UDC 004.056.5:654.02

Security and Efficiency of LoRaWAN Networks: Practical Tips and Recommendations

Alina Yanko, Viktor Krasnobayev, Stanislav Goncharenko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

Annotation

The relevance of this study lies in the fact that, in the modern world, the Internet of Things (IoT) approach is becoming increasingly widespread, and LoRaWAN (Long Range Wide Area Network) technology is one of the key solutions for building LPWAN (Low Power Wide Area Network) networks, which enable long-range communication with low power consumption. The growing popularity of LoRaWAN necessitates ensuring secure data transmission, resilience to attacks, and optimization of network parameters to achieve maximum efficiency.

To achieve the research objective, a comprehensive methodological approach was employed, incorporating the analysis of existing solutions and recommendations for the security and optimization of LoRaWAN networks and equipment. A key element of the study is the examination of up-to-date documentation from the LoRa Alliance, which provides a detailed description of best practices and approaches for LoRaWAN deployment. This documentation is based on the practical experience gained by the LoRa Alliance from network users and operators, allowing for the consideration of various aspects of technology implementation to ensure its efficiency and security. The study also includes an analysis of scientific publications and practical user experiences to gain a deeper understanding of LoRaWAN challenges and opportunities.

The primary objective of this study was to develop recommendations and practical solutions for enhancing the security of data transmission, improving resilience against attacks on LoRaWAN networks, optimizing data transfer rates and device configurations (including end-user devices and LoRaWAN gateways), and ensuring compliance with LoRa Alliance guidelines based on the analysis of existing solutions. The key task is to implement LoRaWAN networks in accordance with the official LoRa Alliance recommendations, meeting all modern security requirements and challenges.

The study revealed that the effective use of LoRaWAN requires a comprehensive security approach, which includes the implementation of modern encryption, authentication, and authorization methods, as well as continuous network traffic monitoring and analysis to detect and prevent potential threats. Data transmission rate optimization is achieved through proper device parameter configuration, selection of the optimal data rate, and consideration of the specific application's requirements.

Adhering to the recommendations of the LoRa Alliance in the design and deployment of LoRaWAN is critically important for ensuring interoperability between devices from different manufacturers, achieving high communication quality, and maintaining network security.

***Keywords*:** LoRaWAN network, data security, network protection, communication channel, data monitoring, device configuration, load optimization, traffic distribution, session keys, session encryption keys, operational stability, attack resilience.

Introduction

Modern technologies are designed to enhance business efficiency, optimize costs, and improve quality of life. One such solution is the IoT-based LoRaWAN network, a wireless communication technology used to build energy-efficient networks with extensive coverage areas. The key advantages of LoRaWAN include low power consumption, the ability to transmit data over long distances up to several tens of kilometers and support for a large number of end devices (approximately 500 devices per LoRa gateway) [1].

LoRaWAN networks are structured around an infrastructure that includes end-user devices such as sensors, detectors, and actuators, as well as gateways for client traffic exchange, network

servers, and application servers. Figure 1 illustrates a typical LoRaWAN network architecture, which consists of the following components [2]:

- **End Devices:** Devices utilized by the end user. Examples include any sensor with a LoRa module for data transmission/reception. For instance: camera, wind farm, lighting system, leakage sensor, or motion detector.
- **LoRaWAN Gateway:** A network gateway that facilitates packet communication between client equipment (End Devices) and the network communication server (Network Server). Communication with user devices occurs via LoRa. Communication with the Network Server occurs via an Ethernet network.
- **Network Server:** A network server that performs the key functions of routing, processing, and filtering data received from gateways. It is also responsible for adapting communication parameters (e.g., ADR (Adaptive Data Rate)) and ensuring network security.
- **Application Server:** A server (typically a cloud service) that processes sensor data and provides users with a convenient interface for managing End Devices. Primarily, this is a web or mobile application.

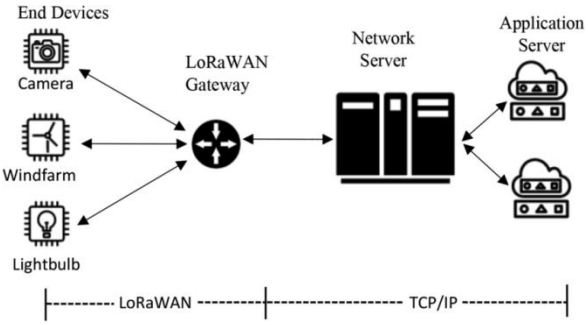

Figure 1: Structural diagram of LoRaWAN networks

The primary purpose of using LoRaWAN is to provide connectivity for IoT devices. LoRaWAN is utilized for environmental monitoring, smart city systems, industrial equipment control, agricultural monitoring, and logistics. The technology addresses challenges related to transmitting small volumes of data, ranging from 0.3 to 27 kbit/s [3], in hard-to-reach areas where traditional solutions such as Wi-Fi or cellular communication are impractical or economically unviable.

LoRaWAN is a popular technology in many countries, including the United States, France, the Netherlands, Germany, and China (see Fig. 2). It is actively employed in smart city applications, industrial automation, environmental monitoring, and logistics. Numerous companies, such as Actility, The Things Industries, Loriot, and Kerlink, are engaged in the implementation and development of LoRaWAN solutions [4].

Figure 2: LoRaWAN network coverage map

In Ukraine, LoRaWAN is also developing, particularly within the framework of the "Kyiv Smart City" project. In Kyiv, a LoRaWAN network is being actively integrated for managing city infrastructure, air quality monitoring, resource consumption metering, and other tasks (see Fig. 3). As of today, a significant number of LoRaWAN gateways, approximately 300 units, have been installed in Kyiv, enabling the efficient use of this technology to meet the city's needs [5]. Given the growing popularity of LoRaWAN, it is important to understand the key recommendations and approaches to its configuration and operation. The operation of LoRaWAN networks is regulated by the LoRa Alliance, which develops standards and provides detailed documentation on all aspects of network functionality. One of the key documents is TR007, which contains comprehensive recommendations for configuring and managing a LoRaWAN network [6].

Figure 3: LoRaWAN gateway on the roof of a house in Kyiv city

1. Practical Recommendations for Configuring a LoRaWAN Network to Ensure Stability and Data Security

In this study, key aspects of configuring a LoRaWAN network will be examined, including best practices for configuration, security management, and performance optimization. The primary focus will be on the practical recommendations outlined in the TR007 document, aimed at enhancing network stability and security.

Network Join Procedure. When a user's sensor is powered on and begins operation, it joins the LoRaWAN network. This procedure has its specificities, but the following key factors must be addressed:

- Choice of Join Method: Use OTAA (Over-The-Air Activation) for better security. ABP (Activation By Personalization) is advisable only in stable or isolated networks.
- DevNonce Counter on the Network Server for OTAA Authorization: Ensure the uniqueness of DevNonce to prevent replay attacks when new sensors join the LoRaWAN network.
- Power Levels. Allowed and recommended adaptive power regulation to improve energy efficiency. This impacts battery savings in user sensors.
- Join Attempt Rate Control. Limit the use of repeated Join requests to avoid network overload.
- Data Protection. Mandatory use of up-to-date AppKey and NwkKey for traffic encryption. This significantly reduces the effectiveness of brute force or guessing attacks [7].

Optimization of Frequency Plan and Channels for the Network Join Process (Fixed Channel Plan Join Process Optimization). The LoRa Alliance emphasizes the need to use frequency parameters specific to the region where the LoRaWAN network is deployed. Key aspects that impact system performance and battery savings during the client sensor's join process to the LoRaWAN network include the following steps:

- Limiting Available Communication Channels. Configured nodes (sensors and LoRa GW gateways) should only use permitted channels in the region, reducing search time (e.g., avoiding searching for US915 frequencies in the EU868 region).
- Frequency Prioritization. Identifying the most stable and least congested channels for priority use.
- Dynamic Adjustment. If Join requests from the sensor frequently fail, adjust the channel list on the gateway (LoRa GW).
- DR (Data Rate) Optimization. Using the appropriate transmission rate for faster connection with minimal energy consumption.
- Parameter Caching. If the device has previously connected, store data about successful channels for quick reconnection [8].

Working with Rolling Session Keys. The end-user sensor communicates in the LoRaWAN network over an encrypted channel. Working with security keys has its specificities and recommendations:

- Regular Updates. Periodic rotation/replacement of AppSKey and NwkSKey positively impacts communication security, complicating potential attacks.
- Use of Rejoin. Utilizing reJoin-request for secure key rotation without requiring a full reconnection.
- Avoiding Predictability. Generating new keys randomly to prevent predictability is a basic and essential security rule.
- Key Storage Protection. Ensuring secure storage of keys on devices, avoiding any leaks, enhances sensor security.
- Synchronization with the Server. Maintaining consistency of keys between the node and the server helps avoid connection loss [9].

Avoiding Synchronous Behavior. This practice can enhance both network security and performance. Synchronous behavior increases security risks and negatively impacts network efficiency, especially when a large number of sensors operate simultaneously. The process consists of the following measures:

- Time Distribution. Avoiding or minimizing the simultaneous activation of a large number of devices to reduce network load.
- Randomized Intervals. Implementing random delays before Join requests and periodic transmissions to prevent packet collisions [10].
- Adaptive Transmission. Using Adaptive Data Rate (ADR) to distribute traffic over time, which also reduces sensor power consumption.
- Diverse Reception Windows. Configuring devices to open data reception windows with slight time variations to improve network efficiency.

- Minimizing Retransmissions. Implementing algorithms on end sensors to reduce the frequency of retransmissions after failed data transmissions [11].

Avoiding Congestion Collapse. In certain situations, a LoRaWAN network may experience congestion due to simultaneous data transmissions, such as periodic sensor reporting or mass network joins (JoinRequest) from multiple sensors at once. LoRaWAN implements a Duty Cycle mechanism to regulate transmission activity, preventing network congestion by limiting the allowable airtime for devices [12]. Table 1 presents Duty Cycle values for different operational time intervals [13].

Table 1

Duty Cycle restrictions

Aggregated during the first hour following power-up or reset	$T_0 < t < T_{0+1}$	*Transmit time < 36 s per hour*	*1% duty cycle*
Aggregated during the next 10 hours	$T_{0+1} < t < T_{0+11}$	*Transmit time < 36 s per 10 h*	*0.1% duty cycle*
After the first 11 hours, aggregated over 24 h, where N refers to days starting at 0	$T_{0+11} + N \times (24$ hours/day) $< t < T_0 + 35 + N \times (24$ hours/day), $N \geq 0$	*Transmit time < 8.7 s per 24 h*	*0.01% duty cycle*

where: T_0 – start of the countdown; T_{0+1} – start of the countdown + 1 hour; t – current time.

To further mitigate traffic congestion in LoRaWAN networks, the following best practices are recommended:

- Limiting Retransmissions. Setting a maximum number of message retransmissions to reduce network load.
- Traffic Distribution. Utilizing different Spreading Factors (SF) and frequency channels to prevent overloading specific communication channels.
- Dynamic Power Adjustment. Reducing transmission power when the connection is stable to optimize network efficiency.
- Device Grouping. Distributing traffic among devices based on time slots or geographic zones to avoid peak loads.
- Monitoring and Adaptation. Implementing network load analysis and adaptive transmission strategies to optimize traffic flow [14].

Discontinuing Retransmissions. Certain practices related to retransmission control can significantly improve network performance, particularly when configurable by end-user devices. If the sensor allows for these adjustments, network efficiency can be greatly enhanced. The key aspects of discontinuing unnecessary retransmissions include:

- Retransmission Limitation. Setting a maximum number of retries to prevent excessive network load.
- Adaptive Strategy. Adjusting SF or frequency instead of continuously retransmitting failed messages.
- Failure Detection. If no acknowledgment is received after several attempts, the device should change its transmission strategy or switch to a low-power mode.
- Time-Based Distribution. Introducing random delays before retransmissions to minimize packet collisions.
- Analytics and Control. Implementing network monitoring to evaluate retransmission efficiency and optimize transmission strategies [15].

Default Channels. The regulatory document [RP002] defines two types of regional channel plans - dynamic and fixed. Default channels are the mandatory channels that must be configured on an end device for a specific region. While the network can disable these channels, all end devices initially operate using the default channels and re-enable all channels after receiving updates via an ADR (Adaptive Data Rate) frame. The following recommendations apply to default channels [16]:

- Compliance with Regional Regulations. Only permitted channels should be used to minimize interference.
- Limiting the Number of Channels. Unused channels should be disabled to reduce the time required for the Join procedure.
- Channel Prioritization. Devices should be configured to prefer the most stable channels.

- Configuration Flexibility. The network should have the ability to dynamically adjust channels based on network load.
- Parameter Updates. Channel settings should be periodically updated to reflect changes in network infrastructure [17].

OTAA Required Persistent Values. This requirement applies to client sensors joining a LoRaWAN network. It refers to a set of stored data within the sensor's memory that must comply with confidentiality and integrity rules:

- Key Retention. AppKey, NwkKey, JoinEUI, and DevEUI must remain unchanged after a sensor reboot.
- Frame Counter (Fcnt) Storage. FcntUp must be preserved to prevent frame reuse issues.
- Join Process Optimization. After a reboot, unnecessary repeated OTAA join requests should be avoided if network parameters remain unchanged.
- Data Security. Secure key storage mechanisms should be implemented to prevent key compromise.

Sensors using ABP (Activation by Personalization) authorization follow the same requirements for their corresponding fields [18].

Adaptive Data Rate (ADR) Support. Used by the network server to optimize the configuration of the end device for better/optimal connection to the LoRaWAN network, minimizing the time the radio module spends in the air and, as a result, reducing the sensor's energy consumption, thereby extending the battery life of the sensor [19]. Figure 4 demonstrates the relationship between speed and the radio module's active time in the air.

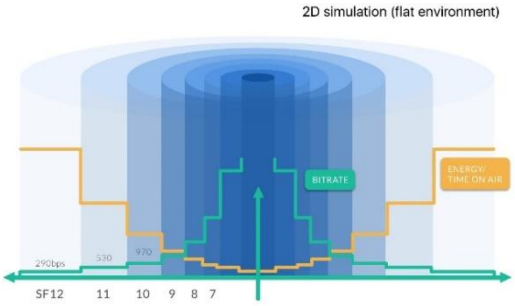

Figure 4: Visualization of the speed versus time of the LoRa module on the air

ADR controls the channel plan, data rate, transmission power, and the number of retransmissions used by the end device. These attributes are dynamically adapted as the network observes changes in radio frequency conditions and configurations of the gateways (LoRa GW) supporting the end device. Direct management and determination of ADR parameters occur on the Network Server since it has access to signal quality parameters and characteristics for the entire network [20].

- Enabling ADR. Using ADR to optimize energy consumption and improve throughput.
- Dynamic Adjustment. The network's ability to automatically adjust SF, transmission power, and frequency for efficient operation.
- Handling Static and Mobile Nodes. It is advisable to activate ADR for all end devices, both stationary and mobile.
- Parameter Monitoring. The network server should analyze SNR, RSSI levels, and communication history to provide the sensor with correct ADR parameters.
- Fallback Mode. If communication with the server is lost, the device should independently adjust data transmission parameters [21].

Power Reduction or ADR Back Off. The ADR system temporarily reduces the transmitter power or adjusts other data transmission parameters to improve signal quality, minimize interference, or optimize network traffic [22]. This includes the following conditions:

- The network server and the end sensor must support a range of functions.
- Adaptive data rate reduction. If the connection quality deteriorates, the spreading factor (SF) increases gradually, avoiding abrupt changes.
- Load minimization. Limiting the frequency of ADR requests to prevent network congestion.
- Stability verification. Parameter adjustments are applied only after multiple failed transmissions..
- Energy conservation. Avoiding frequent SF changes to reduce unnecessary power consumption of the device [23].

Duty Cycle Limitations. The LoRaWAN specification [TS001] defines network operation limitations for each region, affecting both end-user devices and LoRa gateways. These restrictions consider regional specifics, frequency characteristics, and transmitter power parameters, all of which influence network performance in terms of Downlink message transmission and Uplink message reception:

- Compliance with regional regulations. Transmission time restrictions according to regulatory requirements (e.g., 1% duty cycle in the EU868 region).

- Transmission optimization. Utilizing ADR to reduce airtime usage.
- Violation detection. Monitoring spectrum utilization to prevent transmission blocking [24].

Transmit Power. Transmit power is a crucial factor for effectively supporting various operating conditions of an end device, regulated by adjusting the transmitter's power level. Regional parameters are defined in document [RP002], and different regions support different maximum transmission power levels [25]. The following aspects must be considered:

- Compliance with regional limits. Adhering to the allowed maximum (e.g., 14 dBm in the EU868 region) and minimum (e.g., 2 dBm in the EU868 region) transmission power levels.
- Adaptive power reduction. Lowering transmission power when the connection is stable to reduce energy consumption.
- Use of ADR. Allowing the network to automatically adjust power levels based on link conditions.
- Minimization of interference. Avoiding excessive transmission power to prevent network overload and reduce signal interference.
- Performance monitoring. Analyzing signal quality metrics (SNR, RSSI) to determine the optimal power level [26].

Maintaining Time Synchronization. Time synchronization is essential for the proper operation of end-user devices, particularly Class B sensors, ensuring accurate data transmission. Key aspects include:

- Use of Class B sensors. Synchronizing time via GPS or network beacons.
- Clock drift correction. Adjusting internal device timers to prevent synchronization drift.
- Reliable time sources. Utilizing NTP servers or GPS to maintain precise timing in Class A and Class C devices.
- Failure monitoring. Promptly responding to synchronization losses, for example, by re-requesting time updates from the network [27].

Conclusions

LoRaWAN is a powerful technology for energy-efficient and long-range communication in IoT networks. However, the effective deployment of LoRaWAN infrastructure requires adherence to best practices and optimization of configurations. Utilizing OTAA with proper persistent value storage enhances security and reduces network load. Optimizing the connection process through Fixed Channel Plan Join Process Optimization shortens the joining time, while preventing synchronized node behavior helps avoid congestion. At the same time, managing retransmissions and adhering to Duty Cycle limitations are critical for network stability.

To ensure high-quality and reliable communication, it is essential to properly utilize ADR (Adaptive Data Rate) and ADR Back Off, allowing dynamic adaptation of transmission parameters to improve energy efficiency and increase network throughput. Another crucial aspect is the support for 32-bit FcntUp/FcntDown, which enhances security and prevents replay attacks. Compliance with regional Transmit Power regulations and proper Default Channels planning minimizes interference and ensures efficient utilization of the available radio spectrum.

Today, LoRaWAN continues to evolve and secure its place in the business environment. Due to its low cost, flexibility, and ability to be deployed in challenging conditions, this technology is increasingly applied in smart cities, industrial monitoring, agriculture, and logistics. The implementation of advanced approaches to LoRaWAN network configuration not only improves efficiency but also enhances overall communication reliability, making this technology one of the key solutions in the IoT field.

References

[1] The Things Network, “What are LoRa and LoRaWAN?,” The Things Network. https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/.

[2] The Things Network, “LoRaWAN Architecture,” The Things Network. https://www.thethingsnetwork.org/docs/lorawan/architecture/.

[3] “Regional Parameters,” The Things Network. https://www.thethingsnetwork.org/docs/lorawan/regional-parameters/.

[4] Y. Pidhaina, “Only the ‘armed’ will endure: How the Internet of Things helps businesses cope with crises,” Mind.ua, Apr. 29, 2020. [Online]. Available: https://mind.ua/publications/20208969-vistoyat-ozbroeni-yak-internet-rechej-dopomagae-biznesu-vporatisya-z-krizoyu.

[5] M. Katayeva, “Infrastructure for the implementation of the Internet of Things built in the capital,” *Vechirniy.Kyiv.ua*, Feb.

3, 2022. [Online]. Available: https://vechirniy.kyiv.ua/news/61028/.

[6] TR007 Developing LoRaWAN® Devices v1.0.0, "TR007 Developing LoRaWAN Devices v1.0.0," Lora-alliance.org, Feb. 03, 2021. https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[7] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.1.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[8] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.2.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[9] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.5.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[10] "rfc4086," datatracker.ietf.org. https://datatracker.ietf.org/doc/html/rfc4086

[11] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.7.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[12] LoRa Alliance, TS001-1.0.4 LoRaWAN L2 1.0.4 Specification, 2020, sec. 5.3. [Online]. Available: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification.

[13] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, page. 18. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[14] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.8.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[15] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.9.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[16] LoRa Alliance, RP002-1.0.4 Regional Parameters, 2022, sec. 1.3. [Online]. Available: https://resources.lora-alliance.org/technical-specifications/rp002-1-0-4-regional-parameters.

[17] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.10.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[18] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.13.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[19] "Academy for LoRaWAN: Spreading Factors, Airtime, and Adaptive Data Rate | | Academy for LoRaWAN," Semtech.com, 2023. https://learn.semtech.com/mod/page/view.php?id=141.

[20] LoRa Alliance, TS001-1.0.4 LoRaWAN L2 1.0.4 Specification, 2020, sec. 5.2. [Online]. Available: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification.

[21] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.15.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[22] LoRa Alliance, TS001-1.0.4 LoRaWAN L2 1.0.4 Specification, 2020, sec. 4.3.1.1 [Online]. Available: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification.

[23] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.16.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[24] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.17.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[25] LoRa Alliance, RP002-1.0.4 Regional Parameters, 2022, sec. 2.3.3. [Online]. Available: https://resources.lora-alliance.org/technical-specifications/rp002-1-0-4-regional-parameters.

[26] LoRa Alliance, TR007-1.0.0 Developing LoRaWAN Devices, 2021, sec. 3.18.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-0-0.

[27] LoRa Alliance, TR007-1.1.0 Developing LoRaWAN Devices, 2024, sec. 3.20.2. [Online]. Available: https://resources.lora-alliance.org/document/tr007-developing-lorawan-devices-v1-1-0.