UNIZA

LoRaWAN Technology

Professor M. Segeč

STENGER THOMAS
28/04/2025

UNIVERSITY OF ŽILINA

Table of Contents

Glossary

Chirp : A signal in which the frequency increases or decreases linearly with time, used in LoRa modulation.

Spread Spectrum : A technique in which a signal is deliberately spread in frequency domain, resulting in a signal with a wider bandwidth. This is done for reasons such as evading jamming, reducing power flux density, multiple access, and secure communication.

Spreading Factor (SF) : A parameter in LoRa that determines the rate at which the chirp signal spreads in frequency. A higher SF increases sensitivity and range but reduces the data rate.

Adaptive Data Rate (ADR) : A mechanism in LoRaWAN that dynamically adjusts the data rate and spreading factor for each end-device based on the link quality, optimizing network performance and power consumption.

Duty Cycle : The percentage of time a device is allowed to transmit within a given period, often regulated to prevent spectrum congestion.

AES-128 (Advanced Encryption Standard with 128-bit key) : A symmetric block cipher widely used for securing electronic data. LoRaWAN uses AES-128 for both application and network layer encryption.

AppSKey (Application Session Key) : An AES-128 session key shared between the end-device and the Application Server, used to encrypt and decrypt the application payload.

NwkSKey (Network Session Key) : An AES-128 session key shared between the end-device and the Network Server, used to ensure the integrity and authenticity of the MAC layer messages.

UNIVERSITY OF ŽILINA

Introduction to LoRaWAN

LoRaWAN (Long Range Wide Area Network) is a wireless communication protocol designed for low-power wide-area networks (LPWAN). It enables the connectivity of IoT devices over long distances with minimal energy consumption, making it ideal for applications that require extended battery life.

LoRaWAN was developed by the LoRa Alliance, a consortium of companies founded in 2015. The primary goal was to standardize LPWAN communications to ensure interoperability between devices from different manufacturers. Since its inception, LoRaWAN has seen rapid adoption across various sectors, including smart cities, agriculture, industry, and resource management.

LoRaWAN is used in a multitude of applications where long-range connectivity and low power consumption are crucial. Some of the most common applications include:

- Smart Cities : Management of public lighting, air quality monitoring, waste management.
- Smart Agriculture : Crop monitoring, irrigation management, weather condition surveillance.
- Industry : Predictive maintenance, asset tracking, process automation.
- Resource Management : Monitoring of water and energy consumption, management of distribution networks.

LoRa Technology

Lora Modulation Principle

LoRa (Long Range) utilizes a proprietary modulation based on **Chirp Spread Spectrum** (CSS), developed by Semtech. This modulation technique is particularly effective for long-range and low-power communications. Here is a detailed explanation of how it works:

CSS modulation relies on the use of "chirp" signals, which are frequency pulses that vary linearly with time. These signals can be of the "up-chirp" type (increasing frequency) or "down-chirp" type (decreasing frequency). Here are the main characteristics of this modulation:

A chirp is generated by varying the frequency of the signal linearly over a certain bandwidth. For example, a chirp can sweep a frequency band ranging from 868 MHz to 868.1 MHz.

The duration of the chirp depends on the **Spreading Factor** (SF), which determines the number of symbols per second. A higher SF means a longer chirp duration and better sensitivity, but a lower data rate.

Chirps are resistant to interference and noise due to their wide bandwidth. Even if part of the signal is disturbed, it is possible to reconstruct the complete information from the unaffected parts. CSS modulation also makes it possible to detect and correct errors, thus improving the reliability of communications.

At the receiver, the signal is correlated with a reference chirp to determine the initial frequency of the transmitted chirp. This operation makes it possible to decode the transmitted information. CSS demodulation is robust and can work even with very weak signals, which is crucial for long-range communications.

The SF determines the duration of the chirps and directly influences the sensitivity and data rate. A high SF (for example, SF12) offers better sensitivity but a lower data rate, while a low SF (for example, SF7) offers a higher data rate but a reduced range. LoRa devices can dynamically adjust the SF based on communication conditions, thanks to techniques like **Adaptive Data Rate** (ADR).

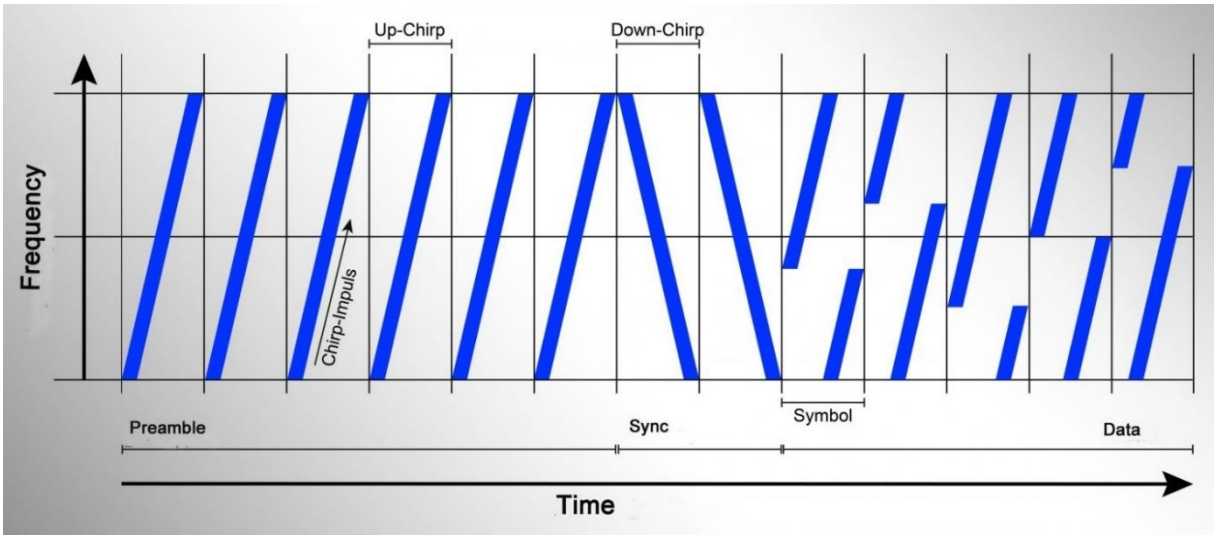

Figure 1: Modulation Lora

Technical Charasteristics

LoRa makes it possible to detect extremely weak signals thanks to its exceptional sensitivity, which can reach up to -149 dBm.

The range of LoRa can reach several kilometers in rural areas and up to 2-5 km in urban areas, depending on obstacles and environmental conditions.

Thanks to its efficient modulation and sleep cycles, LoRa allows devices to operate for several years on a single battery.

The data rate varies from 0.3 kbps to 50 kbps, depending on the spreading factor (SF) and the bandwidth used.

Comparison with other LPWAN Technologies

LoRaWAN stands out from other LPWAN technologies like SigFox and NB-IoT in several ways:

- SigFox: Uses ultra-narrowband (UNB) modulation and offers a similar range to LoRaWAN, but with a lower data rate and limited network capacity.
- NB-IoT: Uses existing cellular infrastructure (LTE) and offers better indoor coverage, but with higher power consumption and greater deployment costs.

LoRaWAN Architecture

The LoRaWAN architecture is designed to be simple and efficient, enabling bidirectional communication between end-devices and applications via a network infrastructure. The main components of this architecture are:

End-Devices :

End-devices are the sensors or actuators that collect data or execute commands. They communicate with gateways using LoRa modulation.

They can be classified into three categories: Class A, Class B, and Class C, depending on their communication needs and power consumption.

Class	Description	Characteristic	Typical Use
Class A	Low-power bidirectional communication	-Receive windows after each uplink transmission -Minimal power consumption - High latency	Temperature sensors, humidity sensors, tracking devices
Class B	Communication with scheduled receive windows	-Receive windows synchronized with periodic beacons - Moderate power consumption -Moderate latency	Devices requiring regular updates, such as smart meters
Class C	Continuous communication	-Quasi-continuous receive windows - High power consumption -Low latency	Devices requiring real-time communication, such as industrial actuators

Gateways :

Gateways act as relays between the end-devices and the Network Server. They receive messages from the end-devices and transmit them to the Network Server via a backhaul connection (often IP/Ethernet). Gateways can cover large areas and manage simultaneous communications with multiple end-devices.

Network Server :

The Network Server is the core of the LoRaWAN network. It manages communications between the end-devices and the gateways, ensures data security, and optimizes network performance.

It is responsible for device authentication, security key management, and Adaptive Data Rate (ADR) to dynamically adjust communication parameters.

Application Server :

The Application Server processes the data received from the end-devices and makes it available for end-user applications. It can also send commands to the end-devices via the Network Server. It enables integration with various cloud platforms and services for data analysis and visualization.

Network Topology

LoRaWAN uses a star topology, where end-devices communicate directly with one or more gateways. This topology simplifies network deployment and management while allowing for extensive coverage. End-devices can send data to gateways (uplink) and receive commands or confirmations (downlink). Furthermore, end-devices can move within the network's coverage area without requiring reconfiguration, thanks to the centralized management by the Network Server.

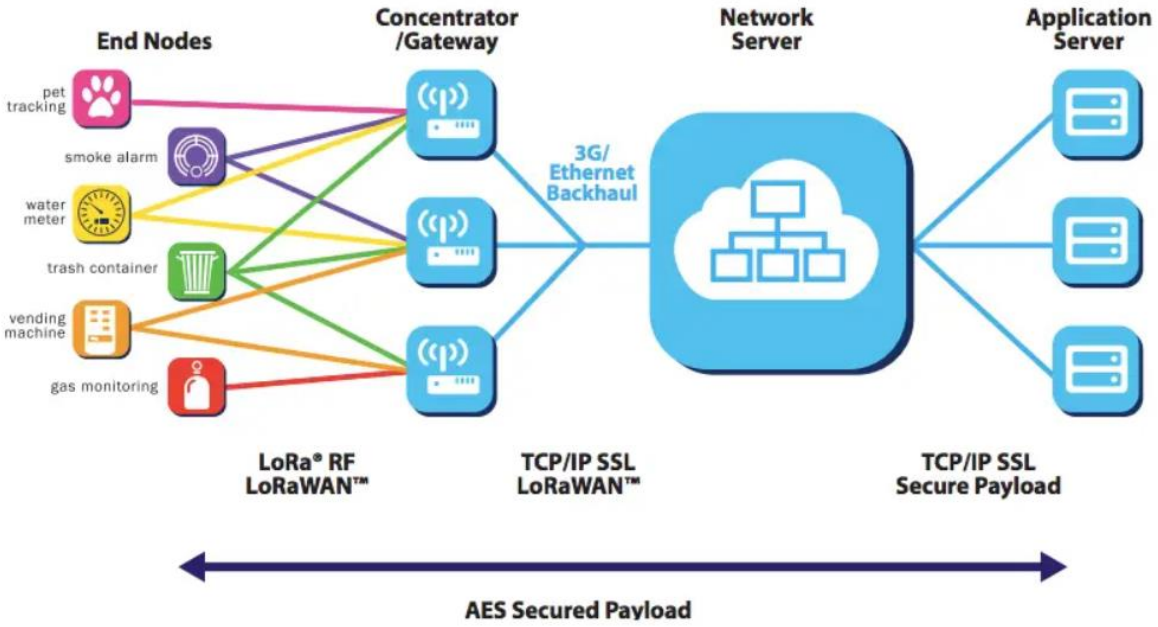

Figure 2 : Architecture diagram

Frequency Bands Used in Slovakia

In Slovakia, LoRaWAN primarily uses the 863-870 MHz frequency band, in accordance with European regulations. This band is divided into several sub-bands to optimize spectrum usage and minimize interference.

In Slovakia, as in the rest of Europe, the duty cycle is limited to 1%. This means that a device can only transmit for 1% of the time over a given period, which is approximately 36 seconds per hour. This limitation is essential to avoid spectrum saturation and ensure harmonious coexistence with other users of the band, such as security systems and medical devices, by reducing interference and ensuring a fair sharing of radio resources.

The transmission power of LoRaWAN devices is regulated to prevent interference with other systems. In general, the maximum authorized power is 14 dBm (25 mW) for fixed devices and 27 dBm (500 mW) for mobile devices.

In Europe, the 863-870 MHz frequency band is divided into several channels reserved for specific uses to ensure the reliability of critical communications.

- The 869.525 MHz channel is dedicated to social alarm systems, such as telecare devices for the elderly or disabled, thus ensuring the reliable and interference-free transmission of alerts.
- The channels from 869.400 MHz to 869.650 MHz are used for bidirectional communication between devices and gateways, allowing for two-way data exchange, which is essential for applications requiring confirmations or remote commands.
- The channels from 868.000 MHz to 868.600 MHz are often reserved for low-power sensors and devices, minimizing interference and optimizing spectrum usage.
- The channels from 868.700 MHz to 869.200 MHz are intended for industrial, scientific, and medical (ISM) applications, ensuring reliable communication for critical equipment such as medical devices or industrial sensors.

Security in LoRaWAN

Security is a crucial aspect of any communication network, and LoRaWAN integrates several mechanisms to ensure the confidentiality, integrity, and authenticity of the exchanged data.

Data Encryption

LoRaWAN uses **AES-128** (Advanced Encryption Standard) encryption to protect the data transmitted between the end-devices and the Network Server. Encryption is applied at two levels :

- The payload data is encrypted with a session key (**AppSKey**) shared between the end-device and the Application Server. This ensures that only authorized applications can access the data.
- The entire message, including headers and payload, is encrypted with a network key (**NwkSKey**) shared between the end-device and the Network Server. This protects against man-in-the-middle attacks and ensures message integrity.

Device Authentication

Device authentication is essential to prevent unauthorized devices from accessing the network. LoRaWAN uses two main methods for authentication :

Activation By Personalization (ABP) :

Activation By Personalization (ABP) is a secure connection method for LoRaWAN devices that simplifies the authentication process. Unlike Over-The-Air Activation (OTAA), where session keys are dynamically generated during the first connection, ABP uses pre-configured keys (NwkSKey and AppSKey) that are stored on both the device and the Network Server. This method allows devices to connect to the network immediately without requiring an initial key exchange, thus reducing complexity and deployment time. However, it necessitates secure key management to avoid any risk of compromise.

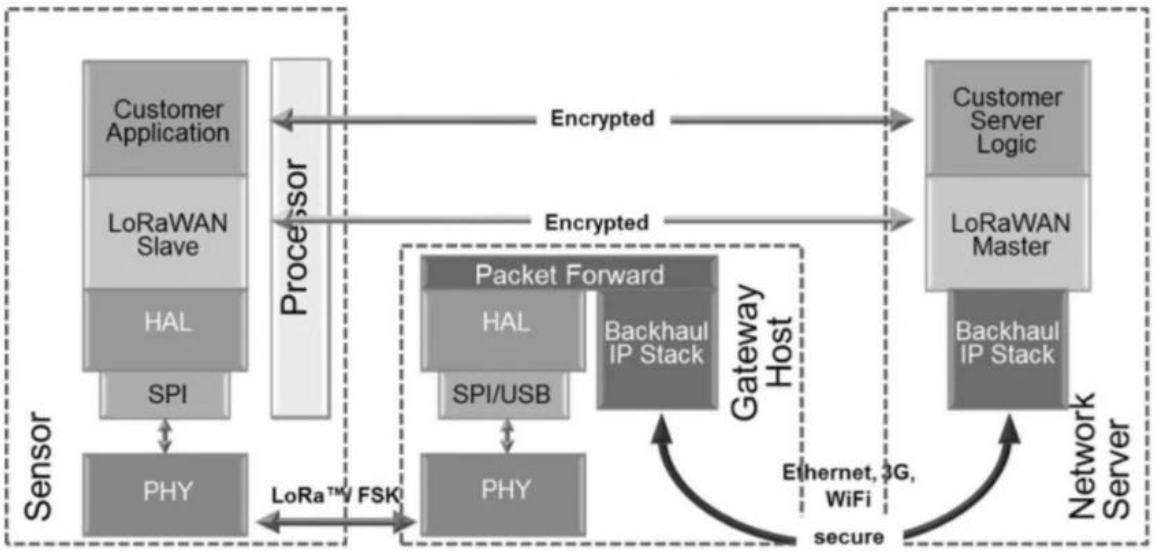

Figure 3 : Authentication ABP

Over-The-Air Activation (OTAA) :

Over-The-Air Activation (OTAA) is a secure connection method for LoRaWAN devices that ensures dynamic and robust authentication. Unlike Activation By Personalization (ABP), OTAA uses a master key (AppKey) to establish a secure session during the first connection. During this activation phase, the device and the Network Server exchange information to dynamically generate the session keys (NwkSKey and AppSKey). This approach offers enhanced security because the session keys are unique for each device and each session, thus reducing the risk of compromise. Although OTAA requires an initial key exchange, it is often preferred for its flexibility and increased security, especially in environments where key management is critical.

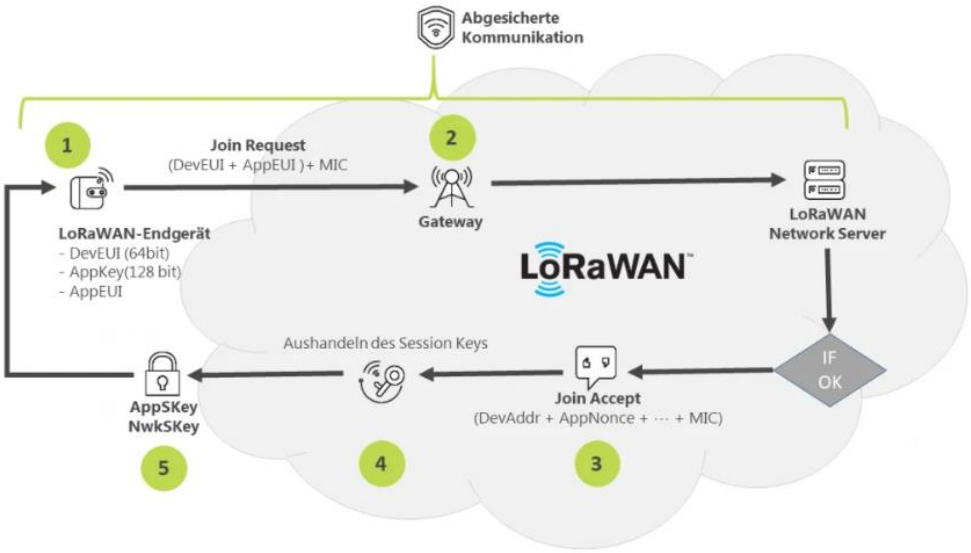

Figure 4 : Authentication OTAA

Security Key Management

Key management is a critical aspect of security in LoRaWAN. Keys must be protected against unauthorized access and leaks. They must be stored in secure memory on the end-devices and servers.

Session keys can be renewed periodically to enhance security. Additionally, network administrators must monitor key access and usage to detect any suspicious activity.

Setting Up a Private LoRaWAN Network

Setting up a private LoRaWAN network allows for a dedicated communication infrastructure, offering better security, control, and customization. Here are the key steps to deploy a private LoRaWAN network.

Firstly, it is essential to properly plan and configure the network. Install gateways in strategic locations to maximize network coverage. Use planning tools to determine the best locations. Then, configure the gateways with the appropriate network parameters, such as frequency band, channels, and duty cycle.

Secondly, configure the Network Server to manage devices and gateways. Define security settings, including encryption keys and authentication mechanisms, to ensure the protection of communications. Also, enable features like Adaptive Data Rate (ADR) to optimize communications and improve network efficiency.

Thirdly, configure the Application Server to receive data from the Network Server and process it according to your specific needs. Integrate the Application Server with your data management and analysis platforms to fully leverage the collected information. This integration allows for the centralization and analysis of data, thereby facilitating decision-making and process optimization.

Network Deployment and Coverage

To ensure optimal network coverage, it is crucial to conduct coverage tests. Perform tests to verify that devices can communicate with gateways throughout the deployment area. If necessary, adjust the locations of gateways to improve coverage and ensure reliable communication.

Use monitoring tools to track network performance and identify potential issues, such as collisions and interference. Based on the results, adjust communication parameters, such as the spreading factor and transmission power, to optimize performance and ensure efficient data transmission.

You can also use management platforms to configure and monitor devices and gateways. These tools allow you to manage software updates, communication settings, and alerts, thereby facilitating network maintenance and optimization.

Finally, deploy monitoring tools to track network performance in real-time. These tools enable the rapid detection of anomalies and the implementation of corrective measures, ensuring optimal network availability and reliability.

Network Scalability and Capacity

The scalability and capacity of a LoRaWAN network are crucial aspects for ensuring efficient and reliable communication, especially as the number of connected devices increases.

In theory, a LoRaWAN network can support thousands of devices per gateway. However, the actual capacity depends on several factors, including the duty cycle, the spreading factor (SF), and the frequency of transmissions.

To estimate the maximum number of end-points that a LoRaWAN network can support, several parameters need to be taken into account. Here is a method to calculate this limit:

The transmission time of a message depends on the spreading factor (SF) used. For example, a message with SF7 will take less time to transmit than a message with SF12. Use the technical specifications of LoRa to determine the transmission time for each SF. This time varies depending on the modulation and the length of the message.

Multiply the transmission time by the number of messages each device sends per day. For example, if a device sends 10 messages per day with a transmission time of 50 ms per message, the total transmission time per day is 500 ms. This calculation is essential to understand the total load each device imposes on the network.

The duty cycle limits the total time a device can transmit. For example, with a duty cycle of 1%, a device can transmit for 864 seconds per day (1% of 86400 seconds). Compare the calculated total transmission time with the limit imposed by the duty cycle to determine if the device complies with this constraint. This ensures that the device does not exceed regulatory limits.

Divide the total transmission time allowed by the duty cycle by the total transmission time per device. For example, if the total transmission time allowed is 864 seconds per day and each device requires 500 ms per day, the maximum number of devices is 864 / 0.5 = 1728 devices. This calculation helps plan network capacity and avoid spectrum saturation.

Conclusion

LoRaWAN is establishing itself as a key technology for long-range, low-power communication networks, meeting the growing needs of the Internet of Things (IoT). Throughout this report, we have explored the technical aspects of LoRaWAN, from the principles of CSS modulation to the establishment of a private network, including device classes, security, and scalability. CSS modulation offers high sensitivity and resistance to interference, enabling long-range communications with low power consumption, while frequency bands vary by region, requiring compliance with local regulations. The star architecture simplifies network deployment and management, with key components (end-devices, gateways, Network Server, Application Server) ensuring secure and efficient bidirectional communication. Classes A, B, and C meet different needs in terms of power consumption and latency, offering flexibility for various applications. AES-128 encryption and authentication mechanisms ensure the confidentiality, integrity, and authenticity of data, while security key management is essential to protect communications against unauthorized access. The choice and configuration of equipment, as well as the optimization of communications, are crucial to ensure network performance and reliability, with management and monitoring tools allowing for real-time parameter monitoring and adjustment. Network capacity depends on several factors, including duty cycle, spreading factor, and transmission frequency, and optimization techniques such as ADR and the use of repeaters can improve scalability and reduce collisions. In conclusion, LoRaWAN offers a robust and flexible solution for long-range, low-power IoT communications, with a modular architecture, advanced security mechanisms, and the ability to adapt to various applications, making it a preferred choice for current and future IoT deployments.

Sources

1. LoRa Alliance. (2023). *LoRaWAN Specification*.
2. Augustin, A., et al. (2016). *Study of LoRaWAN for Metropolitan-Scale Deployment*. IEEE Sensors Journal.
3. Centenaro, M., et al. (2016). *Long Range Low Power Networks for the Internet of Things*. IEEE Internet of Things Journal.
4. LoRa Alliance. (2023). LoRaWAN Security Overview. Récupéré de LoRa Alliance
5. Donmez, M. A., & Rong, T. (2018). A Survey on Security of LoRaWAN. IEEE Access.
6. Butun, I., & Mori, P. (2018). Security Analysis of LoRaWAN. IEEE Internet of Things Journal.
7. LoRa Alliance. (2023). LoRaWAN Network Deployment Guide. Récupéré de LoRa Alliance
8. Semtech Corporation. (2023). LoRaWAN Network Planning and Optimization. Récupéré de Semtech