APPLICATIONS OF LORAWAN TECHNOLOGY

By Döníz Borsos PhD student
Óbuda University, Doctoral School on Safety and Security Sciences, Hungary
borsos.doniz@phd.uni-obuda.hu

Abstract
LoRaWAN is a network specification that has been in continuous development since 2015 by the LoRa Alliance[1]. Its base is the LoRa technology by Semtech, which dates back to 2013[2]. Thanks to the particular modulation of radio technology, it accomplishes long-range, low power consumption wireless communication, even in unfavorable conditions such as in reinforced concrete buildings, underground car parks, basements, or areas without current supply.

Keywords
LoRaWAN, LoRa Alliance, LoRaWAN specification, Information security, Security challenges

INTRODUCTION TO LORAWAN TECHNOLOGY

Technology background

LoRaWAN technology can be used in many areas. Before describing the application areas, it is significant to know the background of the technology.

LoRa technology is on a point-to-point connection. LoRa is the basis of LoRaWAN technology, in which case we can talk about network operation. The LoRa Alliance is developing a network specification. The association currently has seventy-six operator members[1]. The essence of the technology is to create long-range wireless network, even in unfavorable field conditions, while minimizing power consumption. LoRa technology has a long-range wireless network thanks to advanced modulation, the Chirp Spread Spectrum (CSS)[3]. The LoRaWAN communication protocol defines the lower three layers of the OSI model: the physical, the MAC sublayer of the data link layer, and the network layer.

Communication in Europe is at 868MHz and 433MHz in the ISM band. The devices are wirelessly connected, and the data link is bi-directional. Data submission time is limited, with a fill rate of up to 1%. Network devices are interconnected in star-of-stars topology. End-nodes consumption and data transfer rates are low (0.3–50kbit/s). The bridging distance, according to the specification, is 10 - 15km. Communication uses AES-128 encryption[4].

The Network

The LoRaWAN network includes end-nodes, gateway(s), a network server, and application server(s)[5]. The end-nodes may be connected to different sensors and actuators. The end-devices transmit information to the gateways via LoRa. The gateways in the network receive data from the end-nodes and forward it to the network servers. The network server is responsible

for encoding, decrypting, and communicating with the application server.

Communication from the end-node to the application server is bidirectional; a message can be uplinked and downlinked. The messages can be confirmed and unconfirmed. In case of an unconfirmed message, there is no feedback on arrival[5].

The end-nodes are divided into three classes: Class A, Class B, and Class C. The Class A device opens two receive windows after each transmission and can receive messages only during this period. The Class C devices can receive between transmissions. Class B devices can get messages periodically. Depending on these, Class A devices have the lowest consumption and Class C devices the highest.[5]

The essential features have been described above. All of these must be considered when applying LoRaWAN technology.

APPLICATIONS OF THE TECHNOLOGY

Fields of application, examples

The technology is widespread, and there are various applications in critical infrastructures. There are applications in the energy industry, water supply, health care, food industry, transport, and transportation. Before describing the application examples, it is essential to highlight the positive features of the technology. LoRaWAN technology is a transition between indoor wireless networks and outdoor cellular networks. Like cellular networks, it provides long data transmission distances. LoRaWAN has a much longer range than WiFi or Bluetooth Low Energy and has robust results in penetrating underground buildings and ferroconcrete structures. It is suitable for both indoor and outdoor use.

End-nodes are characterized by low power consumption, which means they can operate on a button cell for up to 5 - 10 years[1]. As a result, they can run for many years without maintenance. Another positive feature is the ability to operate under adverse environmental conditions. An additional benefit of the technology is the possibility to build private networks or use a network of service providers. The 10 - 15km data transmission distance should be kept in mind. This distance means that a single gateway provides high coverage.

The most common application of LoRaWAN technology is measurement data collection in the energy industry and tracking in transport management. First, let us look at the electricity industry. Electricity distribution and transportation is a vital issue in the maintenance of critical societal functions. The technology is capable of covering areas – rural, highland, wilderness – where no other technology is available. This allows the entire wiring network to be monitored. There are applications for monitoring wire, copper thefts, various sabotage and attacks, high-voltage pylon integrity, and – of course – monitoring consumption data. Why is it relevant to monitor consumption data? The electricity supplier needs to know the consumption data even for residential customers; otherwise, the demand and supply balance of the electricity network will be affected.

Second, let us look at areas of tracking applications. The most common applications of LoRaWAN technology tracking tools are cargo, fleet, wagon, and car tracking. Real-time positioning and tracking facilitate traffic monitoring. It can be used to monitor loads and traffic on each road section. Usually, GPS tracking devices are supplemented with other sensors, accelerometer, magnetometer. As a result, illegal movements and displacements can also be detected. In places where a GPS signal is not available, it is still possible to send a life signal, a status signal. Because of the positive features described above, the use of technology in tracking is widespread.

Unfortunately, smart meters and trackers represent a potential risk to critical infrastructures. The following section analyzes these issues.

1 Based on average data:
RX Current Consumption: 40mA (10dBm)
Airtime: 100ms
Data length: 10byte
Cycle: 10min
Power consumption of microcontroller and sensors: 10mA
Measuring time: 1ms
Microcontroller consumption in sleep mode: 1uA

Risks of applications in the light of specifications

This section describes the application problems of LoRaWAN technology in light of the specifications. The weaknesses of current products and systems are also taken into account. Then, the following chapter describes the application experience and measurement results.

The specifications released by the LoRa Alliance are V1.0 January 2015, V1.0.1 February 2016, V1.0.2 July 2016, V1.1 October 2017, and V1.0.3 July 2018[5, 6, 7, 8, 9]. Of these specifications, the 1.0.x specification series build on each other, an improved version of 1.0. In V1.0.x, the earlier versions' typos and inaccuracies were mainly corrected[5, 8]. New versions are compatible with older specifications. Version 1.1 is a bit different from the other three. In the V1.1 specification, a Join Server is added to the classical network model: end-nodes, gateways, Network Server, and Application Servers[9]. The role of the Join Server will be discussed later.

Let us look at security challenges for network participants. In the case of end-nodes, physical protection is paramount. The attacks may be a deliberate attack, but it may be that changing environmental factors are causing the problem. In the case of motes, there may be additional design and installation problems. The end-nodes are mainly battery operated, so it is crucial to have continuous automatic power supply monitoring and charge level indication. Most LoRa modules provide this option or can be replaced by an additional circuit. According to the data of the home provider, most of the developments failed due to inadequate antenna selection[10]. Of course, identifiers and keys must be stored securely on the end-nodes. Gateways are the weakest part of the network. If a gateway is dropped from the network in any way, communication will be lost. There are several gateways in a well-designed network. In this way, the inaccessibility of one or a few is not a problem. The servers have many problems. In the V1.1 specification, the Join Server appears. Its job is to store and manage the root keys of the devices[9]. As a result, the specification defines new identifiers and keys (e.g., three new network session keys). Key management poses new challenges for service providers. Unfortunately, most service providers store all keys and IDs on a single network server.

A connection procedure precedes the network operation of the end-nodes. The connection mode can be either ABP or OTAA. ABP mode provides a reduced level of security because the devices use the same keys for communication and there is no key exchange. OTAA mode provides a more flexible and secure connection. The V1.1 specification has a re-key possibility, but it can only be used in OTAA mode[9]. The ABP connection mode is only recommended during the development phase.

The V1.0.x specifications have a single frame counter[5, 6, 7, 8], while V1.1 defines three different frame counters[9]. The three counters are used to track data frames. The specification states that the counters cannot be reset in ABP mode. With this in mind, the counter values must be stored separately in the nodes. Another problem is monitoring the overflow of frame counters. In OTAA mode, the counter cannot be restarted after an overflow[9]. Saturation of the frame counter is also an important design aspect.

There are other remaining issues with the specifications. The V1.1 specification states that a malicious Network Server can change the content of messages. The specification basically considers Network Servers as trusted. As a suggestion, the specification states that additional security features can be incorporated into the communication between the motes and the servers. There is no specific solution in the specification[9].

Another such thing is the exit procedure. What happens to devices when they are no longer part of the network and not used anymore? What happens to keys, IDs, and counters? There is no answer in the specifications.

APPLICATION EXPERIENCES

In the previous section, the applications of LoRaWAN technology were described in the power industry and tracking, and the risks of the applications were presented in light of the specifications. Manufacturers' documentation and technical specifications are not always in line with practical experience and the results

Figure 1: Coverage test in Budapest.

of real-world applications. This chapter describes the results of four measurements and applications.

The first measurement is a coverage test – measuring the data transmission distance by an indoor, private gateway in downtown Budapest. Devices used: Kerlink Wirnet iFemtoCell IoT indoor LoRaWAN gateway, Micromite GPS LoRa MOTE, Loriot network service. Other communication parameters: DR0, SF12, 125kHz, 250bit/s. The measurement was made by walking around the building and monitoring the messages sent by the LoRaWAN GPS device via the Loriot service. The received coordinate was displayed using a map application. Figure 1 shows the results of the coverage test.

The green dot in the middle of the figure represents the location of the gateway. Pins in the red area show received messages from a distance of 160–250m. The percentage of successfully received messages is 50% in the red area. The successful transfer of data from the blue area (100–160m) is approximately 70%. The green area (–100m) contains most of the pins. Here, the rate of successful data transfer is 95%.

The second measurement is similar to the first measurement, the purpose of the measurement: data transmission distance by an indoor gateway in Budakeszi. Devices used: Kerlink Wirnet iFemtoCell IoT indoor LoRaWAN gateway, Micromite GPS LoRa MOTE, Loriot network service. The communication parameters, measurement, and display are the same as the first measurement. Figure 2 shows the results of the coverage test in Budakeszi.

90% of the messages were successfully received within 240m of the gateway (the green area around the green dot). In the blue area (240-450m), only 60% of the messages were received. The two red areas are particular because there are sections where there was no data transfer. In these areas, 80% of the data were successfully received.

The third measurement is also a coverage test. The purpose of the measurement is to examine the network coverage of the national service provider in Budapest. Devices used: Micromite GPS LoRa MOTE, service network, Loriot network ranger tester application. The measurement shows how many

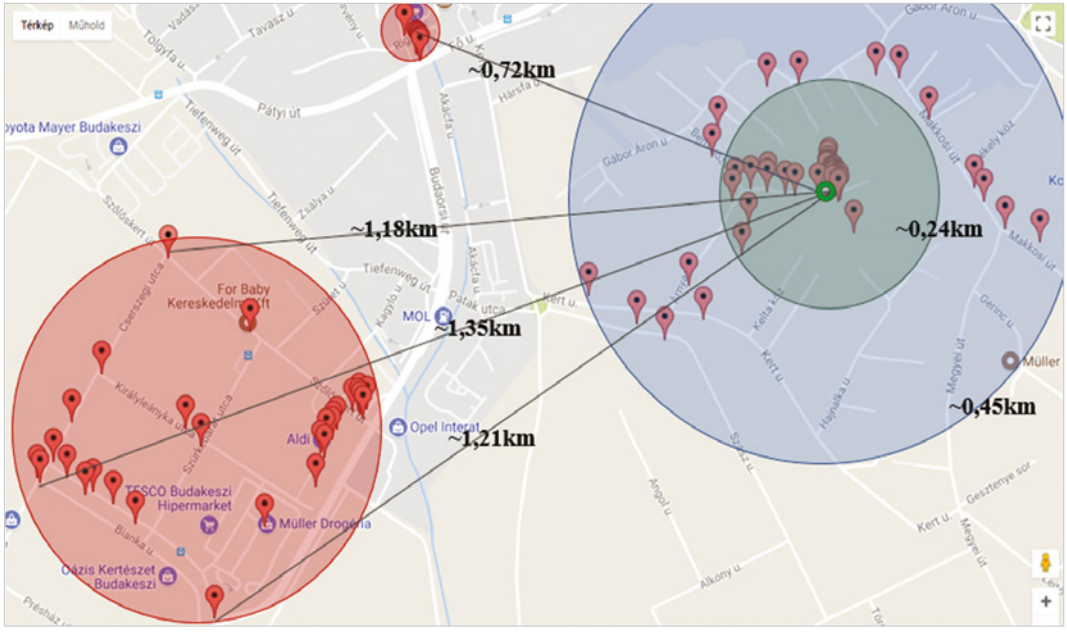

Figure 2: Coverage test in Budakeszi.

gateways the end-nodes see. The following results show the places and buildings that are important for critical infrastructure. Figure 3 shows the result of the measurement at the Árpád Bridge: the end-node sees eight gateways.

On Hungária Boulevard, on average, ten gateways receive messages, but up to 20 in certain parts. In contrast, only 2 - 3 gateways receive messages from the Springfield campus of Óbuda University. 5 - 10 gateways around the Petofi Bridge receive motes messages. During the measurements, an average of five gateways received data in the downtown area, and there was no outdoor location, where messages were not received.

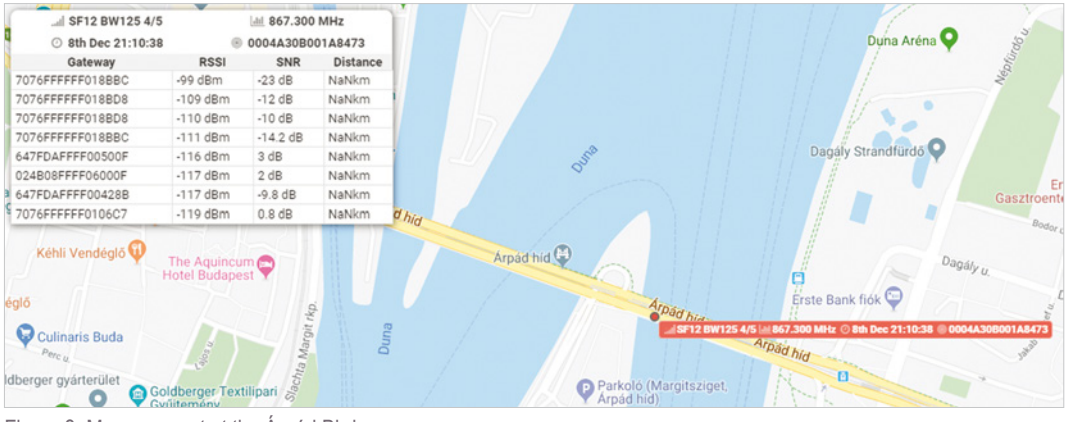

Figure 3: Measurement at the Árpád Birdge.

	Case 1	Case 2	Case 3	Case 4
Data rate limit	290-5470bps No limit	290-5470bps No limit	290-440bps	290-440bps
Payload	16byte	6byte	16byte	6byte
Rate of messages sent and received	56%	80%	82%	90%

Table 1: Underground garage test result.

The fourth measurement was in a reinforced concrete underground garage. Its purpose: to determine the ratio of sent and received messages at different data rates and message lengths. Devices used: RN2483 - LoRa Development Tool, Kerlink iFemtoCell Gateway, and Loriot Network Service. Location of the end-node: underground garage. Location of the gateway: 100m from the mote, 1st floor of a brick building.

Table 1 shows the results of the measurements in the underground garage. Reducing the data transfer rate and the size of the payload, the rate of successful data transfers increases.

CONCLUSION

When using or developing technology, the specification is always the basis. Based on the current specifications, there are still issues that require modifications or improvements. Beyond documentation and specifications, the application experience provides the most information.

The measurement results described above can be relevant when designing a LoRaWAN application. Summarizing the results of the four measurements, the selection of the appropriate gateway is an important consideration. The results show that the data transmission distance of the indoor gateway is well below the coveted 10 - 15km. Based on the tests, it can be concluded that the gateway coverage of Budapest is adequate for most applications. The fourth measurement shows that data transfer is possible under particular conditions.■

REFERENCES

1. About LoRa Alliance https://lora-alliance.org/about-lora-alliance (2019. 10. 15.)
2. Semtech LoRa® Overview Emitech IoT days, 2017 https://www.emitech.fr/sites/emitech.fr/files/5-semtech_emitech_lora.pdf (2019. 10. 15.)
3. What is LoRa? https://www.semtech.com/lora/what-is-lora (2019. 10. 16)
4. What is the LoRaWAN specification? https://lora-alliance.org/about-lorawan (2019. 10. 16)
5. LoRa Alliance: LoRaWAN Specification V1.0, 2015
6. LoRa Alliance: LoRaWAN Specification V1.0.1, 2016
7. LoRa Alliance: LoRaWAN Specification V1.0.2, 2016
8. LoRa Alliance: LoRaWAN Specification V1.0.3, 2018
9. LoRa Alliance: LoRaWAN Specification V1.1, 2017
10. Antenna Hungária: A LoRaWAN IoT szolgáltatói szemmel 1-2. – üzleti aspektusok, presentation, 2019

ABOUT THE AUTHOR

Döníz Borsos is a PhD student and lecturer at Óbuda University. She has been working as a development engineer for two years with unique IoT products and orders. Since 2016 she has been dealing with IoT technologies, especially LoRaWAN. In 2017, she obtained a master's degree in Safety Engineering from Óbuda University. She graduated as an electrical engineer in 2018.