $t$  in (6). These equations are based on Markovian model, in which  $P_D$  represents the energy consumption per unit time,  $B$  is the full capacity of the battery, and  $n$  is the number of energy units present in the battery.

$$P_n(t) = \frac{(P_D \cdot t)^{B-n}}{(B-n)!} \cdot e^{-P_D t}, \quad 0 < n \leq B \quad (5)$$

$$P_0(t) = 1 - \sum_{n=1}^B \frac{(P_D \cdot t)^{B-n}}{(B-n)!} e^{-P_D t} \quad (6)$$

For EDA analysis, the mathematical constructions must be based on the techniques used in the attacks. For instance, consider a scenario in which an attacker crafts bogus packets and sends them to the victim device, forcing its energy consumption to receive the packets and perform security checks (e.g., access control, message integrity checks, and

decryption) [56]. In this case, the energy consumed by the microcontroller during the process of receiving the packet and executing the security algorithms to perform the security checks is described in (7). Here,  $T_{dec}$  is the time required to perform the security checks,  $T_{rx}$  is the time required to receive a packet,  $P_{MCU}^a$  and  $P_{MCU}^i$  represent the power drawn by a microcontroller unit in active and idle mode, respectively, and  $N_r$  is the number of received packets. Also, the energy consumed by the radio module in receiving both the normal and attack packets within a given active period is described in (8), in which  $P_{rx}$  represents the power required to receive a single packet, and  $\tau$  represents the duration of the active period.

$$E_{comp}^{rx} = N_r \cdot (T_{dec} \cdot P_{MCU}^a + T_{rx} \cdot P_{MCU}^i) \quad (7)$$

$$E_{rx} = \begin{cases} N_r \cdot (T_{dec} + T_{rx}) \cdot P_{rx}, & N_r \cdot (T_{dec} + T_{rx}) \geq \tau \\ \tau \cdot P_{rx}, & \text{otherwise} \end{cases} \quad (8)$$

Similarly, consider a scenario in which an attacker compromises an IoT device and then reconfigures it to perform more sensing operations than usual. The extra packets generated by the additional measurement will consume more energy for sensing, encryption, and transmission. In this case, the energy consumed by the MCU in performing cryptographic operations and transmitting data is given by (9). Furthermore, the amounts of energy consumed by the radio module in the transmission of both normal and attack packets within an active period are given by (10). In these equations,  $T_{enc}$  is the time required to encrypt a packet,  $T_{tx}$  is the time required to transmit a packet,  $N_t$  is the number of transmissions,  $\eta$  is the conversion factor of the power amplifier, and  $P_0$  is the electronic power consumption overhead.

$$E_{comp}^{tx} = N_t \cdot (T_{enc} \cdot P_{MCU}^a + T_{tx} \cdot P_{MCU}^i) \quad (9)$$

$$E_{tx} = \begin{cases} N_t \cdot (\eta P_t + P_0)(T_{enc} + T_{tx}), & N_t \cdot (T_{enc} + T_{tx}) \geq \tau \\ \tau \cdot (\eta P_t + P_0), & \text{otherwise} \end{cases} \quad (10)$$

As observed in (7) and (9), the encryption and decryption operations of the MCU play a key role in its energy consumption. Several studies in the literature have evaluated these operations from various aspects, including energy consumption [60]–[62]. Khalifeh et al. [60] presented a review of MCUs for WSNs, providing a comparison of their resources in terms of CPU, RAM, flash, EEPROM, and common radio transceivers. The authors also compared the expected energy consumption of MCUs, based on their datasheets. In their study, three MCUs that use LoRa transceivers were presented: MSP430FR5969 [63], Arm Cortex-M4 MCU (CC3220MODASF12) [64], and Arm cortex M0+ (SAMD21) [65]. TABLE IV presents a summary of key information about these MCUs, including frequency, RAM, and current drawn [60].

Furthermore, Kane et al. [61] presented a comparative study of the time and energy cost for AES encryption and decryption

**TABLE IV**  
COMPARATIVE RESOURCES AND CURRENT DRAW OF MCUs [60]

MCU	Clock Freq. (MHz)	RAM	Current drawn (Active)	Current drawn (Sleep)
MSP430FR5969	16	64 kB non-volatile FRAM	103 $\mu$ A/MHz	0.25 $\mu$ A
ARM Cortex-M4 MCU	80	256kB	229 mA	250 $\mu$ A (LPDS), 4 $\mu$ A (.hibernate)
Arm Cortex M0+	48	32kB SRAM	~7 mA	~12.8 $\mu$ A

According to the datasheet, the ARM Cortex-M4 MCU (CC3220MODASF12) includes a Wi-Fi module, and its current drawn in active mode includes data transmission.

operations, including in Counter mode (CTR) used by LoRa. Although the study did not perform tests on MCUs used in LoRa devices, the results show that encryption and decryption operations have similar time and energy costs, with decryption operations consuming slightly more time and energy. This is confirmed by Thaenkaew, Quoitin, and Meddahi [62], who presented an evaluation of the cost beyond AES-128 LoRaWAN security. They demonstrated that the time and energy cost of AES-128 increases almost linearly for different payload sizes. Based on an experimental setup using Arm Cortex-M0+, they observed that, in a scenario that uses SF7 spreading factor with 500 kHz bandwidth, the time dedicated to payload encryption represents only 2.5% of the transmission time. In addition, the MCU spends a similar cost for MIC calculations, totaling approximately 5% of time cost.

In addition, some state-of-the-art papers have improved the energy modeling study. Sanchez-Vital et al. [51] modeled and evaluated the energy performance of the Long-Range Frequency Hopping Spread Spectrum (LR-FHSS), an advancement in the LoRaWAN protocol to enhance the network's capacity. Yazid et al. [52] included the distance parameter in their study of energy modeling and provided an algorithm to regulate the optimal transmission parameters. Ghaderi and Amiri [59] presented a comprehensive model for the end device energy consumption that evaluates the impact of different parameters like SR, bandwidth, bit rate, and payload size. Lastly, Correia, Alencar, and Assis [57] presented a stochastic modeling that could assess the probability range of energy consumed by end devices.

## B. Energy depletion potential characterization proposal

The literature review of Subsection III-B revealed that several of the described attacks use similar techniques to achieve their goals despite the differences in their objectives. For instance, replay attacks uses techniques also applied in several other attacks, such as downlink routing and join-accept. Other attacks, such as Key Extraction, Security Parameter, Compromising Node, JTAG Exploration, and Firmware Replacement, are based on gaining access to an end device through vulnerabilities of physical access to achieve their aim. Although similar techniques are used, we have classified these attacks into different categories based on their different objectives.

Considering the given scenario, we have opted to select only those categories that share similar objectives to EDAs. First, the Denial-of-Service category has been selected for this work as it has the same objectives as EDAs. In addition, this work has chosen the Multiple/Other category, given that the attacks within this category enable an attacker to achieve several goals, including Denial of Service and EDAs.

Subsequently, Subsection IV-A summarized the following key insights related to the energy consumption of LoRaWAN end devices:

- The energy consumption of an end device is linked to the interplay among its states (MCU, TX, and RX), which often operate simultaneously.
- The duration spent in each state also impacts the energy consumption.
- The power consumption ratio between RX and TX states can range between 5% and 60%, depending on the IoT scenarios (refer to Table III).

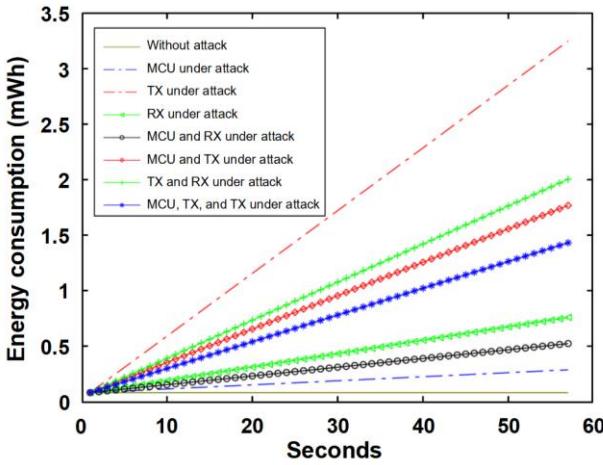
Due to the complexity and diversity of IoT scenarios, we opted to simplify the characterization by proposing five categories: very low, low, medium, high, and very high potentials. Accordingly, the characterization method examines the potential of an attack to increase the three main states of an end device both individually and collectively. This allowed us to study the impact of each of the MCU, TX, and RX states on energy consumption.

To simplify the calculations, we propose an emulation with the following parameters: states 1, 2, 8, 9, and 10 of TABLE II are classified as MCU tasks, state 3 is classified as a TX task, and states 4, 5, 6, and 7 are classified as RX tasks. In addition, we set  $T_{Notif} = 1$  in (1). Furthermore,  $T_{mcu}$  represents the time that the end device spends in MCU state,  $T_{tx}$  represents the time spent in TX state,  $T_{rx}$  represents the time spent in RX states, and  $T_{idle}$  represents the idle time. Consequently, we can propose (11) to calculate the average energy consumption of an end device in a cycle of activities for a LoRaWAN Class A end device, in which  $V$  is the battery voltage.

$$E_{I_{avg}} = V \cdot (T_{mcu} \cdot I_{mcu} + T_{tx} \cdot I_{tx} + T_{rx} \cdot I_{rx} + T_{idle} \cdot I_{idle}) \quad (11)$$

Based on the information provided in Table III, we calculated the average current drawn of the TX state by considering both the minimum and maximum values, which resulted in approximately 61.7 mA. Similarly, the average current drawn of the RX state was found to be 13.2 mA. In addition, based on the data in TABLE IV and excluding the ARM Cortex-M4 MCU due to its Wi-Fi module, the average energy consumption in the MCU state was determined to be 4 mA. This calculation considers the average of the clock frequency multiplied by the average energy consumption per clock cycle.

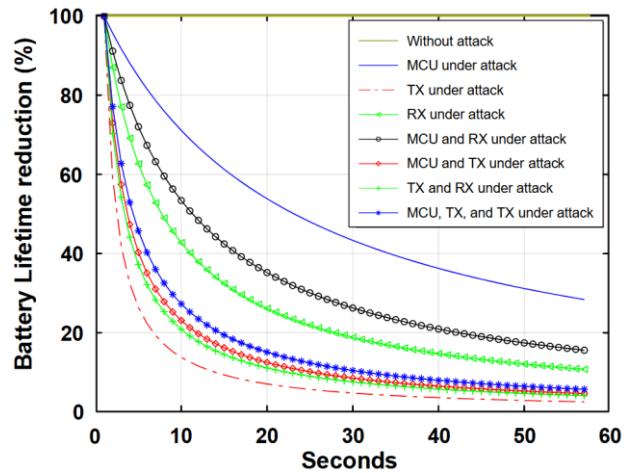
Based on the previous values, Fig. 5 presents a comparison for the energy consumption of various combinations of end device states under attack in a typical scenario in which the end device transmits data every minute. In this case, we set  $T_{tx}=1s$ ,  $T_{rx}=2s$ , with the latter already including the two receive windows. We also set  $T_{mcu} = 0.1s$ , considering that the average time of the MCU state in a transmission is 5% of the time of



**Fig. 5.** Experimental end device states under attack and their effects in energy consumption of the device.

TX state, as observed in [62], but this is doubled due to the MCU processing for transmitted and received data. Finally, we set  $T_{idle} = 56.9s$ , which represents the remainder of the one-minute cycle. In this scenario, the energy consumed by the end device is approximately  $0.0813mWh$  when it is powered by a 3.3V battery. If an attacker manipulates an end device to force it to execute a specific state or a combination of states during the idle time  $T_{idle}$ , then the energy consumption of the end device will be as presented in Fig. 5. The graph shows the MCU state occupying between  $0.1s$  and  $56.9s$ , or  $T_{mcu} < T_{mcu}' < T_{idle}$ , of the end device time cycle and its energy consumption, as well as for TX and RX states, individually. This analysis also considers scenarios where two states are under attack, with each one occupying half of the idle time. In addition, when MCU, TX and RX states are under attack together, each state occupies one third of  $T_{idle}$ . TABLE V provides a summary of the intervals for each emulated scenario.

The primary objective of every EDA has as its main objective to reduce the battery lifetime of end devices. To illustrate this, Fig. 6 shows the reduction in battery lifetime under the same end device states under attack as shown in Fig. 5, using the same simulated parameters. This analysis compares the attack state combinations with a scenario without any attack. Although Fig. 5 shows a significant difference in energy consumption among end device states under attack, Fig. 6 reveals that even the least effective attack, which targets the MCU state, has the potential to reduce the



**Fig. 6.** Battery Lifetime reduction for each one of experimental attacks in the mainly end device states.

battery lifetime by up to 40% in the worst-case scenario, when the MCU occupies all idle time. Therefore, the characterization strategy is based on the reduction of battery lifetime, and five categories are defined according to the following list:

- Very low: Reduces the battery lifetime by up to 20%.
- Low: Reduces the battery lifetime from 20% to 40%.
- Medium: Reduces the battery lifetime from 40% to 60%.
- High: Reduces the battery lifetime from 60% to 80%.
- Very high: Reduces the battery lifetime from 80% to 100%.

Despite the clarity and objectivity of the definition, characterizing device states under attack is challenging because it depends on how much an attack activates different states. Indeed, while the emulation operates within a theoretical realm, a real EDA or other kind of real attack could potentially trigger thousands of different state activations. However, the key point is that regardless of the impacts of an attack on the energy consumption of end devices, the results of the proposed emulation show that even a slight increase in state activity, whether isolated or combined, can significantly reduce the battery lifetime. Furthermore, an increase in TX activity will maximize the energy consumption, followed by RX activity with medium consumption, and finally, the MCU activity with the least consumption. Even in a combination of these activities, the larger or smaller proportion of each activity will impact the energy consumption in the same ratio.

Lastly, TABLE VI presents the characterization method applied in the emulated scenario. This table provides an interval of potential for the combination of end device states

TABLE V

EMULATED ATTACKS AND THE RANGE OF ACTIVE TIME IN STATES

State(s) under attack	Range of time
MCU state	$T_{mcu} < T_{mcu}' < T_{idle}$
TX state	$T_{tx} < T_{tx}' < T_{idle}$
RX state	$T_{rx} < T_{rx}' < T_{idle}$
MCU and RX states	$T_{mcu} < T_{mcu}' < T_{idle}/2$ , $T_{rx} < T_{rx}' < T_{idle}/2$
MCU and TX states	$T_{mcu} < T_{mcu}' < T_{idle}/2$ , $T_{tx} < T_{tx}' < T_{idle}/2$
TX and RX states	$T_{tx} < T_{tx}' < T_{idle}/2$ , $T_{rx} < T_{rx}' < T_{idle}/2$
MCU, TX, and RX states	$T_{mcu} < T_{mcu}' < T_{idle}/3$ , $T_{tx} < T_{tx}' < T_{idle}/3$ , $T_{rx} < T_{rx}' < T_{idle}/3$

TABLE VI

EDA POTENTIAL CHARACTERIZATION FOR EXPERIMENTAL STATES UNDER ATTACK

State(s) under attack	EDA Potential characterization (at least)	EDA Potential characterization (maximum)
MCU state	Low	High
TX state	High	Very high
RX state	Low	Very high
MCU and RX states	Low	Very high
MCU and TX states	High	Very high
TX and RX states	High	Very high
MCU, TX, and RX states	Medium	Very high

under attack, to account for the volatility of energy consumption across different time units. However, this analysis excludes the first 10% of the time unit (approximately 6 seconds), considering that any EDA or other DoS attacks would likely compel end device activities to exceed this rate. According to TABLE VI, light EDAs are those attacks that activate only MCU state, with potential ranging from Low to High. Conversely, heavy EDAs are attacks that maximize the activation of the TX state.

### C. Characterization results

This subsection provides an analysis of the primary end device states that each attack in the DoS and Others/Multiples categories could potentially increase their activities. Consequently, it presents a possible EDA potential characterization for these attacks, based on the discussion from the previous subsection.

For this proposal, we revisited the selected papers and surveys in Subsection III.A. Following that, we conducted a literature review for each of these papers in search of the characteristics of the attacks and the end device states they could potentially affect. Consequently, the characterization method is applied in each attack, based on the results of this search.

TABLE VII presents a summary of the selected papers included in the surveys, along with their potential to alter the activity of the following main states: MCU state, TX state, and RX state. The observations show that almost all attacks potentially affect multiple states simultaneously. However, the selected papers did not provide a specific study of the extent of increase in each activity. Consequently, we characterized the EDA potential of the attacks in the same manner as the analysis applied in TABLE VI. This provides a starting point for understanding the potential of known attacks to achieve the objectives like those of EDAs. We provided below the detailed descriptions for the analyzed attacks:

- Address Squatting:** This attack does not affect any states in the end device, as it primarily aims to prevent an end device from obtaining its link layer identity or network address [40]. Therefore, it is characterized as having a very

low potential for energy depletion.

- Beacon Synchronization:** This attack involves an attacker generating fake beacons at a high frequency to be received and processed by end devices [3], [66]–[69]. It impacts both the MCU and RX states. Therefore, it is characterized as having a potential for energy depletion ranging from Low to Very High.
- Compromising devices:** This attack can manifest in several ways, potentially affecting only the MCU state, or the MCU and RX states, or the MCU and TX states. In the latter scenario, the attacker can compromise the network keys and send data [70], [71]. Given these possibilities, the potential characterization for energy depletion can range from Low (only affecting the MCU state) to Very High (affecting both the MCU and TX states).
- Covert Channel:** This attack does not affect the transmission time of an end device, but it can impact the power of transmission due to the need to alter the signal amplitude [48]. This attack requires further investigation as its effects on energy consumption have not yet been analyzed. For this reason, it is characterized as having a potential for energy depletion ranging from Very Low to Very High.
- Destroy, Remove, or Steal:** As described in [72], this is a physical attack that could render the end device unavailable, but not through altering the end device states. In this scenario, the states are not affected. Therefore, it is characterized as having a Very Low potential for energy depletion.
- Downlink Routing:** This attack aims to affect the routing path between the gateway and the Network Server [67]. Based solely on the objectives of the attack, we do not observe any changing in the states of the end device. Therefore, it is characterized as having a Very Low potential for energy depletion.
- Energy / Battery Depletion:** According to [3] and [5], there are numerous techniques to directly cause battery depletion, which involve the MCU, TX, or RX states. Although this type of attack is the focus of our study, the variety of techniques means that the efficiency of the attack can quite range. Therefore, it is characterized as

TABLE VII  
SELECTED LoRAWAN ATTACKS AND THEIR ENERGY DEPLETION POTENTIAL

Attack	Category	References	End device States affected	EDA Potential characterization (at least)	EDA Potential characterization (maximum)
Address Squatting	DoS	[40]	None	Very low	Very low
Beacon Synchronization	DoS	[3], [66]–[69]	MCU and RX	Low	Very high
Compromising Devices	Multiple / Others	[70], [71]	MCU, TX or RX	Medium	Very high
Covert Channels	Multiple / Others	[48]	TX	Very low	Very high
Destroy, Remove or Steal ED	Multiple / Others	[72]	None	Very low	Very low
Downlink Routing	DoS	[67]	None	Very low	Very low
Energy / Battery Depletion	DoS	[3], [5]	MCU, TX or RX	Low	Very high
False Handover Request	DoS	[40], [73]	None	Very low	Very low
Firmware Replacement	Multiple / Others	[49], [71], [72], [74], [75]	MCU, TX or RX	Low	Very high
Jammer	DoS	[71], [76]–[81]	TX	Very high	Very high
JTAG Exploration	Multiple / Others	[50], [82], [83]	MCU, TX or RX	Low	Very high
Network Flooding	DoS	[72]	MCU and RX, or TX	Low	Very high
Replay	DoS	[84]–[86]	MCU and RX	Low	Very high
Selective Forwarding	DoS	[72]	TX*	Very low*	Very high
Sinkhole	DoS	[72], [87]	None	Very low	Very low
Wormhole	DoS	[32], [78], [88]	TX	Very low	Very high

\* Depends on ACK enabled by Network Server.

- having a potential for energy depletion ranging from Low to Very High.
- **False Handover Request:** The primary outcome of this attack is network server degradation and the end devices are not affected directly [40], [73]. Therefore, it is characterized as having a Very low potential for energy depletion.
  - **Firmware Replacement:** Unlike the previous attacks, this one can inject malicious code to achieve several objectives, including energy depletion [49], [71], [72], [74], [75]. With full control over the firmware, this attack can affect any of the end device states, including combinations of them. Therefore, it is characterized as having the potential for energy depletion ranging from Low, in a scenario where only the MCU state is compromised, to Very High, in a scenario where the TX state is affected, either alone or in combination with other states.
  - **Jamming:** The techniques used in this type of attack are commonly employed by energy depletion attacks, as they lead to an increase in TX activity due to retransmissions [71], [76]–[81]. As such, it is characterized as having a Very High potential for energy depletion.
  - **JTAG Exploration:** This attack is quite similar to Firmware Replacement, as it allows the attacker to access and modify the firmware or bootloader of the end device [50], [82], [83]. This access enables the implementation of malicious code. Therefore, it is characterized in the same way, with a potential for energy depletion ranging from Low to Very High.
  - **Network flooding:** In this type of attack, an end device compromised by an attacker is used to perform network flooding, which increases the TX state. For the target, either the MCU or RX state can be increased [72]. Therefore, it is characterized as having a potential for energy depletion ranging from Low to Very High.
  - **Replay:** This type of attack can be used for several purposes [84]–[86]. One scenario that can increase end device activity is when the replay attack is used to flood an end device, leading to an increase in the MCU and RX states [2]. Therefore, it is characterized as having a potential for energy depletion ranging from Low to Very High.
  - **Selective forwarding:** As a routing attack, its primary goal is usually to tamper with the gateways or routing paths [72], which affects the connectivity of end devices. In this context, the only way to increase energy consumption is when the ACK is activated, forcing the end device to retransmit packets and thereby increasing the TX state. Taking this scenario into account, it is characterized as having a potential for energy depletion ranging from Very Low (without ACK) to Very High (with ACK).
  - **Sinkhole:** This type of attack compromises routing for all end devices [72], [87], potentially leading to a complete network shutdown. In this scenario, the end devices would be disconnected, even denying the retransmission mechanism. Consequently, no states are affected. Therefore, it is characterized as having a Very Low potential for energy depletion.

• **Wormhole:** As described in [32], this type of attack blocks payloads with even the lowest spreading factor and replays them later on [78], [88]. Since it manipulates metadata, it can compel end devices to set a higher spreading factor and transmission power, thereby increasing TX activity. Despite this, the transmission time remains unchanged, with only the transmission power being affected. This aspect requires further investigation. Therefore, we characterize this attack similarly to the Covert Channel, with a potential for energy depletion ranging from Very Low to Very High.

In summary, eleven out of the sixteen analyzed attacks have presented the potential to deplete the energy of end devices. Among these, three have at least a medium potential or higher. This indicates that EDAs and various LoRaWAN attacks are closely related, and the defenses against them need to be strategically designed in tandem.

## V. CURRENT DEFENSES AGAINST EDAS

Drawing on the characterization presented in Table VII, this section offers a literature review of the existing defenses against LoRaWAN attacks, which have been characterized as having at least a low potential to deplete the energy of end devices. It also provides some discussion about the research gap of defenses against EDAs.

### A. Literature review

To begin with, current defenses against Beacon Synchronization usually mitigate the attack, by using Message Integrity Code (MIC) or cryptographic signature instead of the Cyclic Redundancy Check (CRC) of the physical layer [2], [39].

In another study, Chen, Ben-Othman, and Mokdad [89] proposed a detection method against compromising devices attack based on analysis of power greedy behavior with machine learning algorithms. Halder and Newe [90] proposed a distributed anomaly-based IDS, based on fingerprints of carrier frequency offset of end devices. Qadir et al. [91] presented a new key generation and distribution (KGD) mechanism that securely exchanges the root key between the end device and the application server.

Conversely, Hou, Xia and Zheng [48] suggested a detection method against Covert Channels based on enhancements in LoRa nodes that examine amplitude changes in the CSS demodulation process, whereas Shen et al. [92] suggested the use of machine learning in transmission signal data to detect this type of attack.

On a different note, Saxena, Pandey, and Kumar [93] proposed a detection method of energy / battery depletion attack derived from RSS attacks, with consists of a Geometric-Arithmetic (GM–AM) ratio in which GM follows strictly Schur-Concavity property and AM follows non-strict concavity property, whereas Suciu et al. [94] implemented authentication pREAMbles to limit attacker options when forcing nodes to overhear class B beacons.

In addition, Mao et al. [95] proposed a defense against Firmware Replacement attack, which uses the channel activity detection (CAD) to detect negative acknowledgments

(NACKs). Anastasiou et al. [96] proposed a blockchain-based framework to securely update the firmware of IoT devices, whereas Malumbres et al. [97] proposed the use of secure broadcast methods to update firmware among devices.

On the other hand, current defenses against jamming attacks usually analyze the Received Signal Strength Indicator (RSSI) or transmission power. Kalokidou, Nair, and Beach [98] proposed a detection scheme based on previous values of RSSI. Bleszynski, Orfanidis, and Fafoutis [99] provided an analysis of the variability of the signal strength as a first step and then examined the entropy of the received data to detect a potential jammer. Hou, Xia, and Zheng [79] presented a method that can separate LoRa chirps from jamming chirps by leveraging their difference in the received signal strength. Monjur and Yu [100] compared the incoming signal from a LoRa node with a predefined sync symbol through a continuous monitoring framework. Haque and Saifullah [101] proposed to mitigate jamming by recovering interfered physical layer samples, known as collision recovery.

Furthermore, Vishwakarma and Lee [50] suggested the implementation of physical unclonable functions, public key cryptography, challenge-response implementation, and others against JTAG exploration.

In another study, Noura et al. [2] recommended the use of LoRaWAN v1.1 against network flooding attack, whereas Ogbodo, Abu-Mahfouz, and Kurien [35] suggested the use of firewalls and network monitoring.

In a separate study, Huan et al. [102] presented mitigation against replay attack based on a wireless key generation approach named Kerra which integrates a synchronized time measurement, whereas Noura et al. [103] proposed two variants of dynamic key derivation for ABP devices: counter-based and channel information-based.

Meanwhile, Locatelli, Spadaccino, and Cuomo [104] provided a detection method against selective forwarding attack that analyzes the timestamps in which the uplinks are received by the gateways.

Finally, Ogbodo, Abu-Mahfouz, and Kurien [35] suggested the use of end-to-end encryption against wormhole attack, whereas Stanco et al. [39] suggested the use of a low spreading factor to decrease the airtime of a message, beating the time it takes for the sniffer to reach the jammer.

## B. Discussion

A brief analysis of current defenses reveals that they are specifically tailored to their respective attack targets, implying that the proposed solutions are designed to counter single attacks. Furthermore, within the realm of detection solutions, all of them employ signal, RSSI, or traffic analysis, which are all network parameters. Consequently, such methods are not effective against silent attacks. Even the solutions against Compromising Device attack, which form the basis for silent attacks, also rely on the RSSI network parameter.

Several studies have explored techniques to improve firmware updates for end devices [97], [105]. These techniques have enabled fast updates with minimal downtime, thereby facilitating the process. This evolution necessitates extensive research to enhance the security of the process, for instance by applying blockchain techniques, aiming to avoid or mitigate vulnerabilities that could compromise end devices.

Furthermore, the ADR mechanism can be utilized to optimize power consumption during attacks such as jamming by dynamically adjusting transmission parameters based on environmental conditions. Future research should delve deeper into the impact of ADR on EDAs, assessing the extent to which ADR mitigates these threats.

Finally, attackers may orchestrate various LoRaWAN attacks to deplete the energy of end devices. Furthermore, they could exploit unknown vulnerabilities to achieve this goal, effectively bypassing current defenses. Although it is feasible to propose an integrated solution that simultaneously applies multiple defenses, such a solution would likely incur significant costs in terms of processing, memory, and energy resources for constrained devices. Additionally, there are no guarantees that this solution would effectively detect simultaneous attacks.

## VI. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

This paper provided a brief overview of the history of LoRaWAN and Energy Depletion Attacks (EDAs). It presented a classification of notable LoRaWAN attacks found in literature based on their objectives. Furthermore, it summarized a state-of-the-art for energy consumption modeling of end devices. In addition, this work proposed a characterization method to evaluate the potential of attacks to deplete energy from LoRaWAN end devices. The analysis revealed that eleven out of sixteen analyzed attacks have some potential to deplete energy from end devices, making them useful for attackers aiming to exhaust the battery of sensors until they become unavailable. Finally, this paper provided a literature review of the current defenses against LoRaWAN attacks that have the potential to deplete energy and discussed the open challenges in this scope.

Due to the diversity of sources, the mitigation of EDAs is quite complex. Future proposals of enhancements in LoRaWAN protocol must focus on the original attacks. For instance, the use of MIC instead of CRC physical layer [2] and improvements of KGD [91] could address some vulnerabilities. In the context of EDAs detection, there is also a research gap for solutions that can simultaneously detect and mitigate a set of these attacks. Most recent works focus on defenses against individual attacks, with almost all employing techniques based on network analysis [39], [106]. Silent EDAs introduce a complex factor for defense tasks, as these attacks do not alter network behavior, making detection challenging. Solutions that utilize energy consumption behavior might be an effective strategy to meet the requirements for EDA defenses [16].

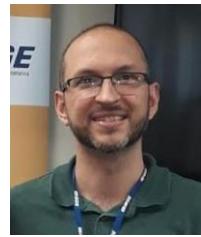
Finally, this paper provided an emulation of the potential for attacks to deplete the energy of end devices, thus opening opportunities for future research to test and evaluate empirical analyses of different attack scenarios in real-world environments, such as industrial settings or agricultural deployments. Such analyses could estimate the energy depletion with greater precision, offering insights into the impact on battery lifetime, network unavailability, and economic losses. Given the potential of several attacks, as previously discussed, these opportunities could be addressed in multiple separate studies.

## REFERENCES

- [1] Beecham Research, "LoRaWAN: Simple, Affordable, Transformative - End of year report 2023," 2023. [Online]. Available: <https://resources.lora-alliance.org/document/lora-alliance-2023-end-of-year-report>. [Accessed: 06-Aug-2024].
- [2] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet of Things*, vol. 12, p. 100303, Dec. 2020.
- [3] X. Yang, E. Karmpatzakis, C. Doerr, and F. Kuipers, "Security Vulnerabilities in LoRaWAN," in 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), 2018, no. April 2018, pp. 129–140.
- [4] M. N. Nafees, N. Saxena, P. Burnap, and B. J. Choi, "Impact of Energy Consumption Attacks on LoRaWAN-Enabled Devices in Industrial Context," in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 2117–2119.
- [5] K. Mikhaylov, R. Fujdiak, A. Pouttu, V. Miroslav, L. Malina, and P. Mlynák, "Energy Attack in LoRaWAN: Experimental Validation," in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, no. November 2020, pp. 1–6.
- [6] D. Farias de Carvalho and C. Miers, "Process Automation and Monitoring Systems Based on IIoT Using Private LoRaWAN Networks: A Case Study of ArcelorMittal Vega Facilities," in Proceedings of the 8th International Conference on Internet of Things, Big Data and Security, 2023, vol. 2023-April, pp. 243–254.
- [7] F. Kuntke, V. Romanenko, S. Linsner, E. Steinbrink, and C. Reuter, "LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 5, pp. 1–20, May 2022.
- [8] K. Taji and F. Ghanimi, "LoRaWAN-Based Smart Irrigation Systems: A Literature Review," 2024, pp. 22–34.
- [9] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," 2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017, vol. 2018-Janua, pp. 811–817, 2018.
- [10] N. Geethanjali and E. Gayathri, "A Survey on Energy Depletion Attacks in Wireless Sensor Networks," *Int. J. Sci. Res.*, vol. 3, no. 9, pp. 2070–2074, 2014.
- [11] V. Shakhev and I. Koo, "Depletion-of-Battery Attack: Specificity, Modelling and Analysis," *Sensors*, vol. 18, no. 6, p. 1849, Jun. 2018.
- [12] D. E. Boubiche and A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," *J. Emerg. Technol. Web Intell.*, vol. 5, no. 1, pp. 18–27, Feb. 2013.
- [13] M. Dabbagh and A. Rayes, "Internet of Things Security and Privacy," in *Internet of Things From Hype to Reality*, Cham: Springer International Publishing, 2019, pp. 211–238.
- [14] Y. W. Law, M. Palaniswami, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Trans. Sens. Networks*, vol. 5, no. 1, pp. 1–38, Feb. 2009.
- [15] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.
- [16] A. Proto, C. C. Miers, and T. C. M. de B. Carvalho, "A lightweight architecture for detection and mitigation of energy depletion attacks in LPWAN," in International Conference on Computer Communication and Informatics (ICCCI-2024), 2024.
- [17] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.
- [18] L. Slats, "A Brief History of LoRa: Three Inventors Share Their Personal Story at The Things Conference," Semtech, 2020. [Online]. Available: <https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference>. [Accessed: 27-Feb-2024].
- [19] T. Attia, M. Heusse, B. Tourancheau, and A. Duda, "Experimental Characterization of LoRaWAN Link Quality," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, no. Section II, pp. 1–6.
- [20] Semtech, "What are LoRa and LoRaWAN?," 2015. [Online]. Available: <https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/>. [Accessed: 27-Feb-2024].
- [21] M. N. Ochoa, A. Guizar, M. Maman, and A. Duda, "Evaluating LoRa energy efficiency for adaptive networks: From star to mesh topologies," in 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2017, vol. 2017-Octob, pp. 1–8.
- [22] S. Loukil, L. C. Fourati, A. Nayyar, and K.-W.-A. Chee, "Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms," *Sensors*, vol. 22, no. 10, p. 3717, May 2022.
- [23] M. Hassan, "LoRa and LoRaWAN," in *Wireless and Mobile Networking*, no. December 2019, Boca Raton: CRC Press, 2022, pp. 218–230.
- [24] LoRa Alliance, "LoRaWAN 1.0.4 Specification Package," 2020. [Online]. Available: [https://lora-alliance.org/resource\\_hub/lorawan-104-specification-package/](https://lora-alliance.org/resource_hub/lorawan-104-specification-package/). [Accessed: 28-Jul-2024].
- [25] P. S. Cheong, J. Bergs, C. Hawinkel, and J. Famacy, "Comparison of LoRaWAN classes and their power consumption," in 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT), 2017, vol. 2017-Decem, pp. 1–6.
- [26] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy Consumption Analysis of LPWAN Technologies and Lifetime Estimation for IoT Application," *Sensors*, vol. 20, no. 17, p. 4794, Aug. 2020.
- [27] H. H. R. Sherazi, L. A. Grieco, M. A. Imran, and G. Boggia, "Energy-Efficient LoRaWAN for Industry 4.0 Applications," *IEEE Trans. Ind. Informatics*, vol. 17, no. 2, pp. 891–902, Feb. 2021.
- [28] LoRa Alliance, "LoRaWAN Security - Full end-to-end encryption for IoT Application Providers," 2017. [Online]. Available: [https://lora-alliance.org/wp-content/uploads/2020/11/lorawan\\_security\\_whitepaper.pdf](https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf). [Accessed: 18-Mar-2024].
- [29] S. Silva, G. Koslovski, M. Pillon, and C. Miers, "Credential Lifecycle Analysis in Private LoRaWAN Networks for Industrial IoT (IIoT)," in Proceedings of the 9th International Conference on Internet of Things, Big Data and Security, 2024, pp. 157–165.
- [30] LoRa Alliance, "LoRaWAN 1.1 Specification," Technical document, 2017. [Online]. Available: [https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm\\_specification\\_v1.1.pdf](https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_v1.1.pdf). [Accessed: 28-Jul-2024].
- [31] F. Alizadeh and A. J. Bidgoly, "Bit flipping attack detection in low-power wide area networks using a deep learning approach," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 4, pp. 1916–1926, Aug. 2023.
- [32] H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak, "LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review," *Sensors*, vol. 22, no. 9, p. 3127, Apr. 2022.
- [33] P. de Moraes and A. F. da Conceição, "A Systematic Review of Security in the LoRaWAN Network Protocol," *ACM Comput. Surv.*, vol. 30, no. 3, May 2021.
- [34] K. Ntshabele, B. Isong, N. Gasela, and A. M. Abu-Mahfouz, "A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions," *Mathematics*, vol. 10, no. 19, p. 3421, Sep. 2022.
- [35] E. U. Ogbodo, A. M. Abu-Mahfouz, and A. M. Kurien, "A Survey on 5G and LPWAN-IoT for Improved Smart Cities and Remote Area Applications: From the Aspect of Architecture and Security," *Sensors*, vol. 22, no. 16, p. 6313, Aug. 2022.
- [36] E. Yocam, "Narrow-band Internet of Things Protocol Standards: Survey of Security and Privacy Control Effectiveness," in 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1–6.
- [37] J. Sanchez-Gomez et al., "Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions," *IEEE Access*, vol. 8, pp. 216437–216460, 2020.
- [38] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A Survey on LPWAN-5G Integration: Main Challenges and Potential Solutions," *IEEE Access*, vol. 10, pp. 32132–32149, 2022.
- [39] G. Stanco, A. Navarro, F. Frattini, G. Ventre, and A. Botta, "A comprehensive survey on the security of low power wide area networks for the Internet of Things," *ICT Express*, vol. 10, no. 3, pp. 519–552, Jun. 2024.
- [40] H. Jradi, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Overview of the mobility related security challenges in LPWANs,"

- Comput. Networks, vol. 186, no. December 2020, p. 107761, Feb. 2021.
- [41] R. Krejci, O. Hujnak, and M. Svepes, "Security survey of the IoT wireless protocols," in 2017 25th Telecommunication Forum (TELFOR), 2017, vol. 2017-Janua, pp. 1–4.
- [42] J. P. Shammuga Sundaram, W. Du, and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 371–388, 2020.
- [43] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," IEEE Commun. Surv. Tutorials, vol. 24, no. 2, pp. 767–809, 2022.
- [44] E. Kail, A. Banati, E. Laszlo, and M. Kozlovsky, "Security Survey of Dedicated IoT Networks in the Unlicensed ISM Bands," in 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), 2018, pp. 449–454.
- [45] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A Survey of LoRaWAN for IoT: From Technology to Application," Sensors, vol. 18, no. 11, p. 3995, Nov. 2018.
- [46] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," IEEE Access, vol. 8, pp. 228922–228941, 2020.
- [47] P. Rojas, S. Alahmadi, and M. Bayoumi, "Physical Layer Security for IoT Communications - A Survey," in 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), 2021, pp. 95–100.
- [48] N. Hou, X. Xia, and Y. Zheng, "CloakLoRa: A Covert Channel Over LoRa PHY," IEEE/ACM Trans. Netw., vol. 31, no. 3, pp. 1159–1172, Jun. 2023.
- [49] N. S. Mtetwa, P. Tarwireyi, A. M. Abu-Mahfouz, and M. O. Adigun, "Secure Firmware Updates in the Internet of Things: A survey," in 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, pp. 1–7.
- [50] G. Vishwakarma and W. Lee, "Exploiting JTAG and Its Mitigation in IOT: A Survey," Futur. Internet, vol. 10, no. 12, p. 121, Dec. 2018.
- [51] R. Sanchez-Vital, L. Casals, B. Heer-Salva, R. Vidal, C. Gomez, and E. Garcia-Villegas, "Energy Performance of LR-FHSS: Analysis and Evaluation," Sensors, vol. 24, no. 17, 2024.
- [52] Y. Yazid, M. Zbairi, A. Guerrero Gonzales, M. Arioua, and A. El Ouakkadi, Extensive energy modeling for LoRaWANs. Elsevier Inc., 2024.
- [53] E. Gelenbe and Y. M. Kadioglu, "Energy life-time of wireless nodes with network attacks and mitigation," 2018 IEEE Int. Conf. Commun. Work. ICC Work. 2018 - Proc., pp. 1–6, 2018.
- [54] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the Energy Performance of LoRaWAN," Sensors, vol. 17, no. 10, p. 2364, Oct. 2017.
- [55] A. Sorensen et al., "Modeling and Experimental Validation for Battery Lifetime Estimation in NB-IoT and LTE-M," IEEE Internet Things J., vol. 9, no. 12, pp. 9804–9819, Jun. 2022.
- [56] G. S. Kuaban, E. Gelenbe, T. Czachórski, P. Czekalski, and J. K. Tangka, "Modelling of the Energy Depletion Process and Battery Depletion Attacks for Battery-Powered Internet of Things (IoT) Devices," Sensors, vol. 23, no. 13, p. 6183, Jul. 2023.
- [57] F. Correia, M. Alencar, and K. Assis, "Stochastic Modeling and Analysis of the Energy Consumption of Wireless Sensor Networks," IEEE Lat. Am. Trans., vol. 21, no. 3, pp. 434–440, 2023.
- [58] H. Rajab, H. Al-Amaireh, T. Bouguera, and T. Cinkler, "Evaluation of energy consumption of LPWAN technologies," Eurasip J. Wirel. Commun. Netw., vol. 2023, no. 1, 2023.
- [59] M. R. Ghaderi and N. Amiri, "LoRaWAN sensor: energy analysis and modeling," Wirel. Networks, vol. 30, no. 2, pp. 1013–1036, 2024.
- [60] A. Khalifeh, F. Mazunga, A. Nechibvute, and B. M. Nyambo, "Microcontroller Unit-Based Wireless Sensor Network Nodes: A Review," Sensors, vol. 22, no. 22, p. 8937, Nov. 2022.
- [61] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. McKague, "Security and Performance in IoT: A Balancing Act," IEEE Access, vol. 8, pp. 121969–121986, 2020.
- [62] P. Thaenkawew, B. Quoitin, and A. Meddahi, "Evaluating the cost of beyond AES-128 LoRaWAN security," in 2022 International Symposium on Networks, Computers and Communications (ISNCC), 2022, pp. 1–6.
- [63] TEXAS INSTRUMENTS, "MSP430FR596x , MSP430FR594x Mixed-Signal Microcontrollers," 2018. [Online]. Available: <https://www.ti.com/lit/ds/symlink/msp430fr5994.pdf?ts=1709610231149>. [Accessed: 05-Mar-2024].
- [64] TEXAS INSTRUMENTS, "CC3220MODx and CC3220MODAx SimpleLink™ Wi-Fi® CERTIFIED™ Wireless MCU Modules," 2021. [Online]. Available: <https://www.ti.com/lit/ds/symlink/cc3220moda.pdf?&ts=1589201716200>. [Accessed: 13-May-2024].
- [65] Microchip Technology Inc., "SAM D21/DA1 Family Low-Power, 32-bit Cortex-M0+ MCU with Advanced Analog and PWM," 2020. [Online]. Available: [https://ww1.microchip.com/downloads/en/DeviceDoc/SAM\\_D21\\_DA1\\_Family\\_DataSheet\\_DS40001882F.pdf](https://ww1.microchip.com/downloads/en/DeviceDoc/SAM_D21_DA1_Family_DataSheet_DS40001882F.pdf). [Accessed: 13-May-2024].
- [66] A. Mart et al., "Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks," in 2008 Third International Conference on Availability, Reliability and Security, 2008, pp. 520–525.
- [67] E. van Es, H. Vranken, and A. Hommersom, "Denial-of-Service Attacks on LoRaWAN," in Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1–6.
- [68] X. Yang, "LoRaWAN: Vulnerability analysis and practical exploitation," Delft University of Technology, 2017.
- [69] I. Butun, N. Pereira, and M. Gidlund, "Analysis of LoRaWAN v1.1 security," in Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, 2018, pp. 1–6.
- [70] S. Chacko and M. D. Job, "Security mechanisms and Vulnerabilities in LPWAN," IOP Conf. Ser. Mater. Sci. Eng., vol. 396, no. 1, p. 012027, Aug. 2018.
- [71] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," in 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), 2017, pp. 1–6.
- [72] I. Butun, N. Pereira, and M. Gidlund, "Security Risk Analysis of LoRaWAN and Future Directions," Futur. Internet, vol. 11, no. 1, p. 3, Dec. 2018.
- [73] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J.-C. Prevotet, "Mobility Management With Session Continuity During Handover in LPWAN," IEEE Internet Things J., vol. 7, no. 8, pp. 6686–6703, Aug. 2020.
- [74] Z. Tyree, R. A. Bridges, F. L. Combs, and M. R. Moore, "Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection," in 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1–5.
- [75] C. Johnson and M. Evangelopoulos, "Defending Against Firmware Cyber Attacks on Safety-Critical Systems," J. Syst. Saf., vol. 54, no. 1, pp. 16–21, Apr. 2018.
- [76] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, "Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure," in 2018 IEEE International Conference on Communications (ICC), 2018, vol. 2018-May, pp. 1–6.
- [77] Z. Feng and C. Hua, "Machine Learning-based RF Jamming Detection in Wireless Networks," in 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 2018, pp. 1–6.
- [78] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. 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, 2017, pp. 363–372.
- [79] N. Hou, X. Xia, and Y. Zheng, "Jamming of LoRa PHY and Countermeasure," ACM Trans. Sens. Networks, vol. 19, no. 4, pp. 1–27, Nov. 2023.
- [80] I. Martinez, F. Nouvel, S. Lahoud, P. Tanguy, and M. El Helou, "On the Performance Evaluation of LoRaWAN with Re-transmissions under Jamming," in 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, vol. 2020-July, pp. 1–7.
- [81] C.-Y. Huang, C.-W. Lin, R.-G. Cheng, S. J. Yang, and S.-T. Sheu, "Experimental Evaluation of Jamming Threat in LoRaWAN," in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1–6.
- [82] K. Rosenfeld and R. Karri, "Attacks and Defenses for JTAG," IEEE Des. Test Comput., vol. 27, no. 1, pp. 36–47, Jan. 2010.
- [83] F. Majeric, B. Goncalvo, and L. Bossuet, "JTAG Fault Injection Attack," IEEE Embed. Syst. Lett., vol. 10, no. 3, pp. 65–68, Sep. 2018.
- [84] W.-J. Sung, H.-G. Ahn, J.-B. Kim, and S.-G. Choi, "Protecting end-device from replay attack on LoRaWAN," in 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018, pp. 167–171.

- [85] SeungJae Na, DongYeop Hwang, WoonSeob Shin, and Ki-Hyung Kim, "Scenario and countermeasure for replay attack using join request messages in LoRaWAN," in 2017 International Conference on Information Networking (ICOIN), 2017, pp. 718–720.
- [86] J. Kim and J. Song, "A Simple and Efficient Replay Attack Prevention Scheme for LoRaWAN," in Proceedings of the 2017 7th International Conference on Communication and Network Security, 2017, pp. 32–36.
- [87] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, Mar. 2019.
- [88] F. Hessel, L. Almon, and F. Álvarez, "ChirpOTLE," in Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020, pp. 306–316.
- [89] M. Chen, J. Ben-Othman, and L. Mokdad, "Greedy Behavior Detection With Machine Learning for LoRaWAN Network," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 3, pp. 2731–2740, Jun. 2024.
- [90] S. Halder and T. Newe, "Radio fingerprinting for anomaly detection using federated learning in LoRa-enabled Industrial Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 143, pp. 322–336, Jun. 2023.
- [91] J. Qadir, I. Butun, P. Gastaldo, O. Aiello, and D. D. Caviglia, "Mitigating Cyber Attacks in LoRaWAN via Lightweight Secure Key Management Scheme," *IEEE Access*, vol. 11, pp. 68301–68315, 2023.
- [92] C. Shen, T. Liu, J. Huang, and R. Tan, "When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient," in 2021 IEEE Symposium on Security and Privacy (SP), 2021, pp. 1304–1317.
- [93] S. Saxena, A. Pandey, and S. Kumar, "RSS based multistage statistical method for attack detection and localization in IoT networks," *Pervasive Mob. Comput.*, vol. 85, p. 101648, Sep. 2022.
- [94] I. Suciu, J. C. Pacho, A. Bartoli, and X. Vilajosana, "Authenticated Preambles for Denial of Service Mitigation in LPWANs," in Ad-hoc, Mobile, and Wireless Networks, 2018, pp. 199–210.
- [95] W. Mao et al., "Reliable and Energy-Efficient Reprogramming for Smart LoRaWAN," in 2023 IEEE Smart World Congress (SWC), 2023, pp. 1–8.
- [96] A. Anastasiou, P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos, "IoT Device Firmware Update over LoRa: The Blockchain Solution," in 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2020, pp. 404–411.
- [97] V. Malumbres, J. Saldana, G. Berné, and J. Modrego, "Firmware Updates over the Air via LoRa: Unicast and Broadcast Combination for Boosting Update Speed," *Sensors*, vol. 24, no. 7, p. 2104, Mar. 2024.
- [98] V. Kalokidou, M. Nair, and M. A. Beach, "LoRaWAN Performance Evaluation and Resilience under Jamming Attacks," in 2022 Sensor Signal Processing for Defence Conference (SSPD), 2022, pp. 1–5.
- [99] B. J. Bleszynski, C. Orfanidis, and X. Fafoutis, "Detection of Mobile LoRa Jammers," in 2023 IEEE Virtual Conference on Communications (VCC), 2023, pp. 288–293.
- [100] M. Monjur and Q. Yu, "CTC: Continuous-Time Convolution based Multi-Attack Detection for Sensor Networks," in 2024 IEEE International Symposium on Circuits and Systems (ISCAS), 2024, pp. 1–5.
- [101] M. A. Haque and A. Saifullah, "Handling Jamming Attacks in a LoRa Network," Proc. - 9th ACM/IEEE Conf. Internet-of-Things Des. Implementation, IoTDI 2024, pp. 146–157, 2024.
- [102] X. Huan, K. Miao, W. Chen, P. Jia, and H. Hu, "Kerra: An Internet-of-Things Wireless Key Generation Resistant to Replay Attacks," *IEEE Internet Things J.*, pp. 1–1, 2024.
- [103] H. Noura, O. Salman, T. Hatoum, M. Malli, and A. Chehab, "Towards Securing LoRaWAN ABP Communication System," in Proceedings of the 10th International Conference on Cloud Computing and Services Science, 2020, pp. 440–447.
- [104] P. Locatelli, P. Spadaccino, and F. Cuomo, "Hijacking Downlink Path Selection in LoRaWAN," in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1–6.
- [105] B. P. Neves, A. Valente, and V. D. N. Santos, "Efficient Runtime Firmware Update Mechanism for LoRaWAN Class A Devices," *Eng.*, vol. 5, no. 4, pp. 2610–2632, Oct. 2024.
- [106] F. Hessel, L. Almon, and M. Hollick, "LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation," *ACM Trans. Sens. Networks*, vol. 18, no. 4, pp. 1–55, Nov. 2022.



**André Proto** is currently a Ph.D. student in Electrical Engineering at the Polytechnic School of the University of São Paulo (USP). He earned his B.Sc. and M.Sc. degrees in Computer Science from the Instituto de Biociências, Letras e Ciências Exatas of São José do Rio Preto, Universidade Estadual Paulista (UNESP), Brazil, in 2008 and 2011, respectively. His current research focuses on cybersecurity on the Internet of Things.

Since 2010, he has worked at the Instituto Brasileiro de Geografia e Estatística (IBGE) as an Information and Communication Technology (ICT) analyst, participating in several support and network projects. From 2020 to 2023, he coordinated the ICT team for the Demographic Census operation in the state of São Paulo, Brazil. He is currently the deputy manager of ICT national support at IBGE.



**Charles C. Miers** is a Santa Catarina State University associate professor. He got his Ph.D. in Electrical Engineering from the Polytechnic School of the University of São Paulo (USP), a Master's in Computer Science from the Federal University of Santa Catarina (UFSC), and graduated from CCT / UDESC. He was head of the Graduate Program in Applied Computing (PPGCAP) at the Department of Computer Science (DCC/CCT/UDESC) from 2020 to

2023. Conducts research in computer networks and information security; the current investigation covers cloud computing, Blockchain, Industrial IoT (IIoT), device/flow-centric authentication, Adversarial AI/LLM, and energy efficiency. He has projects in partnership with Hewlett Packard Enterprise (USA), the University of São Paulo, and UBRI (University Blockchain Research Initiative), which is an initiative of Ripple Labs Inc., a North American company behind the cryptocurrency namesake. He integrates the coordination of the Laboratory of Parallel and Distributed Processing (LabP2D) at DCC / CCT / UDESC. He was a founding partner of one of the pioneering companies specializing in information security in Santa Catarina.



**Tereza C. M. B. Carvalho.** is currently an Associate Professor with Polytechnic School, University of São Paulo (USP), and a Visiting Professor with Université Paris 1 Panthéon-Sorbonne. She has been the Founder and a general Coordinator with the Laboratory of Sustainability on ITC (LASSU), since 2010, and the Center for Reuse and Discard of Informatics Residuals (CEDIR-USP), since 2009. She is also a former Assessor with CTI—USP (Information Technology Coordination), from 2010 to 2013, and the Director of CCE-USP (Electronic Computing Center), from 2006 to 2010. She was a Sloan Fellow with the Massachusetts Institute of Technology (MIT), in 2002. She has been coordinating international and national research and development projects, since 2000, in green computing, cloud computing, IT energy efficiency, IT governance, digital technologies applied to the Amazon production chains, waste electrical and electronic equipment (WEEE), future internet, scientific DMZ, and security. She holds several international patents.