INTERNATIONAL JOURNAL OF APPLIED METHODS IN ELECTRONICS AND COMPUTERS

www.ijamec.org

International Open Access

Volume 12
Issue 02

June, 2024

Research Article

Analysis of Lorawan Protocol and Attacks Against Lorawan-Based IoT Devices

Abdülkadir TEPECİK [a,*], *Ahmet Furkan AĞRAK* [a]

[a] *Computer Engineering Department, Yalova University, Yalova, 77200, Turkey*

ARTICLE INFO

Article history:
Received 29 January 2024
Accepted 14 April 2024

Keywords:
IoT,
IoTSecurity,
LoRaWAN,
Risk Analysis,
LPWAN

ABSTRACT

In this study, the LoRaWAN protocol, which is a promising candidate for Low-Power Wide Area Network (LPWAN) in terms of network capacity, network security, battery life, low cost and data transmission capabilities, has been selected to examine and analyze its security risks. The Internet of Things (IoT) concept has been explored, and various network types and architectures have been investigated and compared with the LoRaWAN protocol. Subsequently, attacks on IoT networks, the countermeasures taken by manufacturers, and relevant academic studies on this topic have been examined. The main subject of the study, LoRaWAN, has been explained in terms of its versions, architecture, components, classes, and network layers. Vulnerabilities, security risks, and types of attacks have been categorized and thoroughly explained and a risk assessment has been conducted to evaluate the impact of these attack types. Based on the findings, solutions to prevent or mitigate attacks for four specific types of attacks against the LoRaWAN protocol have been proposed and presented to end users.

1. Introduction

Today, with the rapid development of technology and the widespread use of the Internet, many devices we use in our daily lives can communicate with each other and connect to the Internet. One of these technologies is the Internet of Things (IoT). The original concept of the Internet of Things (IoT) was first described by Ashton in 1999 [1]. IoT technology has facilitated the transformation and advancement of the devices surrounding us and has contributed to the intelligence of objects [2], [3].

It is expected that the number of devices connected to the internet will exceed 500 billion by 2030 [4], [5].

Network structures such as local area networks (LANs), Personal Area Networks (PANs), Wide Area Networks (WANs), and Low-Power Wide Area Networks (LPWANs) are utilized in IoT applications. The commonly used wireless network technologies in these applications include Bluetooth, Zigbee, WiFi, cellular networks (2G, 3G, 4G, 5G), as well as NB-IoT, Sigfox, and LoRaWAN technologies. Each of these network structures and technologies has its own advantages and disadvantages. Therefore, the selection of a suitable network structure for IoT applications can vary depending on the requirements, taking into consideration factors such as low energy consumption, long-range, speed, and the size of data packets that can be transmitted at once [6]–[8].

Some Security Vulnerabilities in LoRaWAN has been examined by Yang [11].

Physical layer attacks has been researched by Ruotsalainen et al. [12].

2. Method

In this section, three evaluation methods are explained. These are impact, probability and risk assessment methods [9].

2.1. Impact Assessment

The purpose of impact assessment is to observe and categorize the magnitude of a threat posed by an attack. In the impact assessment of an attack, three different levels of impact are used: low, medium, and high. In addition to

[*] Corresponding author. E-mail address: atepecik@yalova.edu.tr
DOI: 10.58190/ijamec.2024.95

these levels, detectability and recoverability, along with the scale level, are employed to enhance the effectiveness of the outcome.

Detectability and recoverability: The detectability of an attack, its impact on the system, and the reversibility of the damage incurred after the attack are categorized as high, medium, and low.

Scale level: The scale of the affected area following an attack is represented by three different categories: end devices, LoRaWAN, and LoRaWAN networks.

Impact of attack: Shows detectability and recoverability using scale level.

Table 1. Attack impact assessment table

Detectability / Scale Level	Low	Medium	High
End Device	Medium	Low	Low
LoRaWAN	High	High	Medium
LoRaWAN Networks	High	High	Medium

2.2. Probability Assessment

In probability assessment, a threat can be measured using three different probability levels: high, medium, and low. Including factors such as technical challenges and motivation in this assessment will positively impact the accuracy of the outcome [9].

Technical challenges: This encompasses the difficulties that an attacker may face while carrying out the attack. We can categorize their solutions as easy, medium, and hard, representing different levels of challenge.

Motivation level: This refers to whether the attacker will proceed with the attack based on the challenges they encounter. We can classify these motivation levels as high, medium, and low.

Probability: It indicates the likelihood of an attack based on the technical challenges and motivation level.

Table 2. Attack probability assessment table

Technical challenges / Motivation	Easy	Medium	Hard
Low	Low	Low	Low
Medium	High	Medium	Low
High	High	High	Low

2.3. Risk Assessment

Probability assessment and impact assessment are integral components of risk assessment. In the risk assessment process, the outcomes are presented in three categories as shown in Table 3. These categories are as follows:

Low risk: This category represents a situation where the probability of an attack occurring is low, and if an attack does happen, its impact is expected to be mild.

Medium risk: This category represents a situation where the probability of an attack is moderate, and if an attack occurs, its impact is anticipated to be of medium severity

High risk: This category represents a situation where the probability of an attack is high, and if an attack takes place, its impact is expected to be substantial or severe.

Table 3. Risk assessment table

Probability / Impact	Low	Medium	High
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

3. LoRaWAN Risk Analysis and Attack Against LoRaWAN

3.1. Weak Points of The Parameters Used For Lorawan Security

In an attack, the target can be considered from two different perspectives: network security and the variables used for network security. When defining the security features of a network, three attributes are examined: confidentiality, integrity, and availability. These attributes are among the most popular security requirements, and when investigating a security vulnerability, these three attributes should be the primary focus. The vulnerability of security parameters in a network can jeopardize the entire network. The impact of a security value varies depending on whether it is a primary or secondary value. If there is a vulnerability in a primary value, it makes the entire system susceptible to exploitation, whereas, in a secondary value, the scope of exploitation is more limited. Table 4 illustrates the primary and secondary values in the LoRaWAN network.

Table 4. Variables in LoRaWAN network security

Variables	Primary/Secondary
NwkSKey	Primary
FrmPayload	Primary
AppSKey	Primary
DevNonce	Secondary
AppNonce	Secondary
Fcnt	Secondary
AppKey	Secondary
MAC komutları	Secondary
DevAddr	Secondary
ACK	Secondary

NwkSKey: This key is generated during device activation and is used to sign the message. If we consider the vulnerability of the confidentiality and integrity of the NwkSKey key, when confidentiality is breached, an external attacker can create their own message and use the NwkSKey key to pass the signature check unnoticed. In the case of a vulnerability in the integrity of the NwkSKey key, all messages in the current session will fail the signature check and be rejected.

FrmPayload: This value is a primary value and carries important data. Sensor data is transmitted through this FrmPayload. If we consider the vulnerability of the confidentiality and integrity of the FrmPayload, in a scenario where confidentiality is breached, sensor data can fall into the hands of a third party. If integrity is compromised, the received data from the sensors cannot be trusted.

AppSKey: This key is used in the application server to decrypt the messages. If we consider the vulnerability of the confidentiality and integrity of the AppSKey key, in a situation where confidentiality is breached, all messages can be decrypted, jeopardizing the confidentiality of the entire network. In the case of a vulnerability in the integrity of the AppSKey key, the end device or application server will be unable to decrypt the messages, rendering the received data useless.

DevNonce: DevNonce is a unique value generated by the end device. It is only used in the OTAA activation process. The DevNonce value is sent from the end device to the network server encrypted by AppKey, and the generated keys are sent back to the end device. If the integrity of the DevNonce value is compromised, the session keys generated on the end device and the server will be different, preventing communication between them.

AppNonce: This value is stored in the network server and is used to generate session keys with the help of DevNonce and AppKey. If we consider the vulnerability of the confidentiality and integrity of the AppNonce value, in a situation where the confidentiality of the AppNonce is breached, an attacker can easily guess the session keys to be generated, making the entire system vulnerable to exploitation. If the integrity of the AppNonce value is compromised, the session keys generated by the end device and the network server will not match, preventing communication between them.

FCnt: FCnt is a counter value stored in plaintext in both the end device and the server. It is used for synchronization between the end device and the server, and if its integrity is compromised, synchronization issues may arise, allowing an attacker to perform replay attacks.

AppKey: This key is used to derive the NwkSKey and AppSKey keys required for the activation of end devices using OTAA. It must be defined both in the end device and the server before activation. If we consider the vulnerability of the confidentiality and integrity of the AppKey key, in a situation where confidentiality is breached, an attacker can perform replay attacks by exploiting the join request. If the integrity of the AppKey key is compromised, OTAA activation cannot be achieved, and the end device cannot connect to the LoRaWAN network.

MAC Commands: MAC commands can be sent within the FrmPayload or FOpts values. It is important to maintain the confidentiality and integrity of MAC commands. Otherwise, if the commands fall into the hands of a third party, it can lead to system breaches based on the captured command.

DevAddr: This value is unencrypted and specifies the identity of the end device. If the integrity of the DevAddr value is compromised, communication between the end device and the server cannot be established.

ACK: This parameter is unencrypted and is used to confirm the received message. In a scenario where the integrity of the ACK parameter is compromised, it is possible to change this value and disable the ACK parameter.

3.2. Attacks against LoRaWAN

In this section of the study, four possible attacks against the LoRaWAN network have been examined and demonstrated.

3.2.1. Eavesdropping attack

Target of the attack

This attack aims to bypass the encryption method used for security in the LoRaWAN network. By eavesdropping on wireless network traffic, the attacker can decipher the encrypted data by leveraging two messages with the same counter value transmitted between the network server and the end device.

Subsequently, as the system's confidentiality is compromised, the attacker gains access to the sensor data transmitted in the network and, more importantly, if the transmitted data is of high importance, this can lead to a more significant breach of confidentiality.

Attacker's requirements

To execute the eavesdropping attack, the attacker must possess the following:

- Basic information about the end device (message format, message type)
- A LoRaWAN listening (sniffer) device to capture packets in the wireless network
- A database to store the captured LoRaWAN network traffic

Additionally, if the attacker has the capability to reset the end device, the success rate of the attack can be increased.

Vulnerabilities in the protocol

The success of this attack is attributed to two vulnerabilities in the protocol. One arises from the ABP activation method, and the other stems from the inability to ensure the security of counters. Another vulnerability exploited by this attack is the inadequacy of the security provided by the block cipher mode. As mentioned in the section describing the technical specifications of LoRaWAN, this mode uses counters instead of a nonce value in the blocks of data messages, which introduces a weakness.

In each reset, the static key used for encryption is reused when the same counter value is used. Consequently, when two messages with the same counter value are transmitted, they will be encrypted using the same key. Exploiting this situation, an attacker who obtains one of the messages encrypted with the same key can violate the encryption.

If we consider two messages encrypted with the same key:

$$UnencryptedMessage1 \oplus Key = EncryptedMessage1$$

$$UnencryptedMessage2 \oplus Key = EncryptedMessage2$$

Given the encrypted form of the message, the process of making the unencrypted form readable begins by attempting to guess a portion of the first unencrypted message and trying to reveal the second unencrypted message. This guessing process involves various patterns. The method employed to increase the likelihood of deciphering the encrypted message is to reset the device continuously. This method is referred to as crib dragging [10].

Detailed description of the attack

Fig. 2. illustrates the setup required for an eavesdropping attack in the LoRaWAN network.

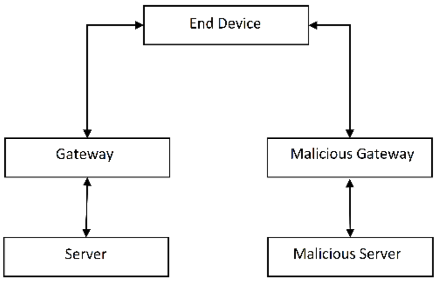

Figure 1. Eavesdropping attack for LoRaWAN

The steps of the attack are as follows:

- LoRaWAN packets are captured and recorded.
- Resetting is performed, and packets continue to be intercepted and recorded. Then, the packets captured before and after the reset are compared, and packets with the same counter value are matched.
- The crib dragging method is applied to extract results.
- As shown in the example of a eavesdropping attack in Fig. 2., the attacker maliciously listens to message packets transmitted from the end device using a rogue gateway. By recording the received message packets, resetting the device, and repeating the process, the attacker aims to match message packets with the same counter value to obtain the unencrypted form of the message.

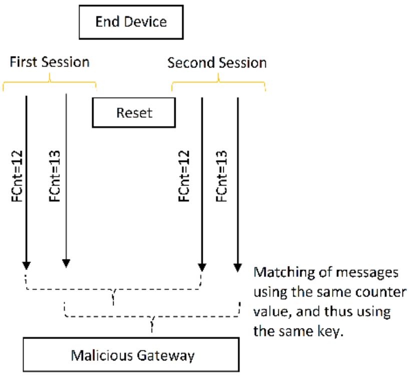

Figure 2. An example of Eavesdropping attack

Attack scenario

The objective of the Eavesdropping attack against LoRaWAN devices using the Activation by Personalization (ABP) method is to violate the confidentiality of transmitted data. The attacker primarily requires a LoRaWAN receiver to capture and decrypt the messages.

For this method based on matching messages with the same counter value, the attacker needs to reset the device to continue capturing messages and obtain the necessary data to decrypt the encrypted message after several resets. If no reset is performed, it may require a long wait to receive enough messages.

Once the encrypted message is decrypted by the attacker, they will be able to decrypt other received encrypted messages as well. As a result, data confidentiality will be compromised unless the session key is changed.

Bit-flipping Attack

Target of the attack

This attack targets the integrity of the message transmitted between the network server and the application server. In such an attack, the application server is unable to determine whether the source of the message is the attacker or the network server.

Requirements of the attacker

The following are the requirements for the attacker to carry out this attack:

- The ability to perform a Man-in-the-Middle (MITM) attack between the network server and the application server.
- Knowledge of the packet payload format.
- Basic information about the type and format of

the message received from the end device.

Vulnerability of the protocol

The LoRaWAN protocol lacks a mechanism for integrity checking in the communication between the network server and the application server. Incoming messages from the uplink are first encrypted and then signed. When the network server receives the message, it checks the message using the NwKSKey key and decides whether to accept it. Once the encrypted message is accepted by the network server, it is processed by the application server. However, the data packet is susceptible to modification while it is in transit between the network server and the application server. The lack of integrity checking for the message reaching the application server is the reason behind this vulnerability.

Detailed description of the attack

The setup of the Bit-Flipping attack is shown in Fig 3. The stages of the attack are as follows:

- If the attacker has access to the network server or can perform a MITM attack between the network server and the application server, they can carry out a Bit-Flipping attack.
- Exploiting the relationship between the unencrypted data and the encrypted data, the attacker manipulates the unencrypted version of the data by making changes to the encrypted data. The parts that the attacker can modify may include the content (FrmPayload), the end device address (DevAddr), and the counter value (FCnt) information.

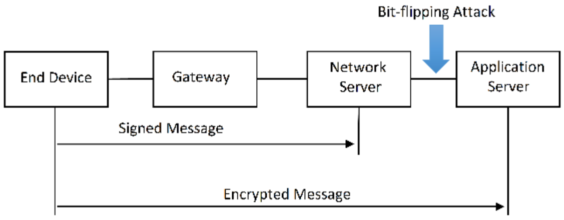

Figure 3. Schema of Bit-Flipping attack

Attack scenario

The threat of this attack arises from the violation of communication between the network server and the application server. In a scenario where the attacker compromises the communication between the network server and the application server through attacks like MITM, the attacker can:

- Modify LoRaWAN packets.
- If the counter value is altered, the application server may reject the received message.
- When FrmPayload is modified, the data received by the application server will be altered. In this case, a sensor data that is received incorrectly may lead to misinterpretation.
- If the DevAddr value is changed, the application server may misidentify the source of the incoming message.

Replay attack

Attacker's objective

Replay attack is a type of DoS and Spoofing attack. The attacker's goal is to make the server believe that the repeated message, sent from a device owned by the attacker, is coming from a legitimate device in the network. Another objective is to prevent the server from accepting the message sent by the target device. This section discusses replay attacks targeting LoRaWAN devices that use the ABP activation method.

Attacker's requirements

To carry out a replay attack, the attacker needs to possess certain qualifications. These include:

- A device capable of transmitting LoRaWAN message packets at the appropriate frequency.
- A device capable of capturing LoRaWAN messages.
- Knowledge of the LoRaWAN message format.
- Awareness of the frequency used by the target device.

Protocol vulnerability

The vulnerabilities exploited for replay attacks are presented in this section.

Due to the use of static keying in the ABP activation method, the same keys are used even if the device is reset. Additionally, in this activation method, no request-acceptance process is required after the devices are activated. In this case, the following requirements must be met for the server to accept a malicious message from the attacker:

- The counter value should be acceptable.
- The DevAddr value should match that of the accepted device.
- The session key should be the same as that of the accepted device.

In a situation where these requirements are met, it is not possible to determine during which session the malicious message, repeatedly sent by the attacker, was transmitted to the server.

Detailed description of the attack

The steps required to carry out the attack are as follows:

1. The uplink message is intercepted and captured using a listening device. The attacker records the intercepted messages.
2. Since the counter values are not encrypted, the FCnt value of the uplink messages is obtained.
3. The attacker waits until the device is restarted or until an overflow occurs in the counter.
4. From the attacker's own database consisting of

captured messages, a message with a suitable counter value is selected.

5. The message is retransmitted to the gateway, and the process is periodically repeated in this manner.

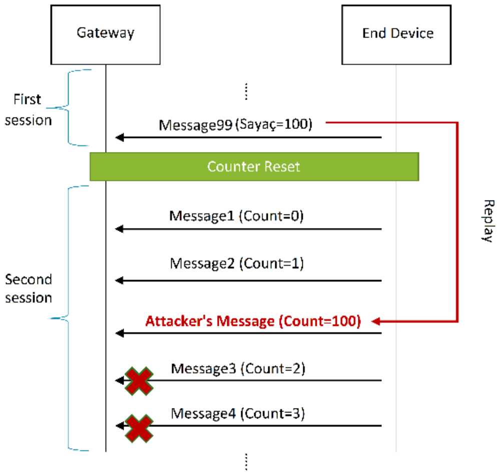

Figure 4. Example of a replay attack

Attack scenario

In this attack, the attacker first listens to the LoRaWAN wireless communication traffic and can replay the messages using a LoRa transmitter device. The impact of this attack can be significant. If the LoRaWAN network is large, the attacker can cause significant damage to the network without requiring a long duration by exploiting counter overflow. The attacker can repeatedly send the malicious message with the maximum counter value, resulting in the rejection of messages from the target device.

ACK spoofing attack

Attacker's objective

In the LoRaWAN protocol, the same ACK can be used for messages sent to the same device. In this attack, the attacker can acquire the ACK value of the message received by the device and use the same ACK value in their own message, thereby exploiting this vulnerability.

Attacker's requirements

The attacker needs certain qualifications to execute this attack. These include:

- The ability to read the content of ACK, use the correct counter and device address (FCnt and DevAddr) values.
- The ability to intercept ACK message transmission.
- Access to the gateway.
- The ability to send the selected ACK message to the device.

Protocol vulnerability

The LoRaWAN protocol does not specify which message an ACK packet belongs to and, therefore, which message it confirms. Only the confirmation of the most recent message exposes the vulnerability of a malicious attack, where the ACK packet of the most recent message can be stored and sent with a desired future message. The acceptance of ACK is determined by the FCnt value on the device, being smaller than the FCnt value in the received message.

Attack scenario

The execution of the ACK attack is possible when the attacker infiltrates with a rogue gateway or eavesdrops on an existing gateway. In this scenario, the attacker can exploit this vulnerability by using ACK packets to cause harm to the network, as described in the protocol vulnerability section.

4. Discussion and Conclusion

In this study, the LoRaWAN protocol, which is one of the networks used in the Internet of Things (IoT) and has gained popularity in recent years due to its long-range and low-power capabilities, has been examined in the context of security. The vulnerabilities of this protocol and the four attacks that can exploit them have been analyzed in Section III, and a summary along with the vulnerabilities they exploit is presented in Table 5.

Table 5. General summary of the attacks

Attacks	Target	Vulnerability	Risk
Eavesdropping (Privacy)	Decrypting the encrypted message results in a privacy breach	Counter management	Medium
Bit-Flipping (Integrity)	Tampering with the transmitted data without detection, causing an integrity breach	Lack of integrity check on the message received by the application	Low
Replay (availability)	Acceptance of malicious messages by the server and rejection of normal messages from legitimate end devices	Counter management and static keying	High
ACK Spoofing (availability)	Disabling the end device and disrupting communication with the gateway	Message transmission control	Medium

When examining the security of the LoRaWAN protocol, it is observed that the Over-The-Air Activation (OTAA) and Activation By Personalization (ABP) methods are used to establish secure communication between end devices and servers. The activation methods are responsible for deriving the session keys used during the connection establishment in the network. Focusing on the advantages and disadvantages of these two methods, it is seen that the OTAA method is more secure compared to the ABP method due to secure key exchange over the air between the end device and the server, dynamic key management at both ends and its usage of dynamic session keys.

In this study, a comprehensive security analysis of the LoRaWAN protocol has been conducted, vulnerabilities have been identified, and it has been demonstrated which types of attacks can exploit these vulnerabilities. As a result, it has been shown that the LoRaWAN protocol is not yet completely secure, and it may pose risks when transmitting critical information and when used in critical systems. However, it has been demonstrated that the risks associated with these vulnerabilities and attacks can be mitigated through the precautions and recommendations presented in this study.

Although the LoRaWAN protocol requires further development in terms of security, we predict that its widespread adoption will continue and its presence in our lives will continue to increase.

References

[1] Ashton K. "That ‘Internet of things’ thing". https://www.rfidjournal.com/articles/view?4986 (25.05.2021).

[2] Nordrum A. "Popular internet of things forecast of 50 billion devices by 2020 is outdated". https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated (25.05.2021).

[3] Evans D. "The internet of things: how the next evolution of the internet is changing everything". Cisco, San Jose Canada, 2011.

[4] Cisco, "Cisco visual networking index: forecast and trends,2017–2022". https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf (25.05.2021).

[5] Cisco, "Cisco visual networking index: forecast and trends,2017–2022". https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf (25.05.2021).

[6] Marcel J. "Wireless connectivity options for iot applications". https://www.bluetooth.com/blog/wireless-connectivity-options-for-iot-applications. (25.05.2021).

[7] Harada R, Sotter E. "Automated monitoring for inspections and condition-based maintenance- Part III: Industrial IoT networks". https://electricenergyonline.com/energy/magazine/1166/article/Automated-Monitoring-for-Inspections-and-Condition-based-Maintenance-Part-III-Industrial-IoT-Networks.htm (25.05.2021).

[8] Kumar R, Au T.W, Susanty W, Suhaili H. "Exploring data security and privacy issues in internet of things based on five-layer architecture". International Journal of Communication Networks and Information Security, 12(1), 108-121, 2020.

[9] Pereira N. Gidlund M. Butun I. "Security risk analysis of lorawan and future directions" Future Internet , 3(1), 11, 2019

[10] Dazell T. "Many time pad attack - crib drag". http://travisdazell.blogspot.com/2012/11/many-time-pad-attack-crib-drag.html (08.04.2021).

[11] Yang, Xueying, Evgenios Karampatzakis, Christian Doerr, and Fernando Kuipers. "Security vulnerabilities in LoRaWAN." In 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 129-140. IEEE, 2018.

[12] Ruotsalainen, Henri, Guanxiong Shen, Junqing Zhang, and Radek Fujdiak. "LoRaWAN physical layer-based attacks and countermeasures, a review." Sensors 22, no. 9 (2022): 3127.