Review of Security Vulnerabilities in LoRaWAN

Junaid Qadir[1](✉), Ismail Butun[2], Paolo Gastaldo[1], and Daniele D. Caviglia[1]

[1] Department of Electrical, Electronic and Telecommunications Engineering and Naval Architecture (DITEN), University of Genoa, 16145 Genoa, Italy
junaid.qadir@edu.unige.it, {paolo.gastaldo,daniele.caviglia}@unige.it
[2] Department of Electrical Engineering and Computer Science, KTH Royal University of Technology, 100 44 Stockholm, Sweden
butun@kth.se

Abstract. The realm of Low Power Wide Area Network (LPWAN) has a paramount influence on the way we work and live. For instance, real-time applications and rapid packet transiting for long-range have now come into practice that was previously considered mysterious. However, euphoria becomes a problem when it comes to security considerations, as low-power devices possess limited processing units that are unable to elucidate robust security algorithms. In this case, the Low Power Wide Area Network (LoRaWAN) stepped into a technological competition that filled the gap by adopting the end-to-end security feature. Though, LoRaWAN protocol entails fundamental security requirements but the implementation matters. This paper presents security analyses in the LoRaWAN networks. In addition, we provide a bibliometric overview of security considerations in LoRaWAN that helps researchers for thorough insights and implementation.

Keywords: IoT · LoRaWAN · Security · Vulnerability · Confidentiality · Integrity · Authenticity · Bibliometric

1 Introduction

The magical appearance of the Internet of Things (IoT) has made communication convenient between physical objects without human intervention. Thus, the word IoT refers to the interconnected devices that detect, collect, and transmit data across the world via existing Internet infrastructure. As per technological prediction by Statista[1], there is expected more than 30.9 billion devices will be connected seamlessly with each other on global Internet.

Several communication protocols have already opened opportunity for IoT devices. For example, ZigBee, Bluetooth, and RFID have revealed their use for IoT resource restricted devices, because of low energy consumption. However,

[1] https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide.

R. Berta and A. De Gloria (Eds.): ApplePies 2022, LNEE 1036, pp. 248–254, 2023.
https://doi.org/10.1007/978-3-031-30333-3_33

they are unable to continue operation for applications requiring coverage for large distance.

Low Power Wide Area Network (LPWAN) enables communication links over long range with low energy consumption. Popular LPWAN technologies including, Long Range Wide Area Network (LoRaWAN) [1], SigFox [6], Narrowband-IoT (NB-IoT) [7] are the most widely used in different use cases. As these technologies provide communication over several kilometers (km); therefore, security for the transmitted packet is the major concern in LPWAN. SigFox provides communication without having consideration of security features, while the NB-IoT possess basic LTE-encryption. Therefore, LoRaWAN is the most preferred choice as it provides strong end-to-end security. By design, LoRaWAN is highly secured as it considers confidentiality and authenticity using many security keys; nonetheless, the network's implementation matters if these keys are kept insecure or reused the same cryptographic numbers.

LoRa is developed by Semtech Inc., Camarillo, CA, USA, which is a physical layer whereas LoRaWAN is the upper layer of LoRa, which defines the communication protocol and system architecture. Together with LoRa, it enables communication over very long distance on local, national and international (using roaming) level, with extremely low power consumption. LoRaWAN system architecture consists of end-device, gateway, network server, application server, and join server (LoRaWAN v1.1). The end-device uses radio waves to communicate with the gateway and utilizes the chirp spread spectrum (CSS) modulation technique [2], which possess the same characteristic as frequency-shift keying (FSK) modulation used in many legacy wireless communication system. However, it is immune to interference therefore increases the communication range. The end-device can be activated using two different methods such as; Activation by Personalization (ABP) and Over-The-Air Activation (OTAA). The only difference between two activation is as the ABP activation stores the security keys permanently, while the OTAA generates security keys dynamically.

Security in LoRaWAN is evolving as it is a constant target of malicious actors [8]. Several security challenges including replay attacks, bit flipping attacks, key management related attacks that affect confidentiality, integrity, and availability are confronted in the literature. And the LoRa Alliance is constantly enhancing the protocol to ensure it stays ahead of the changing security landscape. This paper discusses security vulnerabilities and privacy issues in LoRaWAN specification. We discuss cybersecurity breaches in LoRaWAN off-the-shelf that exhibits several attacks scenario targeting end-device, gateway, and network server. In the last, a bibliometric overview is given, that provides a thorough insights for researchers and engineers looking to deploy LoRaWAN infrastructure and enhance it's security in the future.

2 Cyber Risks and Threats in LoRaWAN

This section discusses cybersecurity risks and threats analysis in LoRaWAN. Though, LoRaWAN specification has been introduced by employing strong security layers. However, some well-known weaknesses have been pinpointed that come with high risks. Therefore, our aim is to highlight security vulnerabilities and privacy issues in LoRaWAN implementation. Several threats and attacks are follows as below

2.1 Confidentiality

Confidentiality is the practice of maintaining data security using conventional cryptographic encryption techniques. The data is considered to be not confidential if disclosed to the intended audience. The following list includes numerous attacks that compromise LoRaWAN's confidentiality:

- Keys Related Vulnerabilities: LoRaWAN security is heavily dependent on security keys, and the implementation becomes vulnerable if the keys are comprised. There are numerous ways to expose keys that are highlighted in [4] including reverse engineering of device, keys disclosure, device tags, hardcoded keys in open source code, and non random keys etc.
- Plain-text Key Capture: Cerrudo et al. [4] published a white paper and mentioned that the LoRaWAN network can be compromised if the text files containing the keys of the end device are shared on the Internet, or not used hardware security module (HSM).
- Eavesdropping Attack: LoRaWAN employs AES in counter mode to ensure the confidentiality of the packet. However, still the ABP devices are vulnerable to eavesdropping attack as these devices use the same encryption keys for long time. Noura et al. in [10], investigated that if two ciphertexts are encrypted with the same key stream, then the attacker may able to decrypt the message by XORing both ciphertexts and can get the original message.

2.2 Integrity

Integrity is the essential step of cybersecurity as it preserves the data from being added, changed, or deleted during transmission from a source to the destination. Attacks that compromise LoRaWAN integrity are discussed below.

- Bit Flipping Attack: In this attack, an attacker intercepts the cipher message and modify the message by adding, changing, and deleting a single or number of bits. As a result, the application server receives a modified version of the packet. In LoRaWAN, the packet is only encrypted using AES counter mode (CTR-mode) that provides XOR operation instead of shuffling the bits. Therefore, the authors in [11] discuss that LoRAWAN is susceptible to Bit-Flipping attack as the attacker can modify the message between the network and application servers.

- Device Cloning: Due to the low cost, the LoRaWAN end-devices are becoming ubiquitous, and attackers with access to the device physically can clone the firmware. Cloning the firmware can compromise the device and expose it to integrity breaches [9].

2.3 Availability

Availability ensures the presence of the network and system while requested by the user. There are numerous attacks that could jeopardize the availability of LoRaWAN.

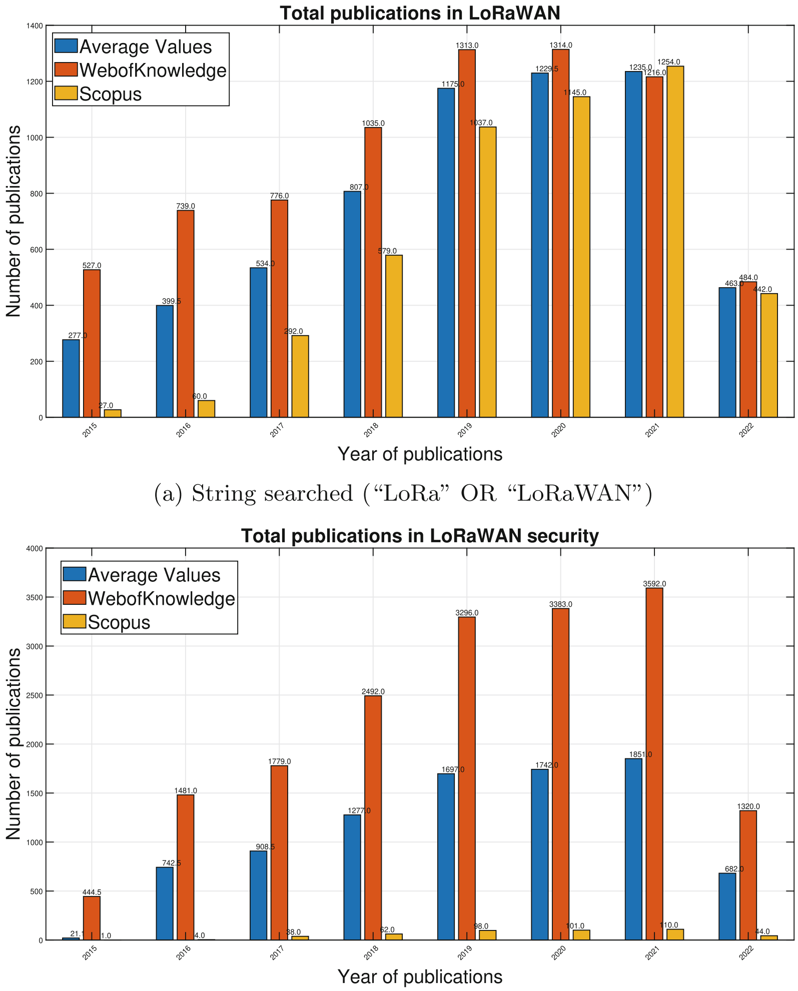
- Replay Attack: Replay attack affects denial-of-service (DoS) of the end-device in LoRaWAN, and consists of re sending the capture messages in the edge of the network. Replay attack issue has been resolved in the new version of LoRaWAN, however, the ABP activated devices remain vulnerable to this attack. In LoRaWAN, the end-devices use two counters such as the uplink and the downlink counters. So, these counters increase with every message. And the value resets until it reaches the maximum value [11]. In replay attack, the attacker hands on the message with higher counter value and injects it when the gets start from the 0. In this case, the network server considers the injected message as legitimate and received a false packet from the attacker.
- Wormhole Attack: The authors in [5] discuss to perform the wormhole attack, it is therefore, needed to have a sniffing and a jamming tool to block the packet sent from the end-device. Consequently, the packet gets lost the destination and can exploit it for the whole network in the form of replay for a time being.
- Selective Forwarding Attack: It is a routing related attack which severally affect the network availability. In LoRaWAN implementation, the attacker choose the packet and can selectively forward it in order to block other end-devices in the network [3].

3 Bibliometric Overview

This section presents the bibliometric overview of LoRaWAN. We collect the data from two different major databases i.e., Scopus[2] and WebofKnowledge[3]. Then, we perform the string such as ("LoRa" OR "LoRaWAN") AND ("Security" OR "Cybersecurity"), and collect all values from each database. Finally, the overall value has recorded graphically using Matlab. Figure 1(a) shows publication record started from 2015 until 2022 and the maximum publications have

[2] https://www.scopus.com/.

[3] https://www.webofknowledge.com/.



(a) String searched ("LoRa" OR "LoRaWAN")

(b) String searched ("LoRa" OR "LoRaWAN")AND("Security" OR "Cybersecurity")

Fig. 1. a) Total number of papers published in LoRaWAN, b) Total papers published in LoRaWAN security.

been recorded in the year of 2020. Furthermore, the number of publications in LoRaWAN security is shown in Fig. 1(b). In addition, Table 1 shows the number of papers that addressed the following attacks.

Since the data were collected in mid 2022, the final numbers on 2022 data are incomplete and should not mislead the reader. The trend within the last decade shows that the 2022 numbers might surpass 2021.

Table 1. Papers dealt with various attacks

String searched	Papers dealt with attacks		Type of documents	
Attacks	Scopus	WebofKnowledge	Article (S+W)	Conference proceedings (S+W)
"LoRAWAN" AND "Key related vulnerabilities"	1	1	(1),(1)	(0),(0)
"LoRAWAN" AND "Plain-text Key Capture"	0	0	(0),(0)	(0),(0)
"LoRAWAN" AND "Eavesdropping Attack"	11	8	(3),(3)	(8),(5)
"LoRAWAN" AND "Bit Flipping Attack"	5	3	(1),(1)	(4),(2)
"LoRAWAN" AND "Device Cloning"	1	1	(0),(0)	(1),(1)
"LoRAWAN" AND "Replay Attack"	35	25	(11),(10)	(24),(15)
"LoRAWAN" AND "Wormhole Attack"	2	1	(0),(0)	(2),(1)
"LoRAWAN" AND "Selective Forwarding Attack"	0	0	(0),(0)	(0),(0)

(S+W) = Scopus +WebofKnowledge

4 Conclusion

LoRaWAN is an emerging protocol that has received widespread acceptance across a variety of useful applications in numerous regions. It advances the packet by keeping in view several security encryption techniques, but there are several flaws that could compromise LoRaWAN's security and privacy. In this paper, we present cybersecurity vulnerabilities of LoRaWAN protocol that previously associated with LoRaWAN implementation. In addition, the bibliometrics overview is presented by providing the number of papers published within the last decade on the cybersecurity of LoRaWAN vs. overall publications in LoRaWAN.

References

1. Alliance, L.: what is lorawan. https://lora-alliance.org/resource_hub/what-is-lorawan/. Accessed March 12 2022
2. Butun, I.: Towards smart sensing systems: a new approach to environmental monitoringsystems by using lorawan. In: 2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC). IEEE (2022)
3. Butun, I., Pereira, N., Gidlund, M.: Analysis of lorawan v1. 1 security. In: Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, pp. 1–6 (2018)
4. Cerrudo, M.C., Fayo, E.M., Sequeira, M.: Lorawan networks susceptible to hacking: common cyber security problems, how to detect and prevent them. IOActive, Seattle, WA, USA, White Paper 1 (2020)
5. Chacko, S., Job, M.D.: Security mechanisms and vulnerabilities in lpwan. In: IOP Conference Series: Materials Science and Engineering, vol. 396, p. 012027. IOP Publishing (2018)
6. Lavric, A., Petrariu, A.I., Popa, V.: Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions. IEEE Access **7**, 35816–35825 (2019)
7. Malik, H., Alam, M.M., Le Moullec, Y., Kuusik, A.: Narrowband-iot performance analysis for healthcare applications. Procedia Comput. Sci. **130**, 1077–1083 (2018)
8. Mohamed, A., Wang, F., Butun, I., Qadir, J., Lagerström, R., Gastaldo, P., Caviglia, D.D.: Enhancing cyber security of lorawan gateways under adversarial attacks. Sensors **22**(9), 3498 (2022)

9. Noura, H., Hatoum, T., Salman, O., Yaacoub, J.P., Chehab, A.: Lorawan security survey: issues, threats and possible mitigation techniques. Internet Things **12**, 100303 (2020)
10. Noura, H.N., Salman, O., Hatoum, T., Malli, M., Chehab, A.: Towards securing lorawan abp communication system. In: CLOSER, pp. 440–447 (2020)
11. Yang, X., Karampatzakis, E., Doerr, C., Kuipers, F.: Security vulnerabilities in lorawan. In: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 129–140. IEEE (2018)