IoT using LoRaWAN: a security analysis*

Anne-Carole Honfoga[1,2,*,†], Michel Dossou[2,†] and Véronique Moeyaert[1,†]

[1]Electromagnetism and Telecommunications Department, Faculty of Engineering (FPMs), University of Mons, Mons, Belgium
[2]Research unit in photonics and wireless communications, LETIA/EPAC University of Abomey-Calavi, Abomey-Calavi, Benin

Abstract

Internet of Things (IoT) refers to the process of connecting cyber-physical objects to the Internet, enabling the exchange of data over wireless communication networks with limited human intervention. These communication networks use licensed spectrum or unlicensed spectrum. Instead of licenced spectrum used by Narrowband Internet of things (NB-IoT) and Long-Term Evolution for Machines (LTE-M), SigFox, MIoTy, and Long Range Wireless Area Network (LoRaWAN) employ unlicenced spectrum for communication between the network entities. Among wireless networks using unlicensed spectrum, LoRaWAN is the most used network in many applications (smart farming, smart building, smart metering) but its presents several vulnerabilities. This paper studies the LoRaWAN threats, malicious attacks and mitigation against attacks.

Keywords

IoT, LoRa, LoRaWAN, Network Security, Vulnerability, Attack

1. Introduction

Internet of Things (IoT) is an essential element that has revolutionized the Information and Communication Technology sector (ICT). Over the past decade, it has been the focus of much academic and industrial interest, with the purpose of making buildings, cities, agriculture and environment smart. This technology refers to the process of connecting cyberphysical objects (machines) to the Internet, enabling the exchange (sending and receiving) of data over wireless communication networks with limited human intervention. These machines are embedded devices which present characteristics such as a low energy consumption, a low computing power, a small size, a small price and a capacity to communicate within a wireless network. There are many wireless communication networks classified in terms of energy consumption and communication range. In terms of energy consumption, they can be divided into low power communication (NFC – Near Field Communication, RFID – Radio Frequency Identifier, Z-Wave, Zigbee, BLE – Bluetooth Low Energy, LTE-M – Long Term Evolution-Machine, NB-IoT – Narrowband IoT, SigFox and LoRaWAN) and high-power communication technologies (Bluetooth, Wi-Fi – Wireless Fidelity, 3G, 4G and 5G). Regarding the communication coverage, there are short range communication networks (< 1km) (e.g. NFC, RFID, Wi-Fi, Bluetooth, BLE, Z-Wave and Zigbee) and long-range communication networks (1-15 km) (3G, 4G, 5G, LTE-M, NB-IoT, Sigfox, and LoRaWAN) [1].

LoRaWAN is a low cost, low power and long-range communication network that is developed to fill a gap in IoT communications. Using this technology belonging to Low Power Wide Area Networks (LPWAN), sensors or actuators can send signals over 5 km in urban areas and up to 15 km in sub-urban areas. Instead of licenced spectrum used by LoRaWAN's main competitors (a.k.a other LPWANs) like NB-IoT and LTE-M, LoRaWAN employs unlicenced spectrum for communication between the network entities [1]. These advantages allow LoRaWAN to be considered as the technology that is improving the operations of many industrial sectors (e.g. agriculture, environment) as a large-scale remote monitoring is then possible. However, like any computer network, and particularly wireless network, this technology suffers from many security problems that can be defined following the three security criteria: availability, integrity and confidentiality. Many specifications of LoRaWAN have been published since its development by Semtech Corporation [2]. The security of these technologies has been improved with the specification version. Indeed, the first version presents more vulnerabilities than the latest version 1.1.

This paper reviews LoRaWAN attacks, vulnerabilities and security measures. It provides a short review and an analysis of LoRaWAN robustness and gives perspectives about the robustness improvement. The outline of the paper is presented as follows: the theoretical background is described (§II), the literature review is presented (§III), the paper is finalized by the conclusion (§IV).

2. Theoretical background

2.1. Introduction to LoRaWAN

Before explaining the behaviour of LoRaWAN protocol, let us compare LoRaWAN to the LoRa (Long Range) modulation. LoRa is the modulation type used between two LoRa devices or between a LoRa device and a gateway (cf Fig. 1). The LoRaWAN term is employed when end-devices can communicate with the LoRaWAN servers. LoRaWAN is the extended version of LoRa technology which connects end-devices to the network server. It includes LoRa modulation that operates at the physical layer of the network. Fig. 1 shows the LoRaWAN topology.

LoRaWAN network includes three sub networks. There is the LoRa radio frequency network presenting a star topology, the backhaul network connecting Gateways and Network Servers using Mesh topology or partial Mesh topology and the backhaul network connecting Network Servers with Join and Application Servers. Beside the two servers (Network Server and Application Server) used in LoRaWAN v1.0, a new server called Join Server is added in LoRaWAN v1.1 to manage the OTAA (Over the Air Activation) procedure more securely. The Join Server has been added in the network to orchestrate in a more secure way the join-

Cotonou'24: Conférence Internationale des Technologies de l'Information et de la Communication de l'ANSALB, June 27–28, 2024, Cotonou, BENIN
*You can use this document as the template for preparing your publication. We recommend using the latest version of the ceurart style.
*Corresponding author.
†These authors contributed equally.
anne-carole.honfoga@umons.ac.be (A. Honfoga)
0000-0002-0550-2611 (A. Honfoga)

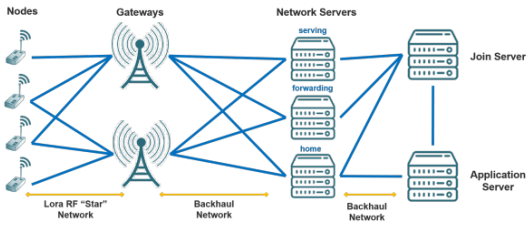

Figure 1: Network architecture of LoRaWAN v1.1 [3]

ing procedure used by end-devices (LoRa devices) to join the network. Also, LoRaWAN v1.1 integrated roaming and mobility techniques for the end-devices by employing extra servers called Join Server (JS), forwarding Network Server (fNS), serving Network Server (sNS).

2.1.1. End-devices joining procedures

The joining procedure creates mutual authentication between an end-device and the LoRaWAN network to which it is linked. Two joining procedures are used to connect the end-devices to the servers. There are Activation By Personalization (ABP) and Over-The-Air Activation (OTAA). Among them, OTAA procedure is the more secure. It provides a more flexible and secure way to establish session keys with the network servers. In OTAA, authentication is required for devices using two different keys for each device that are generated each time the device joins the network: Network session Key (NwkSKey) and the Application session Key (AppSKey). Using two different keys makes it is more difficult to tamper with or read application data, even if one of the keys has been compromised. These keys are generated during the two root keys (NwkKey and AppKey) design. The ABP procedure is not so secure as the end-devices are directly connected to the network without join request and join-accept procedures [1]. Indeed, instead of key generation during each section, the Network section Key and the App section Key are directly defined and stored in the device. This ABP method presents vulnerabilities. By modifying these keys, communications between the device, the gateway and the network server can be seen or intercepted by anyone if the device is connected to the gateway and Network Server. Let us note that the Network section Key and the Application section Key are generated using the same root Key in LoRaWAN v1.0 whereas in LoRaWAN v1.1 the application root key is different from the Network root key. The AppKey and NwkKey are generated using the AES-128-bit encryption method. These keys are specific to each end-device and embedded into the end-device during its fabrication. A Message Integrity Code (MIC) is computed once the encryption is done and is calculated over all the Message Authentication Code (MAC). It ensures the integrity of the message. MAC is used to check the messages and the authentication, ensuring that the integrity of the data has not been altered during transmission. The integrity is protected hop-by-hop. LoRaWAN exploits various methods for generating the MIC depending on the direction of the message, uplink, or downlink [4]. The MIC check is performed on the data to avoid data tampering without the Network section key (NwkSKey). Table 1 presents the comparison of OTAA and ABP procedures.

Table 1
Comparison of end-devices activation procedures

OTAA	ABP
End-device companies generate fundamental provisioning parameters.	The commissioning process is simplified and then less secure.
Secure keys can be refreshed regulary. Then high-level, tamper-proof security options are accessible.	End-devices and Keys are customized during manufacturing.
End devices can stock various "identities" to change network and operator dynamically and securely over their lifetime.	End-devices become directly operational upon powering up.

2.1.2. Device classes: A, B and C

Three kinds of operation for devices are defined in LoRaWAN: class A, class B, and class C. All end-devices must support class A operation. class A device can not receive signal from the gateway if an uplink transmission has not been yet transmitted. It represents the device class in which the end-device spends more time in sleep mode. Only two receive windows are scheduled for down-link messages reception. Class B device can be regularly joined without a previous uplink transmission. It offers regularly-scheduled, fixed-time opportunities for an end-device to receive downlink messages from the gateways, allowing class B end-devices convenient for sensors and actuators monitoring. Class C device can always be joined. It is always listening for downlink messages, unless they are transmitting uplink messages. Like class A device, class C device implements the same two receive windows, but it does not close the second reception window until it sends the next transmission back to the network server. The class C device is a power consuming device compared to the class B device which in turn consumes more energy than the class A device [1] (cf Fig. 2).

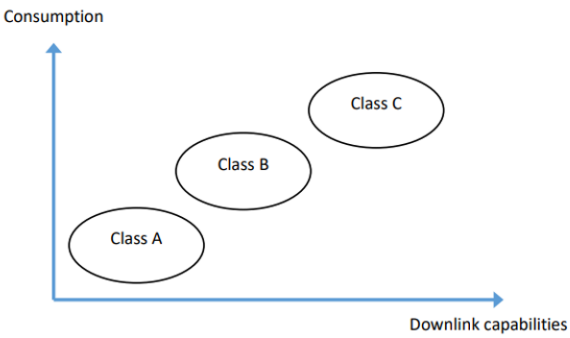

Figure 2: Power consumption and downlink capabilities [1]

2.2. Security Analysis

LoRaWAN security challenges are related to different parts of the network. The main parts are the network entities (gateways, servers, and end-devices), the key distribution methods, the network implementation, and the roaming

techniques integrated in LoRaWAN v1.1, and the backward compatibility challenges. In this section, LoRaWAN vulnerabilities and attacks are presented.

2.2.1. LoRaWAN vulnerabilities

Network security vulnerabilities are weaknesses within the system's software, hardware, or organizational processes. Their can be either non-physical or physical. The main vulnerabilities of LoRaWAN are: the long times communication induced by Long Range transmission, the coexistence problem of LoRa, and backward compatibility challenges.

- **Long times communication induced by Long Range transmission**
  Spreading Factor (SF) is a parameter used in spread spectrum modulation techniques like Long Range (LoRa) modulation, to control the spreading of a signal over a wider bandwidth. The larger SF is, the longer the distance the device can receive or transmit. Eight Spreading Factor (SF5, SF6, SF7, SF8, SF9, SF10, SF11 and SF12) are used in LoRa transmissions whereas in LoRaWAN six SF are used (SF7 to SF12). The elapsed time on air of a LoRaWAN messages increases with the Spreading Factor (SF) and then the transmission distance. Indeed, the time on air increases with the symbol transmission time (T_{symbol}) (1). The symbol transmission time is defined by the formula (2). For a fixed bandwidth, the symbol transmission time increases with the spreading factor value (cf Fig. 3). In particular, symbol duration increases by a factor of 2 from one SF to the next. As shown on this figure, the start frequency (low frequency) is the channel frequency (center frequency) minus the channel bandwidth divided by two. The final frequency (high frequency) is the channel frequency plus the channel bandwidth divided by two.

$$Time - on - Air = n_{symbol} \times T_{symbol} \quad (1)$$

$$T_{symbol} = \frac{2^{SF}}{Bandwidth} \quad (2)$$

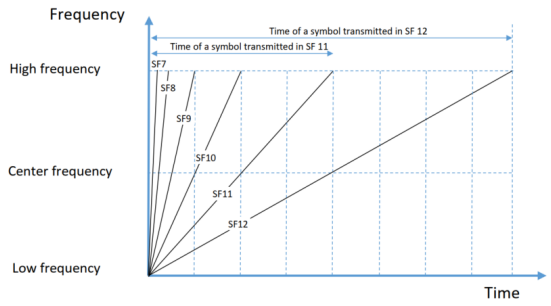

Figure 3: Symbol transmission time [1]

As high SF (up to SF12) is required for the network edge end-devices to communicate with the gateway, a mock device can intercept messages or falsify packets intended for the gateway. Furthermore, there is no time-related information in LoRaWAN packet. As LoRaWAN packet structure does not include any time-based signature or data to validate the time of the message, this vulnerability is used to employ a wormhole attack.

- **Coexistence problem of LoRa**
  LoRa transmission is sensible to interference issues such as interference from Cellular Networks (Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), and Long Term Evolution (LTE)) (which can make less sensitive LoRa receivers, making it hard to receive weak signals) and In-Band and Out-of-Band interference [5]. In-band interference occurs when other devices operate on the same or adjacent channels, while out-of-band interference comes from strong signals outside the useful band. When LoRa transmissions are performed at the same frequency using the same spreading factor in the same area (In-Band interference), they can interfere with each other. This LoRa physical Layer vulnerability can be exploited for jamming attack as this transmission is performed using unlicensed spectrum.
- **Backward compatibility challenges**
  Backward compatibility problems occur when a newer version of a software or hardware system is not able to work with the data or functionality of an older version. In LoRaWAN security case, LoRaWAN v1.1 aims to improve security, but it may be difficult to ensure backward compatibility with devices using earlier versions (v1.0). In fact, the Network Server is responsible for deciding which protocol version to exploit and chooses the highest common version between itself and the End-Device (ED). As LoRaWAN v1.0 presents more security weaknesses than LoRaWAN v1.1, the backward compatibility offered by the evolved version could constitute a vulnerability.

2.2.2. LoRaWAN attacks

- **Jamming attack**
  Radio Jamming attack consists in disrupting the LoRa radio transmission by transmitting a powerful radio signal in the proximity of application devices. It is possible to jam LoRa messages using well timed malicious transmissions. This attack is usually performed using a dedicated hardware (ie Commercial-off-the-shelf (COTS)) to jam LoRa devices. There are no real countermeasures to prevent this attack. But network administrators can easily detect jamming when devices transmitting into the network start to disappear. They may then decide to switch to another frequency in the band to avoid the impact of jamming.
- **Selective jamming attack**
  Selective jamming constitutes the most sophisticated and efficient jamming technique which could be effective using a COTS hardware by extending the jammer with additional software to target a specific device address [2]. Selective jamming only jams selected devices or messages. As other devices or messages on the network are not jammed, it can be much more difficult for the network operator or administrator to decide whether an ED is being jammed, or whether some other technical problem has occurred. Then, the countermeasures available for the classical jamming attack are not possible in the case of selective jamming attack.

- **Replay attack**
  Replay attack is performed on security protocol by repeating the available data transmitted by malicious entity Fig. 4). Replay attack is an attack on the security protocol that consists in resending captured messages from the end-devices. Its objective is in the Denial of Service of an end-device This attack is possible using the communication frequencies and channels to sniff data from transmission between devices (end-devices and Gateways). Predator may intercept and replay legitimate messages, compromising the network's security. The use of frame counters process helps LoRaWAN network to know if the message is sent by the gateway instead of a malicious device. Indeed, once the end-device is activated, both frame counters (from the end-device and the gateway) are set to 0, and each message coming from the gateway, or the device increments the counters. By this way, if a message is received with a lower frame counter than the last message, it is ignored. But this process could be exploited by attackers to produce a Denial of Service.

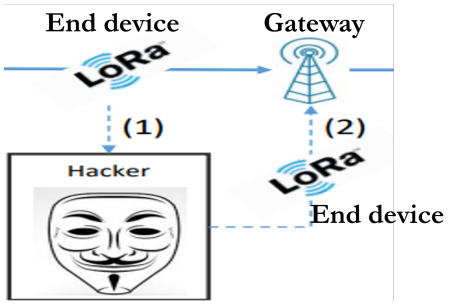

Figure 4: Attack replay

- **Wormhole attacks**
  A wormhole attack is an attack which can be performed against a LoRaWAN network. This attack consists in packet sniffing and replaying them. One malicious device captures the packets from one device and transmits them to another distant located device to replay the captured packet. The two devices which participate to this attack are the sniffer and the jammer. The sniffer captures packets and, transmits signal to the jammer informing that it apprehended the packet [2]. By this way, the packet does not reach the gateway and is still active for validation. This packet could be forwarded to the gateway at any time as there is no time related information in LoRaWAN messages.
- **Eavesdropping**
  As already presented, LoRaWAN implements channel confidentiality through AES in counter mode, where the block counter value is exploited as an input. During a counter reset, the key will remain in place, meaning that the block cipher will reconstitute the same key material. An attacker can exploit this comportment to decrypt messages.
- **Bit-Flipping Attack (Man-in-the-Middle, MitM)**
  LoRaWAN messages are encrypted and carry a MIC. But the encryption and the integrity check are managed at different locations inside a message frame. The payload encryption is handled by the Application Server, while the MIC is checked and terminated by the infrastructure provider (Network Server (NS)) [6]. Then, between the infrastructure provider's network server and the IoT solution provider's Application Server (AS), the content can not be checked for integrity and authenticity. An attacker can attempt to intercept anywhere between the NS and the AS. This attack can be achieved through a variety of approaches, ranging from routing-based approach, such as Border Gateway Protocol (BGP) Route hijacking or IP source routing, to physical and link layer-based ones, such as a compromised device on the path [7]. This attack consists in the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using BGP protocol.
- **Rogue gateway attack**
  LoRaWAN gateways are obeying relays and then constitute the weakest link of the network. Any kind of security problem on this node would interrupt communication between the end-devices and the servers. One of the attacks faced by LoRaWAN gateways is the use of a rogue gateway that acts like as a legitimate gateway. One can distinguish two kind of attacks: LoRa class B attack (beacon synchronization Denial of Service (DoS) attack) and Impersonation attack.
  - Beacon synchronization DoS attack
    This attack is a typical malicious gateway attack that use class B device vulnerability. In LoRaWAN, class B beacons received in downlink transmission are not secured by any methods, indicating that an attacker can deploy a malicious gateway to send counterfeit beacons. The result is that class B end-devices will receive messages in windows out-of-sync with the malicious gateway. By sending out beacons randomly a malicious gateway could desynchronize an end device from receiving windows of another gateway. This could cause a denial of service, as the legitimate gateway sends messages when the end device is not receiving. To deal with this attack, a key should be exploited by gateways to authenticate beacons communications.
  - Impersonation attack
    Gateways can also be impersonated to create attacks against end-devices. End-devices can be listened to and their network address can be determined. Furthermore, a triangulation method (minimum 3 gateways are required in this case to perform the intended capturing attack the end-device).

  Besides the attacks previously presented, there are also network spoofing attack, selective forwarding attack, sinkhole or blackhole attack ... In the following section, a short literature review of papers about LoRaWAN security is presented.

3. Literature review

Table 2 presents a literature review on papers related to LoRaWAN security.

Table 2
Paper summary

Ref (Year)	Objectives	Summary of concept	Results
[2] (2017)	Analysis of potential security weaknesses in LoRa. The network stack is analysed and ED vulnerabilities are presented.	LoRa transmissions are prone to selective jamming (with a commercial off-the-shelf hardware) attacks, replay attack and wormhole attack.	A COTS device is used for jamming test.
[3] (2019)	Analysis of the security risk of LoRaWAN v1.1 by presenting the main security improvement compared to LoRaWAN v1.0.	It presents a related work on security risk of LoRaWAN v1.0. It also highlights security vulnerabilities of LoRaWAN v1.1., possible attacks and defense mechanisms against these attacks	These problems affect the network availability, the data integrity and confidentiality, and mechanisms are proposed.
[7] (2019)	Analysis of the practical capacity of LoRaWAN and its security challenges.	Description of LoRaWAN v1.1 from the joining procedure handling to the keys management, attacks, and network capacity	Main attack: Class B synchronization attack (Beacon transmission by attackers) and Jamming
[8] (2020)	Analysis of LoRaWAN v1.1 security by comparing its vulnerabilities to those of LoRaWAN v1.0	Description of LoRaWAN about data and control packet types, identifiers and keys management (1.0 vs 1.1), ED joining procedure), and PHY attacks (continuous, selective or triggered jamming)	Main attacks: confidentiality (session key Reuse), integrity (bit flipping and ACK spoofing), availability (class B desynchronization), authentication (MiTM).
[4] (2020)	Comprehensive analysis of LoRaWAN versions (1.0.1, 1.0.2, 1.1, 1.0.3) regarding ED, LoRaWAN layers, hardware and operating systems.	Classification of LoRaWAN threat regarding security criteria such as availability, authentication, integrity and confidentiality and analysis of the risk degree of them.	Matching of threats to each attack and mitigation measures LoRaWAN v1.1 security comparison to 1.0.2 vulnerabilities
[9] (2021)	Implementation of three forms of reactive jamming attack and countermeasures for attack mitigation	Reactive jamming using Channel Activity Detection (CAD) mechanism detection, using a combination of channel hopping and transmission, and using CAD detection, channel hopping and transmission	A low-cost commodity hardware based on Arduino platform can be used by attackers to completely interrupt the network

4. Conclusion

This paper presents a security analysis of LoRaWAN v1.1. The main vulnerabilities and attacks are summarized. It gives a review on papers that address this network security. It is shown that the main physical layer security attacks are jamming and attack replay while other attacks can affect the network availability, integrity and confidentiality.

5. Acknowledgments

This work has been carried out under support from the ARES within the frame of a post-doctoral mobility grant in the Electromagnetism and Telecommunications Service (UMONS/FPMs/Belgium).

References

[1] S. Montagny, LoRa-LoRaWAN and internet of things for beginners, Available: www. univ-smb. fr/lorawan (2021).

[2] E. Aras, G. S. Ramachandran, P. Lawrence, D. Hughes, Exploring the security vulnerabilities of LoRa, in: 2017 3rd IEEE international conference on cybernetics (CYBCONF), IEEE, 2017, pp. 1–6.

[3] I. Butun, N. Pereira, M. Gidlund, Security risk analysis of LoRaWAN and future directions, Future Internet 11 (2018) 3.

[4] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, A. Chehab, LoRaWAN security survey: Issues, threats and possible mitigation techniques, Internet of Things 12 (2020) 100303.

[5] K. Michel Gilbert, LoRaWAN gateways: Radio coexistence issues and solutions, LoRa Alliance (2021).

[6] F. Kuntke, V. Romanenko, S. Linsner, E. Steinbrink, C. Reuter, LoRaWAN security issues and mitigation options by the example of agricultural iot scenarios, Transactions on Emerging Telecommunications Technologies 33 (2022) e4452.

[7] M. Santamaria, A. Marchiori, Demystifying LoRaWAN security and capacity, in: 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, 2019, pp. 1–7.

[8] S. J. Philip, J. M. McQuillan, O. Adegbite, LoRaWAN v1. 1 security: Are we in the clear yet?, in: 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys), IEEE, 2020, pp. 112–118.

[9] T. Perković, H. Rudeš, S. Damjanović, A. Nakić, Low-cost implementation of reactive jammer on LoRaWAN network, Electronics 10 (2021) 864.