Analysis of LoRaWAN packets to demonstrate LoRaWAN vulnerabilities

Seokhyeon Bang*, Junyoung Jang*, Minju Ro*, Yuseon Choi†, Doyong Kwon‡ and Kangyeon Lee§
*School of Computer Science and Engineering
Chung-Ang University, Seoul, Korea
Emails: kzrt0123@cau.ac.kr, junjang99@cau.ac.kr, romj98@cau.ac.kr
†Department of Software Engineering
Chonnam National University, Gwangju, Korea
Email: 181133@jnu.ac.kr
‡School of Computer Science and Engineering
Kyungpook National University, Daegu, Korea
Email: doyong365@knu.ac.kr
§Department of Computer and Information Technology
Purdue University, Indiana, United States
Email: lee3245@purdue.edu

***Abstract*—Usage of LoRaWAN on Internet of Things(IoT) has increased since its appearance and now dominates IoT market over other Low Powered Wide Area Networks(LPWAN). However, LoRaWAN security has not been thoroughly developed which can cause critical issues in industries that rely on it. This paper demonstrates vulnerabilities in LoRaWAN by attempting attacks from jamming to replay attack. Attempts are implemented on a configured local network simulating the real environment.**

***Index Terms*—Internet of Things, LoRaWAN, security, risk assessment, vulnerability, jamming, replay attack**

I. Introduction

LoRa is a technology that provides low-power, long-distance communication using a modified Chirp Spread Spectrum(CSS) technology that monitors frequency changes [1]. LoRaWAN is an open networking protocol on top of LoRa [2].

The reliance on Internet of Things(IoT) on LoRa is expanding due to its features which include long-lasting batteries and long-distance data transmission. LoRa technology has benefits over other wireless communication technologies and other low-powered wide area networks(LPWAN), respectively [3]. For example, LoRa makes users easy to build and maintain their personal network which is LoRaWAN at a reasonable cost [4]. LoRaWAN is utilized in smart cities, logistics and transportation management, smart healthcare, smart buildings, public safety, space environment, smart agriculture, and so on [5].

However, despite of benefits of LoRaWAN, the security issues of it remain a secondary factor. Lack of security of LoRaWAN would cause human and property damage since several data in high-risk industries transmitted over LoRaWAN is vulnerable to information loss.

For example, LoRaWAN used in the medical area needs to monitor patients continuously who require real-time and always-on systems. Another example is that agricultural production will suffer greatly if farmers receive the inaccurate information regarding to soil, and water data. LoRaWAN has been confirmed to be vulnerable to replay attack, ack spoofing, eavesdropping, bit-flipping attack, and LoRa class B attack [6]. However, details of the environment where those attacks are conducted are insufficient. Therefore, this research focuses on figuring out vulnerabilities of LoRaWAN security under an experiment environment similar to the real world with specific configurations.

With emerging IoT technology and exponentially increasing IoT devices, protecting confidentiality, integrity, and availability in IoT communication is becoming important. This paper demonstrates and analyzes the vulnerabilities of the system by attacking the local LoRaWAN that embodies the real world. It also describes details about the architecture of a local network in the most popular way which reflects reality.

II. Literature Review

In this section, the benefits of LoRaWAN are introduced. The basic structure of LoRaWAN from a security perspective, prior researches about hacking method of LoRaWAN, and its countermeasure are discussed next.

A. The advantages of LoRaWAN

Compared to other wireless communication technologies such as Wi-Fi and Bluetooth, LPWAN is specialized for transmitting small data to a remote area. It is split into two categories based on the frequency band used to transmit data. Narrow Band-Internet of Things(NB-IoT) and Sigfox [3] are representative technologies that utilize licensed and unlicensed frequencies, respectively. LoRa has a higher data transmission rate compared to Sigfox although they are both using unlicensed frequency domains. In addition, the battery life of end devices of LoRaWAN lasts longer as the power consumption of LoRa is lower than NB-IoT.

B. The authentication process in LoRaWAN

The architecture of LoRaWAN consists of end devices, gateways, and 3 servers: network server, application server, and join server [7]. Sensor data from the end device is sent to the network server through the gateway. Since the end device is registered to the network server rather than a specific gateway, the network server deletes duplicate messages from multiple gateways. The application server processes data received from the network server, and the join server allows the end device to authenticate and sends a join acceptance message.

Before the end device transmits a message, it needs to be activated in one of two ways: Over-The-Air-Activation(OTAA) and Activation by Personalization(ABP). In OTAA mode, LoRaWAN guarantees security through the join procedure, a process that checks whether the end device is registered with the network server [1]. The end device that tries to connect to the network sends a join request to the join server. The join server sends a join accept to the end device if it is a legitimate device and delivers session keys to other servers to secure the traffic between end device and the servers. However, in ABP mode, it uses a fixed device address and session keys which makes the network insecure [8].

C. The security issues of LoRaWAN

Prior studies [6], [9]-[12] have shown that the LoRaWAN remains vulnerable to hacking and cyberattacks.

- Jamming

  Jamming is a technology that prevents the use of certain frequencies or radio waves by emitting Radio Frequency(RF). Accordingly, packet transmissions using the corresponding frequency are completely blocked by jamming.

  It is essentially a fundamental problem that wireless networks have and also researched in various radio technologies, such as Wi-Fi, Bluetooth, Zigbee and so on. This being said, methods of LoRaWAN jamming have no big difference from other wireless network jamming methods. As a known fact, reducing the risk of jamming is theoretically possible by limiting the duty cycle. This method is not effective enough in reality because attackers can easily disregard the constraints [10].

  Jamming can also be utilized to manipulate and limit the LoRaWAN device calculations. If the receiver is placed in the saturation state with high power jamming, the RegRssiWideband register which stores wideband Received Signal Strength Indicator(RSSI) measurement value to generate a random number will have a maximum value. Otherwise, RSSI can be forced with a fixed power. These actions eventually reduce randomness in the random number generator which can lead to DoS attack [11].

  Instead of an active method that directly prevents the threat of jamming, a detection method for jamming LoRaWAN was also presented. From a statistical point of view using Kullback-Leibler Divergence(KLD) and Hamming Distance(HD), it is possible to check whether jamming is conducted [12].

- Replay attack

  Yang *et al.* [6] discovered vulnerabilities in the LoRaWAN system and described the replay attack that maliciously repeats the data and results in a Denial of Service(DoS) attack. It confirmed that hackers are able to interrupt data transmission by repeating the previous message. Replay attack for ABP-activated nodes was executed in the paper published by Yang *et al.* [6]. In contrast, this paper implements the attack for OTAA-activated nodes. The paper [6] focused on analyzing the weak point in LoRaWAN and conducting experiments in a controlled environment. However, there is not sufficient explanations about the experimental environment of LoRaWAN.

This paper describes the procedure for setting up a local LoRaWAN environment where multiple hacking methods are attempted without constraints. Also, a method of sniffing LoRaWAN packets using a Software Defined Radio(SDR) device is presented in the next section.

REFERENCES

[1] N.Blenn, F.A.Kuipers, "LoRaWAN in the Wild: Measurements from The Things Network," 2017, Blenn, Norbert and Fernando A. Kuipers. "LoRaWAN in the Wild: Measurements from The Things Network." ArXiv abs/1706.03086 (2017): n. pag.

[2] LoRa Alliance, "What is LoRaWAN® Specification," lora-alliance.org, https://lora-alliance.org/about-lorawan/(accessed Sep. 15, 2022).

[3] F. L. Coman, K. M. Malarski, M. N. Petersen and S. Ruepp, "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766430.

[4] The Things Industries, "Why you should use lora technology and LoRaWAN® for your next IOT use case," The Things Industries, https://www.thethingsindustries.com/news/why-you-should-use-lora-technology-and-lorawan-for-your-next-iot-use-case/ (accessed Oct. 10, 2022).

[5] TEKTELIC Communications Inc., "LoRaWAN - Most Common Applications and Use Cases" iotforall.com, https://www.iotforall.com/lorawan-most-common-applications-and-use-cases (accessed Sep. 28, 2022).

[6] X. Yang, E. Karampatzakis, C. Doerr and F. Kuipers, "Security Vulnerabilities in LoRaWAN," 2018 IEEE/ACM Third Int. Conf. on Internet-of-Things Design and Implementation (IoTDI), 2018, pp. 129-140, doi: 10.1109/IoTDI.2018.00022.

[7] Semtech, "What are LoRa® and LoRaWAN®," lora-developers.semtech.com, https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan (accessed Sep. 14, 2022).

[8] The Things Stack, "ABP vs OTAA," The Things Stack for LoRaWAN, urlhttps://www.thethingsindustries.com/docs/devices/abp-vs-otaa/ (accessed Oct. 13, 2022).

[9] IoActive, "LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them.", urlact-on.ioactive.com, https://act-on.ioactive.com/acton/attachment/34793/f-87b45f5f-f181-44fc-82a8-8e53c501dc4e/1/-/-/-/-/LoRaWAN\%20Networks\%20Susceptible\%20to\%20Hacking.pdf (accessed Oct. 14, 2022).

[10] C. -Y. Huang, C. -W. Lin, R. -G. Cheng, S. J. Yang and S. -T. Sheu, "Experimental Evaluation of Jamming Threat in LoRaWAN," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1-6, doi: 10.1109/VTCSpring.2019.8746374.

[11] S. Tomasin, S. Zulian and L. Vangelista, "Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks," 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2017, pp. 1-6, doi: 10.1109/WCNCW.2017.7919091.

[12] 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," 2018 IEEE International Conference on Communications (ICC), 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422721.