A Security-Conscious Primer on LoRa and LoRaWAN Technologies

Tomás Simões, Tiago Cruz, Bruno Sousa and Paulo Simões
University of Coimbra, CISUC, DEI, Portugal

tfds@student.uc.pt
tjcruz@dei.uc.pt
bmsousa@dei.uc.pt
psimoes@dei.uc.pt

Abstract: At its core, the Internet of Things (IoT) paradigm encompasses a wealth of devices, mainly sensors, actuators and systems that can connect and exchange data through any means of communication, as long as they're individually addressable and are a part of a network. There is a wide array of possible network types, among which Low-Power Short-Range Networks (LPSRNs) and Low-Power Wide-Area Networks (LPWANs) offer a great deal of potential to support energy efficient communications with low maintenance. LoRa (an abbreviation of "Long Range"), one of the most popular technologies for implementing LPWANs, is a radio-based technique derived from Chirp Spread Spectrum (CSS) technology (where "Chirp" stands for Compressed High Intensity Radar Pulse). However, when used as a standalone technology, it exposes exchanged data as LoRa devices simply transmit packets publicly without any built-in security. The LoRaWAN (LoRa Wide Area Network) framework addresses these shortcomings by providing a software layer on top of LoRa, supporting device addressing, management and message acknowledgement, while also providing a security framework with network and application encryption layers based on the AES-128 algorithm. LoRaWAN security mechanisms provide authentication and integrity protection of transmitted packets to the LoRaWAN Network Server (LNS), to ensure end-to-end encryption at the application layer. Due to its widespread application in IoT scenarios such as smart cities, smart transportation and environmental monitoring, the security of the LoraWAN framework is fundamental to ensure the security and safety of critical metering and telemetry infrastructures. In this paper we provide a primer on LoRa and LoRaWAN technologies and address the security and management-related aspects of this framework, also presenting a threat model for LoRaWAN networks based on the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) methodology, providing a convenient starting point for risk assessment and preventive/mitigation action planning.

Keywords: IoT, LPWAN, LoRa, LoRaWAN, Security

1. Introduction

Sensor deployment has become a widely adopted and cost-effective approach to monitor transportation networks and other ecosystems, automating interactions and data retrieval (LoRa Alliance, 2022). This approach goes hand-in-hand with the recent growth in the popularity of IoT applications. LoRa and LoRaWAN have the potential to revolutionize sensor networks, as LoRa possesses the capability to transmit packets over a distance of up to 20 km outdoors and up to 7 km indoors (Murata, n. d.), subject to the surrounding environment and utilized hardware, and LoRaWAN provides the necessary features to unify devices into one functional network, enabling packet encryption, integrity, and two-way device-server communications.

This paper provides an overview of LoRa and LoRaWAN technologies, describes the deployment of a LoRaWAN network, discusses LoRaWAN's included safety measures and offers solutions to some possible security and privacy vulnerabilities. Moreover, it also includes a threat model for LoRaWAN networks based on the STRIDE methodology, which can be used for risk assessment purposes and/or to plan and develop preventive/mitigation actions.

The rest of this paper is organized as follows. Section 2 introduces LoRa, its modulation techniques, and related European regulations. Section 3 provides an overview of the LoRaWAN protocol and the components of a LoRaWAN network, explaining the roles of end nodes, gateways, and network/application/join servers, while also covering packet structure, device classes and LoRa Alliance specifications. Section 4 covers security-related aspects, such as the implementation of the AES-128 algorithm, the differences between different LoRaWAN release versions and activation procedures, also presenting the STRIDE-based risk model for LoRaWAN. Section 5 concludes the paper.

2. An Overview of LoRa

LoRa's development began in France circa 2009, by Nicolas Sornin and Olivier Seller (Slats, L., 2020). In 2010, they partnered with François Sforza to create a company (Cycleo) with the aim of adding wireless communication capabilities to electricity, gas, and water meters. Semtech later acquired Cycleo (in May of 2012), due to its potential for long-range and low-power transmission.

LoRa achieves long-range transmission with low-power consumption by adopting CSS, which is a long-range radiofrequency technology that uses wideband linear frequency pulses that leverage the entire allocated bandwidth to improve robustness against channel noise. It operates in sub-gigahertz ISM (Industrial, Scientific, and Medical) bands, with 863-870 MHz being the available frequency range in Europe (referred to as the EU863-870 MHz band) for unlicensed use (The Things Network, 2025b). It can also operate at the 2.4 GHz band, but with significantly reduced range.

LoRa encodes information through linear frequency modulated signals, known as 'chirps' (Tektelic, n. d.), and filters LoRa symbols, ignoring other RF parameters such as amplitude and phase (The Things Network, 2025a). Interestingly, Ningning, H., Xia, X., Zheng, Y. (2022) discovered that the LoRa physical layer leaves enough space to implement a covert channel over the LoRa PHY (using orthogonal modulation schemes), also proposing a countermeasure that relies on the ability of the LoRa gateway to monitor aspects such as amplitude changes (characteristic of an Amplitude Modulation-based side channel).

The EU863-870 MHz band supports between 24 and 80 channels. The LoRa Alliance recommends a 1% duty cycle limit per day, which is the ratio between active time and non-active time of a device in a day, in the EU863-870 MHz band, with a maximum Effective Isotropic Radiated Power (EIRP) value of +16 dBm, which signifies the antenna gain in a single direction. These guidelines are set in place to avoid potentially disruptive interference towards other devices on the same band.

The European Telecommunications Standards Institute (ETSI) has imposed additional restrictions, while segmenting the European band into 6 sub-bands, as per Table 1.

Table 1: Subdivision of the EU863-870 MHz band following the ETSI's restrictions (ETSI, 2018)

Sub-band	Frequency range (MHz)	Duty cycle (%)	Duty cycle (seconds)	Maximum EIRP (dBm)
K	863 – 865	0.1	86.4	+16.15
L	865 – 868	1	864	+16.15
M	868 – 868.6	1	864	+16.15
N	868.7 – 869.2	0.1	86.4	+16.15
P	869.4 – 869.65	10	8640	+29.15
Q	869.7 – 870	1	864	+16.15

LoRa doesn't encrypt payload data, as LoRa frames are composed of 8 preamble symbols, which are upchirps that are used to detect LoRa signals, 2 synchronization symbols, downchirps used for timing synchronization, and the payload itself (Ghoslya, S., n. d.). It only converts data to chirps for transmission, and every device in range, equipped with a LoRa chip and antenna, can catch these packets. This reinforces the assumption that all data from packets transmitted without the LoRaWAN protocol can be potentially compromised.

3. Introducing LoRaWAN

At the same time the first LoRa chips were launched, the LoRaWAN protocol (initially known as LoRaMAC) was created (Slats, L., 2020). LoRaWAN is a software layer that operates on top of LoRa and introduces the MAC layer that defines the communication standard and system architecture. It allows for device addressing, device management, message acknowledgement, and introduces a security framework for network and application layer encryption (The Things Network, 2025a; Semtech Corporation, 2024a).

The LoRa Alliance, an open, non-profit association with the mission to standardize and promote the use of LoRaWAN networks, was founded in February of 2015, being the entity responsible for the maintenance and development of the LoRaWAN protocol.

LoRaWAN applications are diverse, encompassing scenarios such as (but not restricted to) Healthcare, Smart City, Smart Building or Agriculture scenarios, ensuring personal telemetry, environmental sensing, telemetry, crop or livestock monitoring, among others. In this sense, this technology provides support for a new generation of distributed Industrial Automation and Control Systems (IACS).

3.1 LoRaWAN Specifications and Device Classes

LoRaWAN currently has 2 main specification series, v1.0 and v1.1 (The Things Network, 2025a), with the most recent version from both series being v1.0.4 and v1.1, respectively. Version 1.0.4 was released in October 2020 and, in terms of security, isn't as robust as version 1.1, which was released in October 2017.

Both LoRaWAN versions identify devices with an identifier, the *DevEUI*. This identifier is a global application ID in the IEEE EUI64 address space that unequivocally identifies an end device across roaming networks. Join servers are also identified using an IEEE EUI64 address space unique identifier, the *JoinEUI* (LoRa Alliance, 2017; LoRa Alliance, 2020).

Regardless of the specification version, there are three different classes of LoRaWAN devices (Semtech Corporation, 2024c): A, B, and C, with class A being mandatory. Class A devices open two time windows, known as RX1 (first window) and RX2 (second window), for receiving downlinks, which are messages from the LNS to end devices, after uplink transmission, which are messages from end devices to the LNS. The latter can be done at any given moment, although usually class A devices send uplinks with little frequency, to preserve battery life.

Class B devices work similarly to class A devices, but they periodically open receive windows called 'ping slots', for downlink message reception. Beacons periodically broadcasted by gateways, used to synchronize end devices' internal clocks with the network, signal class B devices when to open these ping slots. The delay between the beginning of two beacons is called the beacon period. Class B devices can work in class A mode.

Class C devices use more power than class A and class B devices, as these only close receive windows when transmitting uplinks. After uplink transmission, the RX2 window is open until the start of the RX1 window. When the RX1 window closes, the RX2 window opens again and only closes when the device sends the next uplink. This mode is used to perform firmware updates over-the-air (FUOTA). Class C devices can also work in class A mode.

3.2 LoRaWAN Networks

LoRaWAN networks consist of end nodes, gateways, a LoRaWAN Network server (LNS), one or more application servers (which can also provide dashboards to display end node data), and the join server (The Things Network, 2025e). Using LoRaWAN, end devices transmit packets that are forwarded by gateways within range, which by their turn are connected to the LNS. Payloads are then sent to the corresponding application servers or to the join server using higher bandwidth communication protocols. Figure 1 illustrates the components of a typical LoRaWAN network.

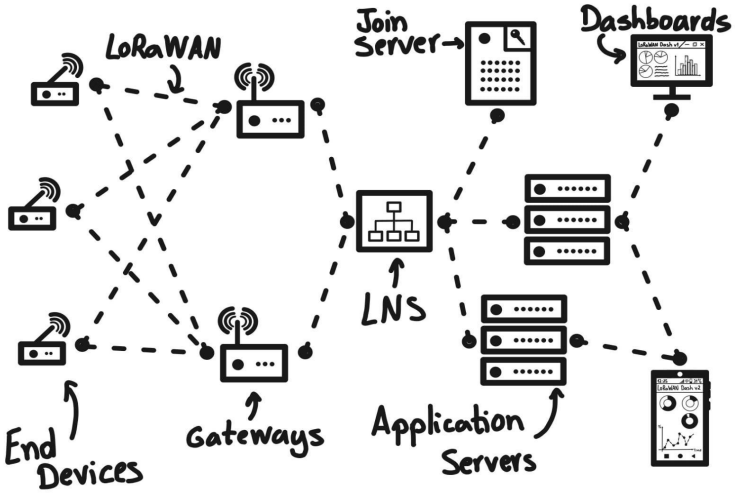

Figure 1: LoRaWAN Network diagram with all the referred components

The role of each LoRaWAN network element will be next presented into detail:

- **End devices** usually consist of battery-powered microcontrollers equipped with sensors or other digital-to-analog/analog-to-digital/mechanical extensions. These devices possess a LoRa transmitter and can implement the LoRaWAN protocol. They connect to the LNS through gateways using LoRa RF Modulation, with its device ID and authentication keys.

Activation can take place via Over-The-Air Activation (OTAA) or Activation By Personalization (ABP). In OTAA devices are provisioned with root keys - the *AppKey* for LoRaWAN 1.0.x and, in case of LoRaWAN 1.1x, also an *NwkKey* - both set during manufacturing and used to join a network, used to generate session keys change for each new communication session (Semtech Corporation, 2024a; Semtech Corporation, 2024c; The Things

Network, 2025e). In ABP activation, pre-selected network and device parameters are hardcoded into the end device, allowing to skip the join procedure.

- **Gateways** simply forward packets from end devices in range to the LNS, checking only the packet's integrity through its CRC and dropping the packet if it's incorrect, as the gateways only operate at the physical layer (Semtech Corporation, 2024a; The Things Network, 2025e). Since it is possible for an end device to be in range of multiple gateways, the LNS chooses the gateway closest to the end device by checking the packet's received signal strength indicator (RSSI). It's recommended that gateways support more than a single LoRa channel, as single-channel gateways are not considered LoRaWAN-compliant, since they may become potentially overwhelmed if there are multiple devices nearby.
- **LoRaWAN Network server (LNS)**. Its purpose is to moderate a LoRaWAN network and its devices, and to forward information from end devices to the application server/join server and the other way around. Since multiple gateways can forward the same packet to the LNS, it deletes all copies apart from the gateway closest to the end device. The *AppSKey* session key, used to decrypt the information sent by and to the end devices, is not known to the LNS (Semtech Corporation, 2024a; The Things Network, 2025e).
- An **Application server** manages packets transmitted by end devices. Such servers can be used to feed dashboards that allow to group and visualize decrypted data. In both LoRaWAN v1.0.4 and v1.1, the *AppSKey* (specific session key, later discussed) is used for payload encryption and decryption (Semtech Corporation, 2024a; The Things Network, 2025e; LoRa Alliance, 2020; LoRa Alliance, 2017).
- **Join Server.** A LoRaWAN join server manages the connection of devices to the LNS through OTAA. It receives join requests and generates the corresponding join accept frames, while instructing the LNS to which application server an end device should transmit. It also provides, to an end-device, a non-repeating value, the *JoinNonce*, which is used by end devices to derive session keys.

Together, these elements enable the creation of networks that follow a *star-of-stars* topology, without having any explicit connection between the end nodes and the gateways, as the latter simply listen for packets and forward them without the need for handshakes.

3.3 LoRaWAN Packets

LoRaWAN packets can be organized in two formats: explicit and implicit (The Things Network, 2025c), with explicit framing being used for uplink and downlink packets (see Figure 2). Their structure includes a preamble, used to synchronize the receiver with the transmitter and consists of 8 symbols at first, with an extra 4.25 symbols being added by the radio transmitter, and the physical payload, containing the frame generated by the MAC layer, and its size is region specific and depends on the data rate, which is the number of bits transmitted per unit of time and depends on the utilized LoRa configuration.

Explicit packets can also contain a physical header (PHDR), which contains the payload size and information about the cyclic redundancy check (CRC), another optional field that detects and corrects errors in uplink messages' payload. It can also contain the physical header CRC (PHDR_CRC), used to detect and correct errors in the physical header.

Figure 2: Uplink/Downlink (explicit) packet structure

The *PHYPayload* (See Figure 3) is composed by the MAC header (MHDR), which specifies the frame version and type, the *MACPayload*, containing the transmitted information, and the Message Integrity Code (MIC), which is used to verify the transmitter's identity (Semtech Corporation, 2024b).

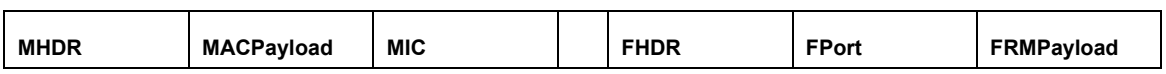

Figure 3: *PHYPayload* (*left*) and *MACPayload* (*right*) frame structures

The *MACPayload* (See Figure 3) contains a frame header (FHDR) followed by an optional port (*FPort*) and frame payload (FRMPayload) fields. The FHDR contains the short end device address (DevAddr), as well as frame control flags, options, and a counter. The FPort, which identifies application-specific data, should be present if there is an FRMPayload.

Implicit packets (see Figure 4) are more commonly used to transmit beacons, having no LoRa physical header and no appended radio CRC. Their structure includes a preamble (of 10 unmodulated symbols) and the beacon payload.

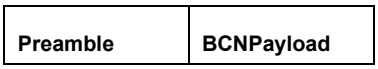

Figure 4: Beacon (implicit) packet structure

LoRaWAN devices that support the EU863-870 MHz band must guarantee that channels 868.10, 868.30, and 868.50 are implemented, as these are chosen at random and used to send join requests from the end devices. These three channels have a bandwidth of 125 kHz, with data rates ranging from DR0 (250 bit/s) to DR5 (5.470 kbit/s). Data rate is the number of bits that are transmitted per unit of time, and it depends on the LoRaWAN configuration that is being used. LoRaWAN devices must support either (i) DR0 – DR5 (minimum for LoRaWAN certification); or (ii) DR0 – DR7 (up to 11 kbit/s); (iii) DR0 – DR11, corresponding to all data rates implemented on the end device (The Things Network, 2025b).

4. LoRaWAN Network Security

LoRaWAN encrypts payloads using AES-CCM* (Counter with CBC Message Authentication Code) mode, as per the IEEE 802.15.4 recommendation (IEEE, 2011). Each LoRaWAN device is given a 128-bit AES key, the Application Key (*AppKey*), and, in the case of LoRaWAN v1.1 devices, another 128-bit AES key is provided, the Network Key (*NwkKey*).

Devices can be activated with Over-The-Air Activation (OTAA), allowing them to be rekeyed if necessary, or via Activation By Personalization (ABP) for secure device provisioning. In OTAA devices, and considering LoRaWAN v1.0.4, the *AppKey* (which is the device-specific AES-128 root key that is also provisioned into the Join Server) is used by the Join Server to generate the *NwkSKey* and the *AppSKey* session keys (which are derived by the end device from the *AppKey* and an *JoinNonce* provided in a *Join Accept* message sent by the Join Server).

In the case of LoRaWAN v1.1, the Join Server, which was provisioned with the end device *AppKey*, *NwkKey* and *DevEUI*, generates the *AppSKey, FNwkSIntKey, SNwkSIntKey* and *NwkSEncKey* session keys – these are later derived by the end device from the *AppKey* and *NwkKey*, and a *JoinNonce* provided in a *Join Accept* message (*AppSKey* is derived from *AppKey* and *FNwkSIntKey*, *SNwkSIntKey*, and *NwkSEncKey* are derived from the *NwkKey*).

Depending on the LoRaWAN version, AES algorithms ensure end-to-end encryption for the application server, with version 1.1 also providing authentication and integrity for the network server (albeit with some flaws, discussed in the next sections). These two security layers can enable the creation of multitenant network scenarios, where the network operator cannot access the users' payload data.

4.1 Version and Activation-Specific Differences

LoRaWAN-specific security mechanisms are implemented in different ways, according to specific release version and activation processes. For instance, LoRaWAN v1.0.X only uses two session keys (LoRa Alliance, 2020): the Network Session Key (*NwkSKey*) and the Application Session Key (*AppSKey*). On the other hand, LoRaWAN v1.1 uses four session keys (LoRa Alliance, 2017), namely: the Forwarding Network Session Integrity Key (*FNwkSIntKey*), the Serving Network Session Integrity Key (*SNwkSIntKey*), the Network Session Encryption Key (*NwkSEncKey*), and the *AppSKey*. Version 1.1 also implements two keys for interaction with the join server: the Join Server Integrity Key (*JSIntKey*) and the Join Server Encryption Key (*JSEncKey*). There are other notable differences, namely:

- **For Join Servers and End Devices.** For OTAA, session keys are generated from an *AppKey* (both LoRaWAN v1.0.4 and v1.1), and from the *NwkKey* (LoRaWAN v1.1 only). The *JoinNonce* response sent by the Join Server is handled in a different way by end devices. In LoRaWAN v1.0.4 with OTAA, it is used to generate the *AppSKey* and the *NwkSKey* from the *AppKey*. In LoRaWAN v1.1, the OTAA device generates, using the *JoinNonce*, the *FNwkSIntKey*, the *SNwkSIntKey*, the NwkSEncKey, and the *AppSKey*. It should be mentioned that the Join Server was introduced in version 1.0.4 (until then, the LNS ensured this role).

On the contrary, ABP makes the device's connectivity less flexible by tying it to a specific network, although easing the join process. This makes these devices more vulnerable to key gathering attacks.

- **For the LoRaWAN Network server (LNS).** In LoRaWAN v1.0.4, the *NwkSKey* session key is used for MAC command payload encryption/decryption and for MIC calculation, used to verify transmitted packets' integrity, but, in LoRaWAN v1.1, both the *FNwkSIntKey* and *SNwkSIntKey* are used for MIC calculation and the *NwkSEncKey* for MAC commands' payload encryption/decryption (LoRa Alliance, 2020; LoRa Alliance, 2017).

It should be mentioned that, while there are other differences regarding pre-1.0.4 versions, their discussion was deemed outside the scope of this paper.

4.2 Securing LoRaWAN Networks

Being the cornerstone of many distributed IACS, LoRaWAN constitutes a desirable target for all sorts of malicious activity, pretty much in line with what already happened in the past with SCADA (Supervisory Control and Data Acquisition) systems (Rosa et al., 2014). However, and unlike early SCADA systems, LoRaWAN networks already have several security features in place, like secure AES-128 channels between end devices and application servers, the dynamic re-keying of OTAA devices' session keys, and the fact that the *AppSKey*, that can be used to encrypt and decrypt data from end devices, is only known to the end device itself and to the application server.

However, there are weak spots that must be considered. For instance, since end devices store all necessary keys after joining a LoRaWAN network, they constitute a target of interest for potential attacks. In fact, when left unprotected, such devices can be subject to physical and key extraction attacks, with ABP-capable devices being particularly vulnerable, as they don't perform re-keying of the session keys. Another example are LoRaWAN gateways: since they receive every packet from all devices within range (thus allowing for eavesdropping) they are prone to denial-of-service attacks, especially if they don't have enough channels to put up with the traffic generated by a large number of devices.

Figure 5 includes some attacks detailed in the available literature (Ningning, H., Xia, X., Zheng, Y., 2022; Yang, X. et al., 2018; Noura, H. et al., 2020; Butun, I. et al., 2022), using the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat model. Such attacks are next described:

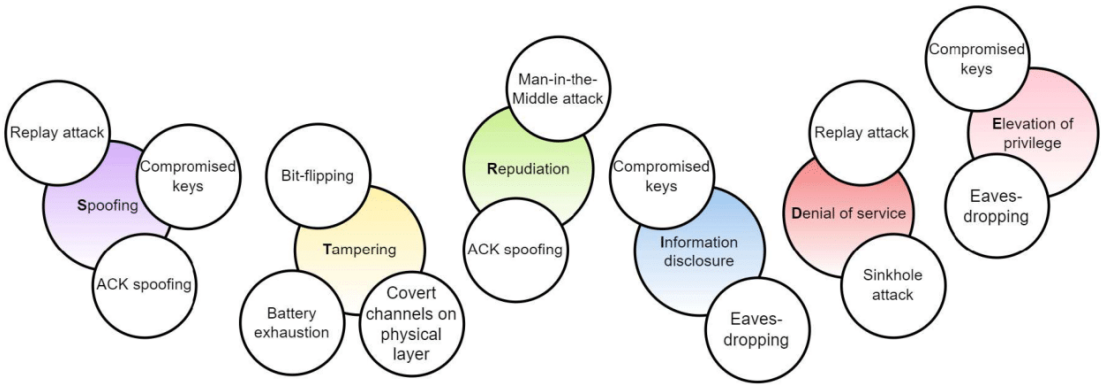

Figure 5: LoRaWAN attack models described in the available literature

- **Replay attack** (Yang, X. *et al.*, 2018; Noura, H. *et al.*, 2020): Frame counters are used to count uplinks and downlinks and are device-specific for connected end devices. Both the end device and the LNS store frame counters. End devices' sent packets can have greater frame counters, with a maximum permitted value, than the expected frame counter, because it's normal for some packets to not reach the LNS, but they can't be lower than the expected frame counter, so the LNS will ignore these packets. Since devices' frame counters reset to 0, if the device is reset or if the frame counter overflows, attackers can use previous higher frame counters and devices' session keys to temporarily end the communication between an end device and the network server. ABP devices are especially susceptible to these attacks as they re-use the same static session keys. LoRaWAN v1.1, addressed this by introducing replay protection mechanisms, as well as proper management of nonces and frame counters.
- **Compromised keys** (Noura, H. *et al.*, 2020): If an attacker has physical access to an end device, they can either alter or copy its firmware, compromising its keys. This allows the attacker to invalidate a device, decrypt uplinks and downlinks, and deploy compromised devices in the network.

- **ACK Spoofing** (Yang, X. *et al.*, 2018; Noura, H. *et al.*, 2020): Since ACK messages do not explicitly state to which message it belongs, only taking into consideration the downlink frame counter, an infected/malicious gateway could retain ACKs sent by the LNS by turning off downlink transmission. When an end device sends a packet, the infected gateway could forward it to the LNS and store the ACK message. The device, if expecting the ACK message, will try to resend the same packet another 7 times, and, if no ACK is received, it will consider the packet to be lost/rejected. Upon receiving a different message by the same end device, the infected gateway can activate downlink transmission and send the previously stored ACK message while dropping the new received message. Since the end device will still have the same downlink frame counter as the one present in the ACK message, it will believe that the most recent transmitted message reached the LNS. LoRaWAN v1.1 addressed this by implementing a message association check mechanism.
- **Bit-flipping** (Yang, X. *et al.*, 2018; Noura, H. *et al.*, 2020): Since the MIC is checked and discarded by the LNS, attackers can alter the transmitted data before it reaches the corresponding application server. This attack has a higher success rate if there are no additional integrity checks implemented in the transmitted data.
- **Battery exhaustion** (Yang, X. *et a*l., 2018): Because class B devices open extra time windows based on the beacons transmitted by the network's gateways, an attacker can send out beacons to a class B network to force the devices to be active for downlink transmission for a long total period of time.
- **Covert channels on physical layer** (Ningning, H., Xia, X., Zheng, Y., 2022): Since amplitude modulation is orthogonal to CSS modulation, amplitude modulated packets aren't detected as being compromised, this allows for covert channels to be deployed in the LoRa physical layer through amplitude modulation.
- **Man-in-the-Middle attack** (Noura, H. *et al.*, 2020; Butun, I. *et al.*, 2022): An attacker can intercept messages sent by the end device and alter the payload, and, if they have access to the NwkSKey (LoRaWAN v1.0.4), or to both the *FNwkSIntKey* and *SNwkSIntKey* (LoRaWAN v1.1), they can then generate a valid MIC and send the packet to a gateway for forwarding to the LNS, where the MIC code is checked and discarded, and the packet is subsequently sent to the corresponding application server.
- **Eavesdropping** (Yang, X. *et al.*, 2018; Noura, H. *et al.*, 2020): As explained for the replay attacks, frame counters are reset to 0 if the device is restarted or if the frame counter overflows. The frame counter is also used as a parameter for the AES-128 algorithm. This means that if the session keys remain the same but the frame counter resets, the keystream for packets with the same frame counter will be equal, and it allows the attacker to XOR cyphers to get XORed plaintexts. An attacker can then guess parts until they're readable and repeat this process to decipher the plaintexts. LoRaWAN v1.1, addressed this by introducing replay protection mechanisms, as well as proper management of nonces and frame counters.
- **Sinkhole attack** (Noura, H. *et al.*, 2020): Infected/malicious nodes can direct traffic through a specific route on the network, for example, disabling some gateways will cause the remaining ones to handle all the network's uplinks and downlinks, which can cause congestion and subsequently, denial-of-service.

Most of these vulnerabilities explore intrinsic properties of the LoRaWAN technology, some of which have been mitigated between different protocol versions. As such, and whenever possible, it is important to try to standardize on recent releases, avoiding exposure to attacks in fallback cases, since LoRaWAN 1.1 allows for backwards compatibility with v1.0.2 devices (Dönmez, T., Nigussie, E. 2018).

While the protection of LoRaWAN networks is outside of the scope of this paper, it becomes evident that the adoption of recent releases for new deployments may provide net benefits in terms of security, but infrastructure operators should learn from past lessons, adopting IEC 62443 recommendations (IEC, 2013) and introducing adequate security countermeasures, such as data diodes (de Freitas et al., 2019), network domain isolation or even virtualized components (Cruz et al., 2013) for streamlined infrastructure update and maintenance.

5. Conclusions

This paper has presented a security-minded introduction to LoRa and LoRaWAN, encompassing aspects such as the origins of these technologies, the motivation behind their creation, as well as other implementation-related aspects and imposed regulations in Europe. Security-wise, it also covered several relevant aspects such as the inherent vulnerabilities of each technology and existing mitigation mechanisms, also including an explanation

on the usage of the AES-128 algorithm in the scope of LoRaWAN and how different versions implement it to generate session keys. Furthermore, LoRaWAN networks were also discussed, detailing its main components and presenting an overview of some attacks studied in the available literature.

One of the main takeout points of this paper has to do with framing known vulnerabilities within the scope of a STRIDE threat model. Besides constituting a systematized perspective about the relevant security aspects to consider when deploying LoRaWAN technologies, it also provides a convenient starting point for preventive and mitigation action planning or risk assessment, providing valuable insights for developing a defense-in-depth strategy focused on the distinct stages of a killchain-like model.

Acknowledgements

This work has been supported by Project "Agenda Mobilizadora Sines Nexus". ref. No. 7113), supported by the Recovery and Resilience Plan (PRR) and by the European Funds Next Generation EU, following Notice No. 02/C05-i01/2022, Component 5 - Capitalization and Business Innovation - Mobilizing Agendas for Business Innovation. This work was also financed through national funds by FCT - Fundação para a Ciência e a Tecnologia, I.P., in the framework of the Project UIDB/00326/2025 and UIDP/00326/2025.

AI Declaration: No AI tools were used to write this paper.

Ethics Declaration: No ethical clearance was needed for the research documented in this paper.

References

Butun, I. *et al.* (2022) 'Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks', *Sensors 2022*, 22(9). doi: https://doi.org/10.3390/s22093498

Cruz, T., Proença, J., Simões, P., Aubigny, M., Oedraogo, M., Graziano, A., & Yasakhetu, L. (2014). Improving cyber-security awareness on industrial control systems: The CockpitCI approach. Journal of Information Warfare, 13(4), 27-41.

Cruz, T., Simões, P., Reis, N., Monteiro, E., Bastos, F. Laranjeira, A. (2013) 'An architecture for virtualized home gateways', 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, Belgium, 2013, pp. 520-526.

de Freitas, M.B., Rosa, L., Cruz, T., Simões, P. (2019). SDN-Enabled Virtual Data Diode. In: Katsikas, S., et al. Computer Security. SECPRE CyberICPS 2018 2018. Lecture Notes in Computer Science, vol 11387. Springer, Cham. https://doi.org/10.1007/978-3-030-12786-2_7

Dönmez, T., Nigussie, E. (2018) 'Security of LoRaWAN v1.1 in Backward Compatibility Scenarios'. Procedia Computer Science, Vol 134, pp. 51-58. doi: https://doi.org/10.1016/j.procs.2018.07.143

European Telecommunications Standards Institute (2018), 'ETSI EN 300 220-2 - Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for access to radio spectrum for non specific radio equipment'. Available at: https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf (Accessed: 28 February 2025)

Ghoslya, S, 'LoRa: Symbol Generation', *All About LoRa and LoRaWAN*. Available at: https://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html (Accessed: 16 February 2025)

IEEE (2011), 'IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4TM-2011 (Revision of IEEE Std 802.15.4-2006), September 2011.2687'.

International Electrotechnical Commission (2013), 'IEC 62443-3-3}- Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels".

LoRa Alliance (2017) *LoRaWAN® Specification v1.1*. Available at: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 (Accessed: 15 February 2025)

LoRa Alliance (2020) *TS001-1.0.4 LoRaWAN® L2 1.0.4 Specification*. Available at: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification (Accessed: 15 February 2025)

LoRa Alliance (2022) *LoRaWAN® Leads Global, At-Scale LPWAN Deployments Across All Metrics: Most Solutions, Devices Deployed, Messages Sent and Network Availability*. Available at: https://lora-alliance.org/lora-alliance-press-release/lorawan-leads-global-at-scale-lpwan-deployments-across-all-metrics-most-solutions-devices-deployed-messages-sent-and-network-availability/ (Accessed: 15 February 2025)

Murata, *What is the realistic range of LoRa? What is the actual range that can be achieved?*. Available at: https://www.murata.com/support/faqs/lpwa/lora/hardware/0008 (Accessed 15 February 2025)

Ningning, H., Xia, X., Zheng, Y. (2022) 'CloakLoRa: A Covert Channel Over LoRa PHY', *IEEE/ACM Transactions on Networking*, 31(3), pp. 1159 – 1172. doi: https://doi.org/10.1109/tnet.2022.3209255

Noura, H. *et al.* (2020) 'LoRaWAN security survey: Issues, threats and possible mitigation techniques', *Internet of Things*. doi: https://doi.org/10.1016/j.iot.2020.100303

Semtech Corporation (2024a) *LoRa® and LoRaWAN®*. Available at: https://www.semtech.com/uploads/technology/LoRa/lora-and-lorawan.pdf (Accessed: 15 February 2025)

Semtech Corporation (2024b) *Sending and Receiving Messages*. Available at: https://www.semtech.com/uploads/technology/LoRa/sending-and-receiving-messages.pdf (Accessed: 15 February 2025)

Semtech Corporation (2024c) *LoRaWAN® Device Classes*. Available at: https://www.semtech.com/uploads/technology/LoRa/lorawan-device-classes.pdf (Accessed: 15 February 2025)

Slats, L. (2020) 'A Brief History of LoRa®: Three Inventors Share Their Personal Story at The Things Conference', *Semtech's Corporate Blog*, 8 January. Available at: https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference (Accessed: 15 February 2025)

Tektelic, *What is Chirp Spread Spectrum | TEKTELIC Glossary*. Available at: https://tektelic.com/what-it-is/chirp-spread-spectrum/ (Accessed: 15 February 2025)

The Things Industries *Join Server | The Things Stack for LoRaWAN*. Available at: https://www.thethingsindustries.com/docs/concepts/architecture/components/join-server/ (Accessed: 15 February 2025)

The Things Network (2025a) *What are LoRa and LoRaWAN? | The Things Network*. Available at: https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/ (Accessed: 15 February 2025)

The Things Network (2025b) *EU863-870 MHz Band | The Things Network*. Available at: https://www.thethingsnetwork.org/docs/lorawan/regional-parameters/eu868/ (Accessed: 15 February 2025)

The Things Network (2025c) *LoRa Physical Layer Packet Format | The Things Network*. Available at: https://www.thethingsnetwork.org/docs/lorawan/lora-phy-format/ (Accessed: 15 February 2025)

The Things Network (2025d) *Regional Limitations of RF Use in LoRaWAN*. Available at: https://www.thethingsnetwork.org/docs/lorawan/regional-limitations-of-rf-use/ (Accessed: 15 February 2025)

The Things Network (2025e) *LoRaWAN Architecture | The Things Network*. Available at: https://www.thethingsnetwork.org/docs/lorawan/architecture/ (Accessed: 15 February 2025)

Yang, X. *et al.* (2018) 'Security Vulnerabilities in LoRaWAN', *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 129-140. doi: https://doi.org/10.1109/IoTDI.2018.00022