The Design of Security Framework for LoRaWAN FUOTA

Nur Hayati

Department of Electrical Engineering, Faculty of Engineering, Universitas Muhammadiyah Yogyakarta
Center of Artificial Intelligence and Robotics Studies, Universitas Muhammadiyah Yogyakarta
Bantul, 55183, Daerah Istimewa Yogyakarta, Indonesia
Email: nuha.nurhayati@umy.ac.id

Abstract – *This research outlines a comprehensive security framework for LoRaWAN Firmware Updates Over-The-Air (FUOTA), which is essential for ensuring the reliability of IoT devices in critical infrastructures. It addresses multiple security threats specific to the wireless transmission of firmware updates, initiating an assessment of the vulnerabilities faced by the LoRaWAN FUOTA process. The framework incorporates several security measures, including secure transmission using lightweight encryption to maintain data confidentiality, robust authentication and authorization strategies to prevent unauthorized access, and digital signatures for integrity verification to ensure only authentic firmware updates are installed. It also includes anti-replay measures like sequence numbers and timestamps to protect against replay attacks and emphasizes efficient resource management to optimize power and computational resources for IoT devices. Additionally, secure multicast management techniques are employed to handle the challenges of simultaneously distributing updates to multiple devices. The framework provides an integrated and detailed approach to enhancing the security and operational efficiency of LoRaWAN FUOTA, making it an invaluable resource for practitioners and researchers in the field.*

Keywords*: LoRaWAN; FUOTA; Security; Framework; IoT*

I. Introduction

Firmware updates over the air (FUOTA), is an essential procedure for wirelessly updating the firmware of LoRaWAN devices. It enables the deployment of security updates, new features, and optimization patches with minimal human involvement, ensuring that the devices stay updated [1]. FUOTA is part of a broader device management system that includes software updates, protocol querying, device configuration, security provisioning, and monitoring, highlighting its significance in the overall management of IoT devices [2].The LoRa Alliance has introduced specifications such as multicast, fragmentation, and clock synchronization to support efficient FUOTA over LoRaWAN networks, addressing the challenges posed by the technology's limitations in data rates and duty cycle restrictions [3].

LoRaWAN FUOTA marks a significant advancement in managing and maintaining the vast arrays of IoT devices deployed across various industries. FUOTA allows for efficient updates of device firmware without physical access to the devices. However, this convenience also introduces potential security issues that are of primary concern to researchers and network administrators [4] [5]. Thus, addressing these security vulnerabilities within FUOTA processes is a critical area of focus for ongoing research and development efforts in the field of IoT security[6]. This paper presents the security vulnerabilities that likely arise during the FUOTA process and design security frameworks to address these vulnerabilities.

II. Related work

There are several studies that have discussed LoRaWAN FUOTA by focusing on different issues, such as energy efficiency, protocol design and security. Study conducted in [4] addresses the challenges of supporting FUOTA in LoRaWAN networks. It discusses the introduction of new specifications by the LoRa Alliance to enable efficient FUOTA through multicast, fragmentation, and clock synchronization, evaluating the impact of different FUOTA parameters. Next, study [2] offers a thorough examination of firmware updating techniques for LPWANs. This study provides insights into the latest technologies for firmware updates in LPWAN systems by examining different

Manuscript received October 2023, revised December 2023

over-the-air update processes.

Research in [7] focuses on ensuring reliable and energy-efficient reprogramming for Smart LoRaWAN devices. This research addresses the challenges of firmware updates in Low Power Wide Area Network (LPWAN) and proposes solutions to enhance the reliability and energy efficiency of reprogramming processes. Meanwhile, research in [8] proposes a novel blockchain-based solution for updating firmware on IoT devices over LoRa networks. By leveraging blockchain technology, this paper offers a secure and reliable method for managing firmware updates, tackling the challenges associated with updating devices in IoT environments.

Furthermore, study conducted in [1] defines and emphasizes the significance of FUOTA for ensuring the reliability and security of LoRaWAN devices over their extended lifetimes. It discusses the challenges and solutions for efficient FUOTA implementation in LoRaWAN networks. Then, the study [5] focuses on energy-efficient firmware updates for TinyML models in LoRaWAN agricultural networks. This paper presents a study of the FUOTA process for LoRaWAN networks, analyzing its feasibility in the context of TinyML firmware updates and evaluating energy consumption and packet delivery ratio in various network scenarios.

III. Security Vulnerabilities of LoRaWAN FUOTA

Security is essential parameter in LoRaWAN FUOTA, as the updates are carried wirelessly over potentially large and unmanaged geographical areas. The FUOTA process in LoRaWAN networks introduces several vulnerabilities that could potentially be exploited by cyber threats. These vulnerabilities stem from the unique characteristics and operational environments of LoRaWAN. Fig. 1 depicts the diagram of key vulnerabilities of LoRaWAN FUOTA.

III. 1. Data Interception

Given that firmware updates are transmitted wirelessly over LoRaWAN, there is a natural risk of data interception by unauthorized entities. Data interception can occur through eavesdropping and man-in-the-middle (MitM) attacks. Unauthorized actors might capture wireless transmissions between the server and the IoT devices. Attackers could intercept and alter the data being transmitted in real-time. In the case of FUOTA, this could mean modifying the firmware itself, inserting malicious code that could lead to compromised device functionality or turning devices into nodes for further attacks within the network.

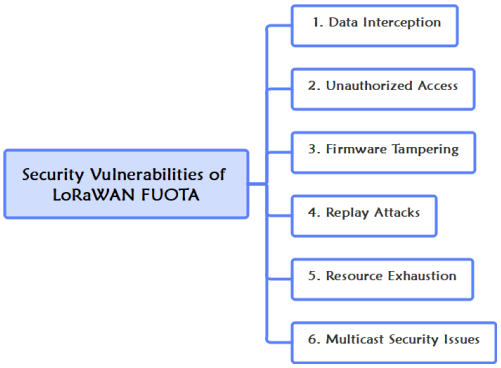

Fig. 1. Security Vulnerabilities of LoRaWAN FUOTA

III. 2. Unauthorized Access

Insufficiently secure authentication techniques pose a danger of unauthorized devices receiving and installing firmware upgrades. This could lead to scenarios where malicious firmware is pushed to devices, thereby compromising their functionality or turning them into nodes for further attacks.

III. 3. Firmware Tampering

Firmware tampering poses a substantial security risk that greatly impact the integrity and reliability of LoRaWAN. Tampered firmware has a potential to damage the operation of devices or turn them completely inoperative, hence possibly disrupting vital services and operations. In addition, tampered firmware may contain backdoors or other vulnerabilities that grant unauthorized access to network operations or sensitive data, jeopardizing the security of the entire network.

III. 4. Replay Attacks

Replayed firmware update commands cause devices to reinitiate update procedures unnecessarily, leading to operational delays and disruptions, especially if the device restarts or enters a maintenance mode. If multiple devices receive replayed update packets simultaneously, it could lead to increased traffic on the network, causing congestion and potentially denying service to other devices trying to communicate normally. Additionally, repeated and unnecessary updates caused by replay attacks can

lead to excessive power consumption, reducing the operational lifespan of the devices.

III. 5. Resource Exhaustion

LoRaWAN end devices, especially those in remote or hard-to-access locations, rely on battery power to function. The FUOTA process, which involves receiving, processing, and installing firmware updates, can be power-intensive compared to the device's normal operations. Frequent or poorly managed updates can lead to excessive power consumption, draining the battery more quickly than anticipated. Firmware updates often require devices to perform intensive computational tasks such as decrypting and verifying the integrity of the received firmware. For devices with limited processing power, these tasks can lead to significant system strain, reducing the device's operational efficiency and responsiveness.

III. 6. Multicast Security Issues

Standard LoRaWAN encryption mechanisms are designed for unicast communications where each device has a unique set of keys. In multicast, the same payload is sent to multiple devices, potentially using the same encryption keys. This commonality makes it easier for attackers to intercept and decrypt multicast transmissions if they gain access to the shared key. Since the same message is sent to multiple devices, an attacker who manages to eavesdrop on the multicast transmission can potentially access the content intended for all those devices.

To address these vulnerabilities, it is essential to provide a robust security framework that includes encryption, secure authentication, integrity verification, and efficient resource management. This framework helps to minimize the risks and protect the integrity of data transmitted within LoRaWAN networks.

IV. Security Framework of LoRaWAN FUOTA

A thorough security architecture is crucial to mitigate the vulnerabilities revealed in the LoRaWAN FUOTA process. This framework should include multiple layers of security mechanisms specifically designed to protect against potential attacks and guarantee the integrity and confidentiality of the firmware upgrades. In this section, we provide a detailed explanation of the security framework for FUOTA over the LoRaWAN, and it is summarized in Table 1.

IV. 1. Secure Transmission

Securing the transmission of firmware updates is mandatory in the FUOTA process for LoRaWAN to minimize the possibility of interception and unauthorized access [9]. Secure transmission relies on two primary elements: encryption and the utilization of secure channels.

IV. 1. 1. Lightweight Encryption

Encryption in firmware updates safeguards the data from being intercepted, altered, or misused by unauthorized entities. Encryption ensures that the information remains unreadable in the event of data interception unless the correct decryption key is used. Given the attributes of LoRaWAN, such as its low power consumption and long-range capabilities, encryption methods must be both secure and efficient, therefore reducing computational burden and energy consumption [10]. Efficiency, frequently attained by employing lightweight encryption methods, is crucial for preserving IoT devices' battery life and operational effectiveness,

Table 1. Security framework of LoRaWAN FUOTA

Vulnerabilities	Security Framework	Technical Solution Approach	Technological Options
Data Interception	Secure Transmission	Lightweight Encryption Secure Channel	AES - 128-bit, SPECK, SIMON, PHOTON DTLS, DICE, TLS
Unauthorized Access	Authentication and authorization	Device Authentication RBAC	Mutual Authentication, Pre-shared Keys. LDAP, Active Directory
Firmware Tampering	Integrity Verification.	Digital signatures Checksums	ECC, RSA, DSA CRC, MD5, SHA-1
Replay attack	Anti-Replay Mechanisms	Timestamping Sequence numbers	RTC, SNTP Incremental Logic
Resource Exhaustion	Efficient Resource Management	Optimized Protocols Adaptive Data Rates	Lightweight protocol and algorithm CA-ADR, Kriging ADR
Multicast Security Issue	Secure Multicast Management	Group Key Management Segmentation	G-IKEv2, LGKCMP MQTT2MULTICAST

guaranteeing that they are not excessively strained during encryption and decryption tasks.

IV. 1. 2. Secure Channels

Utilizing secure communication channels to enhance firmware transmissions' security is important. Protocols such as DTLS and TLS accomplished this goal. DTLS is well-suited for scenarios where data is transmitted over a UDP transport, which is common in environments where devices might have limited resources and connectivity. The DTLS In Constrained Environments (DICE), which a working group has discussed, is focused on supporting DTLS Transport-Layer Security in IoT environments. Therefore, DICE is an ideal protocol for IoT applications such as FUOTA in LoRaWAN. In contrast, TLS is commonly utilized with TCP connections to offer robust security measures well-suited for reliable network environments.

IV. 2. Authentication and Authorization

It is essential to guarantee that only valid and authorized devices receive and implement firmware upgrades to protect the network's security and integrity[11]. These two fundamental processes, authentication, and authorization are used to achieve this.

IV. 2. 1. Device Authentication

LoRaWAN has been equipped with an authentication mechanism so that each end device and server confirm each other's identities before beginning any firmware updates. In addition, the researchers can improve mutual authentication mechanisms using digital certificates or pre-shared keys (PSK). While digital certificates, supported by Public Key Infrastructure (PKI), offer a higher security level and are preferable in high-security environments, they can be resource-intensive in terms of processing and power, posing a challenge for less capable devices. On the other hand, PSK offers a simpler and less resource-demanding alternative, making it suitable for environments where managing a PKI is impractical and for devices with limited computational and energy resources.

IV. 2. 2. Role-Based Access Control (RBAC)

RBAC ensures that only authorized devices receive specific firmware updates according to their roles and assigned permissions by the LoRaWAN server. This is managed at the network server level, where a database keeps track of each device's roles, the firmware updates they are allowed to receive, and the conditions under which these updates are permitted. Additionally, RBAC can be supported by management software or platforms that help define roles, assign devices to these roles, and manage permissions effectively. These systems often integrate with directory services like Active Directory or LDAP, allowing centralized role management.

IV. 3. Integrity Verification

LoRaWAN has been enhanced with integrity verification, i.e., message integrity code (MIC), that supports the FUOTA process within the networks. Ensuring the integrity of firmware updates during transmission is significant for maintaining trust and reliability [11]. Further, alternative methods utilized to accomplish integrity are digital signatures and checksums.

IV. 3. 1. Digital signatures

Digital signatures are precious in IoT environments for ensuring the integrity and authenticity of firmware packages. In the FUOTA process, a LoRaWAN server uses a secure hashing and signing algorithm to sign the firmware before transmission; then, the receiving IoT end device verifies this signature to ensure that the firmware has not been altered and to confirm the sender's identity. However, the main drawback of using digital signatures in IoT is the high computational demand of asymmetric cryptographic operations, which can be challenging for resource-constrained IoT devices.

IV. 3. 2. Checksums

Checksums provide a more efficient and less computationally demanding approach to guaranteeing data integrity. They are especially beneficial for conducting rapid integrity verifications before and after data transmission. Checksums, although without encryption or key-based methods, are highly successful in detecting data corruption resulting from problems in data transmission, such as noise or signal abnormalities. However, they do not offer protection against intentional tampering. Checksums are beneficial for low-power IoT devices that lack the ability to execute complicated cryptographic operations due to their minimal processing needs.

IV. 4. Anti-Replay Mechanisms

Securing and maintaining the integrity of communications between devices and network servers is the highest priority [12]. Implementing anti-replay mechanisms is necessary for preserving

against potential threats, such as replay attacks. Two commonly used mechanisms are time-stamps and sequence numbers.

IV. 4. 1. Embedding a *timestamp*

Embedding a timestamp within each transmitted firmware update packet is imperative for accurate timestamping. This timestamp indicates when the packet was initially sent, offering a chronological context to the receiving device or server. Upon receiving a packet with a timestamp, the receiver can assess the "freshness" of the packet by comparing the timestamp within the packet to its current time. If the packet's timestamp falls outside of an acceptable range, it can be considered a replayed packet and, therefore, rejected. For timestamps to work effectively, it is mandatory to have synchronized clocks between the transmitting and receiving devices. However, synchronization can pose a significant challenge, especially in distributed networks such as those utilizing LoRaWAN. These networks often involve devices with limited power and processing capabilities, making it challenging to maintain accurate time if the devices go offline or reboot.

IV. 4. 2. Effective anti replay mechanism

Another effective anti-replay mechanism is the use of *sequence numbers*. Every packet in a communication session is assigned a distinct sequence number that increases with each subsequent packet. The receiving device records the sequence numbers of previously received packets. Upon the arrival of a new packet, its sequence number is compared to the expected values. Suppose the packet's sequence number is lower than expected, suggesting that it has been encountered previously or falls outside the anticipated range. In that case, the packet is considered a replay and is disregarded. Implementing sequence numbers is challenging, similar to the process of time stamping. Managing sequence numbers is important, mainly when dealing with packet loss and reordering issues frequently encountered in wireless communications like LoRaWAN. A robust protocol should incorporate a mechanism to effectively manage such scenarios, ensuring that legitimate packets are not erroneously rejected.

IV. 5. Efficient resource management

Efficient resource management is of utmost importance in LoRaWAN networks to enhance the performance and sustainability of connected devices, particularly during firmware updates [13]. Effective management solutions, such as improved protocols and adaptive data rates, are vital for maintaining functioning while decreasing operational expenses.

IV. 5. 1. Optimized Protocols

The FUOTA process can significantly strain network resources as it involves transmitting potentially large firmware updates to multiple devices. Efficiently managing the communication protocols utilized during these updates is crucial for reducing energy consumption and optimizing bandwidth usage in LoRaWAN networks. We can minimize the data transmitted in each update session by developing lightweight, effective communication protocols. Efficient data formats ensure minimal overhead from headers and non-payload elements.

IV. 5. 2. Adaptive Data Rates

Feature of LoRaWAN is specifically designed to optimize data transmission rates by considering the network conditions and the capabilities of each device. This feature is especially advantageous during the FUOTA process. ADR dynamically adjusts the data rate for each device by selecting the most optimal spread factor and bandwidth. Adjustments are made based on the quality of the link, which may be affected by factors like distance from the gateway, interference, and physical obstructions. Through the optimization of transmission rates, ADR effectively conserves bandwidth and energy while also improving the overall reliability of data transmission. Reliable transmission guarantees the completeness of the firmware received during updates, ensuring the LoRaWAN end device receives all data updates and properly functions post-update.

IV. 6. Secure Multicast Management

In LoRaWAN networks, the effective and secure management of firmware upgrades requires the simultaneous delivery of updates to numerous devices through secure multicast[14]. Two optional approaches to achieving this multicast management are group key management and a segmented update procedure.

IV. 6. 1. Group Key Management

Group Key Management [15] is essential for ensuring the security of multicast transmissions in LoRaWAN networks. The goal is to guarantee that only authorized devices belonging to a predetermined group can decrypt and use the sent data. Regularly changing encryption keys helps to

mitigate the risk of prolonged unauthorized access, guaranteeing that any security breach has a restricted timeframe of influence. Further, the system should be supported by a secure channel for distributing the multicast group keys to devices.

IV. 6. 2. Segmenting

Segmenting the firmware update into smaller parts is a strategy to enhance the efficiency and reliability of multicast FUOTA. This approach has several benefits in handling complex and large-scale updates across multiple devices: Efficiency in Transmission, Error Checking and Recovery, and Handling Device Variability. By dividing the firmware into smaller segments, each piece can be transmitted rapidly and with potentially lower error rates. Segmenting the update process allows for more granular error-checking and recovery mechanisms. Each segment can be independently verified for integrity and completeness. If errors are detected in any segment, only the affected parts must be retransmitted, not the entire firmware file.

V. Conclusion

The security framework for LoRaWAN FUOTA is fundamentally designed to address multiple layers of potential vulnerabilities, ensuring the robustness and reliability of the network. Key components of this framework include secure transmission to prevent data interception, stringent authentication and authorization processes from restricting access, and integrity verification methods like digital signatures to safeguard against firmware tampering. Additionally, anti-replay mechanisms and efficient resource management are essential to protect against replay attacks and conserve device resources, respectively. Secure multicast management further enhances the framework by ensuring that updates transmitted to multiple devices simultaneously are protected. Together, these elements form a comprehensive security strategy that mitigates a wide range of risks and bolsters the overall health and effectiveness of IoT deployments using LoRaWAN, making it a dependable choice for future-proof network security in diverse applications.

References

[1] J. Catalano, "LoRaWAN Firmware Update Over-The-Air (FUOTA)," *JICTS*, Apr. 2021, doi: 10.13052/jicts2245-800X.913.

[2] M. Pule and A. M. Abu-Mahfouz, "Firmware Updates Over the Air Mechanisms for Low Power Wide Area Networks: A Review," in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, Vanderbijlpark, South Africa: IEEE, Nov. 2019, pp. 1–7. doi: 10.1109/IMITEC45504.2019.9015851.

[3] N. Sornin, "LoRaWAN®: Firmware Updates Over-the-Air," 2020.

[4] K. Abdelfadeel *et al.*, "How to Make Firmware Updates over LoRaWAN Possible," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Cork, Ireland: IEEE, Aug. 2020, pp. 16–25. doi: 10.1109/WoWMoM49955.2020.00018.

[5] C. Nicolas, B. Naila, and R.-C. Amar, "Energy efficient Firmware Over The Air Update for TinyML models in LoRaWAN agricultural networks," in *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)*, Wellington, New Zealand: IEEE, Nov. 2022, pp. 21–27. doi: 10.1109/ITNAC55475.2022.9998338.

[6] S. El Jaouhari, "Toward a Secure Firmware OTA Updates for constrained IoT devices," in *2022 IEEE International Smart Cities Conference (ISC2)*, Pafos, Cyprus: IEEE, Sep. 2022, pp. 1–6. doi: 10.1109/ISC255366.2022.9922087.

[7] W. Mao *et al.*, "Reliable and Energy-Efficient Reprogramming for Smart LoRaWAN," in *2023 IEEE Smart World Congress (SWC)*, Portsmouth, United Kingdom: IEEE, Aug. 2023, pp. 1–8. doi: 10.1109/SWC57546.2023.10449002.

[8] A. Anastasiou, *et al.*, "IoT Device Firmware Update over LoRa: The Blockchain Solution," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Marina del Rey, CA, USA: IEEE, May 2020, pp. 404–411. doi: 10.1109/DCOSS49796.2020.00070.

[9] N. Hayati, S. Windarta, M. Suryanegara, B. Pranggono, and K. Ramli, "A Novel Session Key Update Scheme for LoRaWAN," *IEEE Access*, vol. 10, pp. 89696–89713, 2022, doi: 10.1109/ACCESS.2022.3200397.

[10] N. Hayati, K. Ramli, M. Suryanegara, and Y. Suryanto, "Potential Development of AES 128-bit Key Generation for LoRaWAN Security," in *2019 2nd International Conference on Communication Engineering and Technology (ICCET)*, Nagoya, Japan: IEEE, Apr. 2019, pp. 57–61. doi: 10.1109/ICCET.2019.8726884.

[11] J. Qadir, *et al*., "Mitigating Cyber Attacks in LoRaWAN via Lightweight Secure Key Management Scheme," *IEEE Access*, vol. 11, pp. 68301–68315, 2023, doi: 10.1109/ACCESS.2023.3291420.

[12] N. Hayati, K. Ramli, S. Windarta, and M. Suryanegara, "A Novel Secure Root Key Updating Scheme for LoRaWANs Based on *CTR_AES* DRBG 128," *IEEE Access*,

vol. 10, pp. 18807–18819, 2022, doi: 10.1109/ACCESS.2022.3150281.

[13] D. K. Nilsson and U. E. Larson, "Secure Firmware Updates over the Air in Intelligent Vehicles," in *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*, Beijing, China: IEEE, May 2008, pp. 380–384. doi: 10.1109/ICCW.2008.78.

[14] J. Navarro-Ortiz, et all, "A LoRaWAN Network Architecture with MQTT2MULTICAST," *Electronics*, vol. 11, no. 6, p. 872, Mar. 2022, doi: 10.3390/electronics11060872.

[15] F. Samiullah, M.-L. Gan, S. Akleylek, and Y. Aun, "Group Key Management in Internet of Things: A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 77464–77491, 2023, doi: 10.1109/ACCESS.2023.3298024.

Authors' information

Nur Hayati received the bachelor's degree in applied science (telecommunications engineering) from the Electronic Engineering Institute of Surabaya, in 2010, and the master's and Ph.D. degrees in computer engineering from Universitas Indonesia, in 2015 and 2022, respectively. She is currently an Assistant Professor with the Department of Electrical Engineering, Universitas Muhammadiyah Yogyakarta. Her research interests include embedded systems, computer networks, and security in the IoT.