www.czasopisma.pan.pl PAN www.journals.pan.pl

INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 4, PP. 841-854
Manuscript received October 16, 2022; revised November 2022. DOI: 10.24425/ijet.2022.143893

LoRaWAN Communication Implementation Platforms

Joanna Szewczyk, Mariusz Nowak, Piotr Remlein, and Aleksandra Głowacka

***Abstract*—A key role in the development of smart Internet of Things (IoT) solutions is played by wireless communication technologies, especially LPWAN (Low-Power Wide-Area Network), which are becoming increasingly popular due to their advantages: long range, low power consumption and the ability to connect multiple edge devices. However, in addition to the advantages of communication and low power consumption, the security of transmitted data is also important. End devices very often have a small amount of memory, which makes it impossible to implement advanced cryptographic algorithms on them. The article analyzes the advantages and disadvantages of solutions based on LPWAN communication and reviews platforms for IoT device communication in the LoRaWAN (LoRa Wide Area Network) standard in terms of configuration complexity. It describes how to configure an experimental LPWAN system being built at the Department of Computer Science and Telecommunications at Poznan University of Technology for research related to smart buildings.**

***Keywords*—Long-Range (LoRa); Intelligent Building; LPWAN; wireless network; security communication; Smart City; IoT**

I. Introduction

THE Internet of Things and Wireless Sensor Networks (WSNs) are now a key part of our lives. All around us, we are able to see the utilization of IoT elements – including enhancing our quality of life, automating many processes, or reducing energy consumption - which to some extent allows us to reduce greenhouse gas emissions into the atmosphere. From the 2019 European Union (EU) research report, it can be seen that the energy sector emits the most greenhouse gases into the environment [1]. The data shown in Figure 1 are from before the pandemic when the economy functioned normally. The data from 2020 onwards are disrupted by a change in the style of society, where the vast majority did not move. The degree of greenhouse gas emissions in the EU is shown in Figure 1. According to a report by Ericsson, the use of IoT could potentially reduce CO_2 emissions by up to 63.5 gigatons by 2030 [2]. IoT and WSN are used in many areas of our lives, which are listed below.

Health care, where we can monitor our vital signs in real-time, around the clock, so we can react much faster to abnormalities in our bodies, but IoT is also used to monitor the elderly and people with chronic diseases, and people practicing various sports, also for health purposes.

Smart building and smart city - in these two sectors, IoT and WSN play a key role. They allow us to control, among other things: indoor microclimate, which is very important, since many of us work in buildings and during the Covid pandemic have become accustomed to working remotely and staying at home a significant amount of the time. They also allow you to control the state of air quality or the state of congestion on the roads.

Controlling energy consumption - IoT and WSN solutions allow us to control the energy used while consuming little energy. Many devices used for these solutions need a small power supply, which is very often battery-powered, and because these devices can go to sleep and turn on at specific moments, they can operate on battery power for many years. Additionally, by powering them with, e.g., solar energy, we extend their operation time.

Security - IoT solutions are very often used in intelligent monitoring systems. They allow for automatic detection of unwanted activities (e.g., vandalism, theft, robbery), automation (opening gates, barriers), control, and surveillance of persons (face detection registration of persons entering mass events - matches, concerts).

This is only a part of the most common examples of use. There are many more possibilities. Sensor networks are often placed in places where human intervention is not possible [3]. With each passing day, the number of IoT devices connected to the network continues to grow. By 2025, it is expected that more than 55 billion IoT devices will be connected to the Internet [4]. Most of them are placed in specific locations, which requires these devices to work for a long time on battery power. Therefore, minimizing power consumption is so important for IoT. It can be noted that mobile network operators are also trying to minimize energy consumption. An example is Orange, where, in 2015 the power consumption was 1.4 kWh for each 1 GB of data, while in 2019 it is already 0.2 kWh [5].

Our data collection devices mainly use wireless transmission, not only in IoT. Nowadays, everyone uses wireless communications intensively. With wireless communications, we can work and exchange information from anywhere in the world. Hence, it is necessary to have the best possible transmission for real-time monitoring and control of devices in Smart Home and Smart City. However, the communication itself is just the beginning. One very critical issue is the security of this transmission. The security of data exchanged between devices is an essential component of a properly functioning network system.

This work was supported from funds granted by the Ministry of Science and Higher Education under Task No. 0312/SBAD/8162.

Joanna Szewczyk and Piotr Remlein, are with Poznan University of Technology, Institute of Radiocommunications, Poland (e-mail: joanna.szewczyk@cs.put.poznan.pl; piotr.remlein@put.poznan.pl).

Mariusz Nowak and Aleksandra Głowacka are with Poznan University of Technology, Institute of Computing Science; Poland (e-mail: mariusz.nowak@cs.put.poznan.pl, aleksandra.glowacka@student.put.poznan.pl).

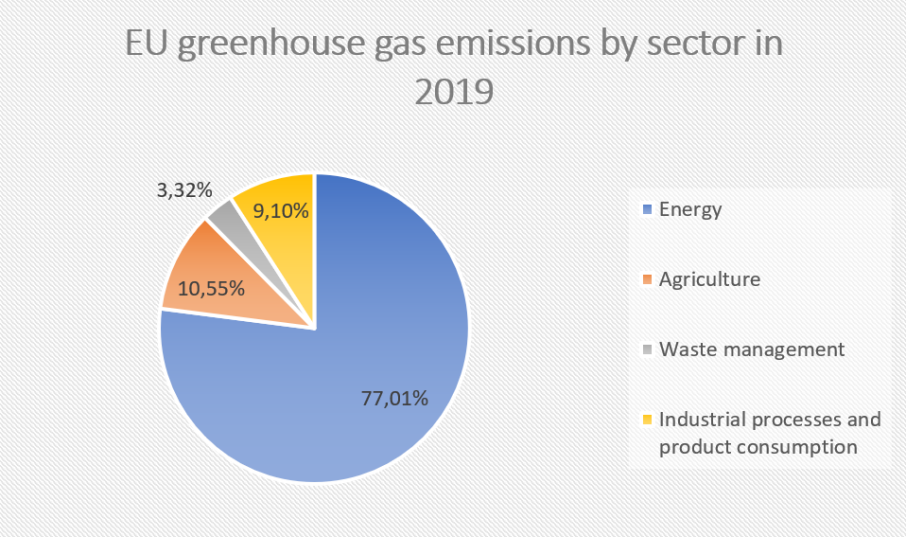

Fig. 1. Greenhouse gas emissions by sector in the European Union in 2019 [own work based on: [1]]

While for Smart Home communication the use of Wi-Fi, Zigbee, or BLE is also sufficient, in the case of Smart City, the utilization of those technologies may be costly. The aforementioned examples of wireless communications only work at short ranges. Therefore, using LPWANs - free, low-energy long-range networks - can be a good solution.

The purpose of this publication is to compare the most popular types of wireless communications used in smart buildings and smart cities, with the aim of presenting the advantages of LPWAN communications over other types of wireless communications, the security features of LPWAN communications, and comparing the advantages and disadvantages of current solutions that enable the implementation of solutions based on LoRaWAN communications. This is an introductory work for the authors, who plan in the next step to conduct research of the author's solutions, where algorithms will be implemented to optimize communication in terms of energy and in terms of increasing the security of communication.

The structure of the publication is as follows. The second chapter characterizes the most important types of wireless communication used in Smart Home and Smart City solutions and collects and compares the most important parameters of the described technologies. The next chapter presents the advantages and possibilities of using LPWAN in Smart solutions. The fourth chapter describes the difference between current network servers for LoRaWAN solutions. The fifth chapter describes the risks we may face when using LPWAN technology and presents current work on improving the security of LPWAN communications. Chapter six is a summary of the work.

II. Overview of Wireless Communications Used in Smart Solutions

Each of the edge devices used in IoT uses wireless communications. Depending on the needs, we can use different types of wireless communications to communicate with smart devices. Below is a brief description of some of the most popular wireless networks.

Wi-Fi

The Wi-Fi technology (IEEE 802.11 standard) is the most popular and widely used wireless network technology to communicate with the Internet. It is a good choice for Smart Home solutions, which allows users to monitor and reduce energy consumption and control many processes. Nowadays, every smart device (wearables, latest home appliances, consumer electronics) has a built-in Wi-Fi module, which allows for easy and fast communication with other devices that can collect and monitor data [6]. Wi-Fi technology is the most popular and currently the most developed for Smart solutions. Many sensors are adapted for specific solutions. In [7-11] the authors propose the use of Wi-Fi-based sensors in health monitoring. In [12-14] they provide proposals for tracking human activity, in [15-17] they provide proposals for tracking human gestures, while in [18, 19] we can learn about ways to track people and their activity through walls. In [20-22] there are examples of ways to control processes to increase security, and [23-25] presents ways to use Wi-Fi to control processes in a smart building.

Bluetooth Low Energy (BLE)

In 2010, the Bluetooth Low Energy (BLE) technology was introduced. It uses less power and is intended for nodes and applications that require lower data transfer speeds. It uses less power than standard Wi-Fi, resulting in a slower data transfer rate. Many new IoT gadgets have been introduced as a result of their low power consumption. This technology is suited for applications that necessitate the transmission of small amounts of data across short distances. Countless gadgets have been invented employing BLE technology to date, e.g., in medicine or home entertainment equipment [26, 27]. After Wi-Fi, BLE technology is the second most popular wireless communication technology. In [28-31] authors presented the use of BLE beacons for Smart solutions. In [32-35] presented the use of BLE technology for health monitoring, while the article [34] presents the use of both BLE and Wi-Fi for monitoring elderly people at home. In [36-38] the authors present the use of BLE

technology in building automation, whereas in [38] also present the use of both BLE and Wi-Fi for process control.

ZigBee

ZigBee is an open wireless networking standard based on IEEE 802.15, a technology with short range, low data rate, and low power consumption. ZigBee can build networks with a range of 10 to 100 meters. Decentralized networks, in which each node administers itself, can divert and connect to new nodes as needed. This makes ZigBee perfect for Smart Home applications, such as remote control of home automation and sensor measurement monitoring. This technique is sensitive to distortion and interference due to its low transmission power. Distortion caused by technologies such as Wi-Fi, USB, Bluetooth, and microwave ovens can adversely affect ZigBee's functioning in the 2.4 GHz range [26, [27], 39]. ZigBee technology also finds many applications in Smart solutions. In [40] authors present the design and implementation of a temperature and humidity monitoring system based on Zigbee and Wi-fi technology. In [41] The authors present an application of Zigbee and 4G communication for the monitoring of photovoltaic systems. In [42, 43] the authors propose Zigbee-based solutions for monitoring intelligent buildings. In [44] authors present a parking system based on Zigbee technology. In [45] the authors propose an intelligent garbage monitoring system. In [46] authors present a smart system based on Zigbee and LoRa technologies.

Z-Wave

In the realm of home automation, Z-Wave is another type of wireless technology that competes mostly with ZigBee and BLE. BLE and ZigBee share a 2.4 GHz bandwidth, whereas Z-Wave has a bandwidth of less than 1 GHz. The actual bandwidth differs by country, which can present issues if you wish to sell your items globally. Z-Wave operates at 908 MHz in the United States and 868 MHz in Europe.

Lower frequencies have two advantages: they have a greater range and less interference. Radio waves with lower frequencies go further. The 2.4 GHz spectrum used by BLE, and ZigBee is also used by Wi-Fi, Bluetooth Classic, and even microwaves, causing significant interference [47]. Smart systems based on Z-Wave networks are the least found when comparing with other technologies. In [48] the authors have developed their own Blackbox, which aims to increase safety in vehicles. This box is supposed to automatically inform the appropriate services about the accident. The entire project is based on Z-Wave technology. In [49] the authors analyzed a smart home control system based on wireless Z-Wave transmission to remotely control an electronic lock. In [50] the authors discussed the development and application of Z-Wave technology in smart homes.

Cellular networks

When a permanent connection is not necessary, a cellular connection in Smart solutions can be employed. This technology has the advantage of having been around for a long time, having broad coverage, being affordable in cost, and having great security. The disadvantage of mobile communication is that it requires sharing the network with a large number of other users, which might cause network congestion in some instances [51]. Cellular networks are also widely used in Smart systems. In [52] the authors proposed a smart solution for diabetes diagnosis and personalized treatment based on 5G networks, while in [53] the authors presented a way to recharge home spirometry tests using 5G smart devices. In [54, 55] the authors present the possibilities of using mobile networks in health care. In [56] authors described a solution to track the amount of e-waste generated. In [57] authors proposed a hybrid fog and cloud-based computing architecture for use in vehicle-to-grid (V2G) networks based on 5G technology. In [58] the authors present the impact of 5G technology on smart cities, and intelligent transportation systems, including vehicular communications, while in [59] authors presented research on 5G communication in Vehicle-to-everything (V2X). In [60] authors propose a network architecture for a high-speed rail system based on 5G technology.

LPWAN technologies

LPWAN is a long-range wireless network. It enables communication over very long distances while consuming low power. There are several LPWAN standards. The most popular ones are: LoRa/LoRaWAN, SigFox, and NB-IoT

LoRa/LoRaWAN

LoRaWAN is a Low Power Wide Area (LPWA) networking protocol used to wirelessly connect Internet of Things (IoT) devices in regional, national, or worldwide networks. The LoRa Alliance was responsible for its creation. The LoRaWAN network design is based on a star topology, with gateways forwarding communication between edge devices and end-users via a server (Fig. 2).

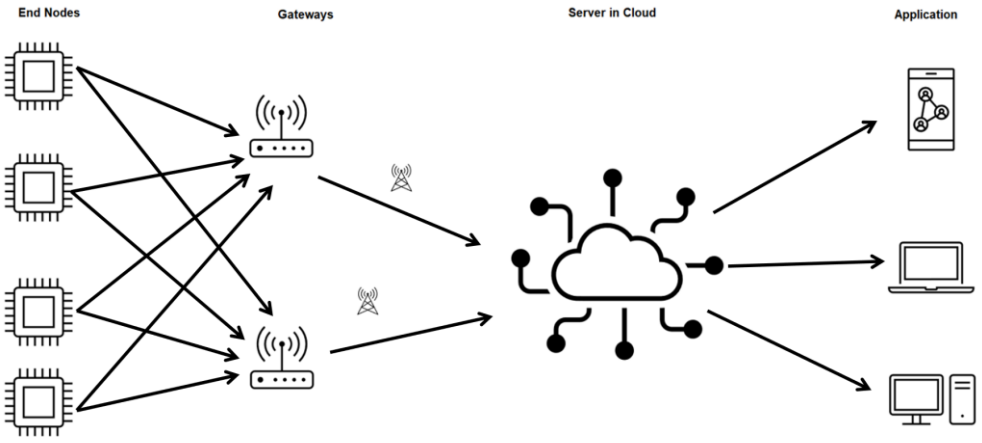

Fig. 2. LoRaWAN architecture [own work]

Wireless communications take advantage of the physical layer's long-range capabilities, allowing connections between edge devices and one or more gateways. The LoRaWAN protocol allows for bidirectional communication over vast distances (up to 20 km). CSS (Chirp Spread Spectrum) modulation is used. The data is transmitted in an unlicensed bandwidth at the following frequencies: 433 MHz in Asia, 868 MHz in Europe, and 915 MHz in the United States. The ability to transmit data over long distances makes it a useful solution for use in Smart City [61-64].

Sigfox

Sigfox is a low-power wide-area network (LPWAN) technology that uses Ultra Narrowband (UNB) modulation. To reduce interference, this modulation technique allows the receiver to listen to only a tiny area of the spectrum. In the United States, Sigfox runs at 902 MHz, while in Europe, it works at 868 MHz. Bidirectional communication is currently supported by Sigfox. Like LoRaWAN, the Sigfox network architecture is built on a star topology [63-65].

NB-IoT

NB-IoT, unlike LoRa/LoRaWAN, is a cellular technology. It is more expensive to implement, requires more power, and is more complicated to install. It does, however, provide a higher mobile connection quality and direct Internet access [66].

Table I summarizes and compares the key features of the LPWAN systems described, while Table II compares the selected features of wireless technologies used in Smart Home and Smart City.

TABLE I
LPWAN SYSTEMS COMPARISON TABLE [66-70]

	LoRa/LoRaWAN	**Sigfox**	**NB-IoT**
Frequency (frequency bands)	863–870 MHz (unlicensed)	863–870 MHz (unlicensed)	GSM 900 MHz, LTE 800 MHz (licensed)
Bandwidth	0.3–11 kbps <50 kbps (FSK)	UL: 100 bps DL: 600 bps	20-250 bps
Max message per day	Unlimited	140 Up, 4 Down	Unlimited
Range	5–20 km	10–40 km	2–35 km
Confidentiality	AES128	Default: None Optional: AES128	LTE
Encryption	Yes	No	Yes
Battery life	10 years	10–20 years	10 years

TABLE II
COMPARISON OF THE ABOVE DESCRIBED WIRELESS TECHNOLOGIES [54, 78]

Technology	**Distance**	**Bitrate**	**Energy consumption**	**Use of**
WiFi	20–100 m	2 Mbps–1.7 Gbps	High	SCADA, smart devices, Smart Home
Bluetooth/ BLE	8–10 m	1–24 Mbps	Bluetooth: Medium BLE: Very low	smart devices, Smart Home
ZigBee	10–100 m	20–250 Kbps	Very low	Smart Home
Z-Wave	30 m	9–40 kbps	Very low	Wireless mesh network
LPWAN	<50 km	0,3-50 Kbps	Very low	Smart Home and Smart City technologies

III. WHY LPWAN COMMUNICATION IN SMART HOME/CITY?

LPWAN is a wireless technology that has been specifically designed for Smart solutions. It allows for a long communication range (up to 50 km, depending on the de-vice), can communicate with a large number of devices, and ensures low power consumption and low operating costs. Thanks to these advantages, LPWAN is growing in popularity and use every year. LPWAN is very well-suited for small data transmissions, such as sensor data, over long distances, which is competitive with other wire-less technologies [79].

Figure 3 presents a plot of the relationship between bandwidth and power consumption and data transmission range for selected wireless networks used in Smart Home and Smart City.

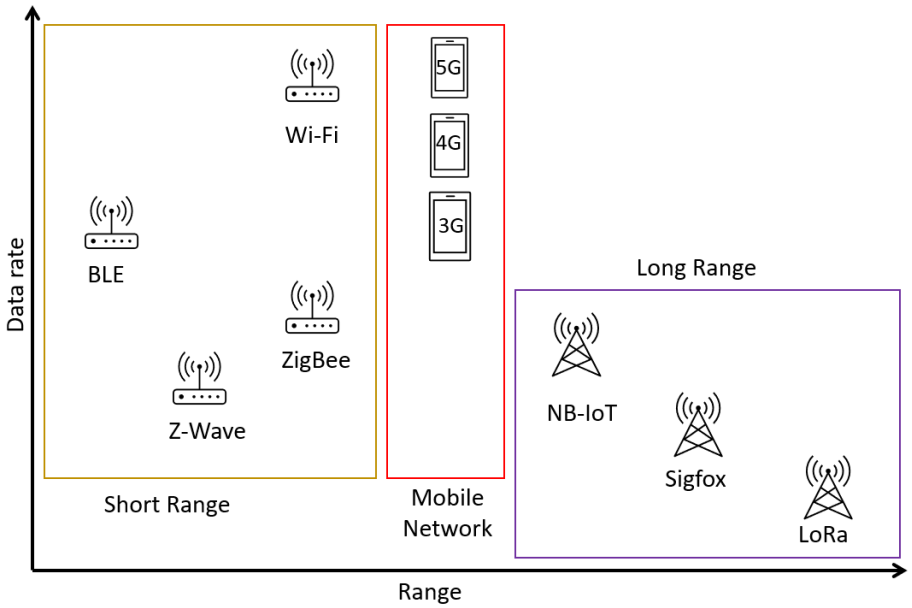

Fig. 3. Bandwidth-to-range ratio in selected types of wireless communications [own work based on: [79, 97]]

A. *Benefits of LPWAN on the example of LoRa/LoRaWAN technology*

Long range - LoRaWAN gateways can transmit and receive signals over many kilometers.
Low operating costs - by using the unlicensed ISM band, LPWAN technology is in-expensive because one does not have to pay large license fees for a particular frequency. The ISM band is a radio band whose original purpose was for industrial, scientific, and medical use [80]. Besides, nowadays, buying edge devices that will communicate and collect data is also inexpensive. For private solutions, cloud solution owners provide data collection and visualization capabilities for free.
High bandwidth - Web servers can accept millions of messages from multiple gateways.

Easy to implement - Implementing a LoRa-based connection is not that difficult at all. Currently, there are ready-made cloud solutions that easily communicate with gateways [63, 67, 81]. Until now, the biggest platform was TTN (The Things Network) [82], which has recently expanded to TTS (The Things Stack) [83, 84] platform. In addition to TTS, the Thing speak platform [84], open-stack [85], chirps tack [86], and thethings.io [87] allow data collection through LoRa communication. Besides, Arduino IoT Cloud integrates with TTS to be able to easily collect measurement data from dedicated Arduino devices for communication through LoRa [88].
Bi-directional communication - It allows not only for sending data from edge devices to the gateway but also the devices can receive messages. This can be useful in communication in sensor networks - we can not only send collected data to the server but also from the server level send messages to sensors, e.g., with firmware updates [61].
Low power consumption - LPWAN terminal devices are configured to operate in low-power mode for many years (up to 10 years) on a single battery. The low-power nature of this communication is influenced by, among other things, adaptive data rate setting and the selection of one of three classes of terminal devices. Adaptive Data Rate (ADR) is a mechanism used in LoRaWAN networks to optimize the transmission rate, which also affects the energy consumption of the network [63, 67, 81, 83, 89].

Class A: this class distinguishes end devices with the lowest power consumption. It is the default class supported by all end devices. Communication is bi-directional and asynchronous. Transmission on the uplink can be sent at any time and is immediately followed by two short windows on the downlink, allowing for bidirectional communication and control commands. In Class A, end devices can enter sleep mode for a specified period. This just makes Class A the lowest power consumption mode of operation, while still being able to communicate in the uplink at any time. However, the fact that the downlink here always follows the uplink, means that downlink communication must wait until the uplink occurs, which can cause delays [61, 92]. Figure 4 shows how packets are transmitted in class A.

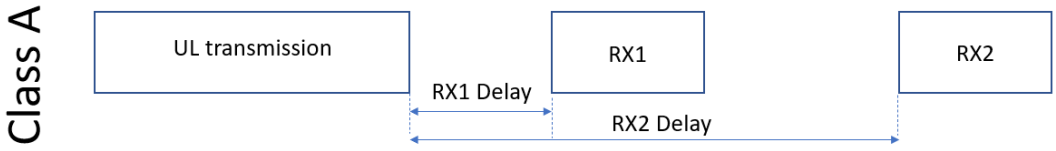

Fig. 4. Devices classes - Class A [own work based on: [82, 90, 91]]

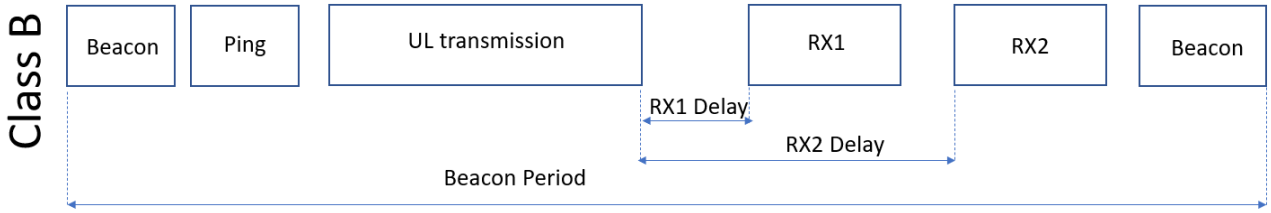

Fig. 5. Devices classes - Class B [own work based on: [82, 90, 91]]

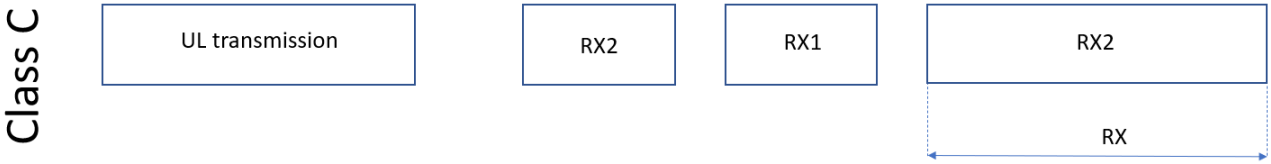

Fig. 6. Devices classes - Class C [own work based on: [82, 90, 91]]

Class B: in this class, downlink access for end devices is allocated deterministically - devices in this class perform synchronized communication in allocated slots at specified times. This reduces the latency of downlink messages, except that it increases our energy consumption. Nevertheless, the power consumption is low enough to run on battery-powered devices [61, 92]. Figure 5 shows how packets are transmitted in class B.

Class C: in this class, the least transmission delay is provided, as the receiver of the end device is constantly open, even when the devices are not transmitting. However, this comes at the cost of higher power consumption. In this class, the end devices need a steady power supply [61, 92]. Figure 6 shows how packets are transmitted in class C.

B. Opportunities for use

The LPWANs technology can be used in many Smart Home and Smart City measuring systems. In [62] the authors present a simple, practical use of sensor networks communicating in LoRa to collect measurement data and analyze room microclimate.

In [67] the authors proposed a system using LoRaWAN to communicate with electricity meters and monitor the power supply network in buildings.

In [71] author shows that LPWAN networks can be a good solution for metering systems and remote-control systems in water and wastewater management. The use of Lora technology in such systems allows for the non-invasive installation of measurement systems, as there is no need to run wires, but everything works on battery power or from renewable energy sources.

In [72] author presented the possibility of using a prototype solution based on the RFM95x module communicating in LoRaWan standard for an energy storage system based on thermoelectric generators (TEG).

In [73] authors described a novel animal tracking system powered solely by thermal energy. The tracked data was sent by the authors to The Things Network, a platform dedicated to LoRaWAN.

In [74] authors proposed to use of LoRaWAN technology for communication between electric vehicles The authors' research shows that LPWAN technology is capable of handling a large amount of information, and one LoRa base station is capable of supporting up to 438 electric vehicles per cell and 1408 vehicle charging points.

In [75] authors proposed a solution for drone control and communication in LPWAN for city monitoring. Using LPWAN for drones may be a good solution considering that drones operate on battery power and need to minimize power consumption where possible.

In [76] authors present a solution based on the LoRaWAN standard for precision irrigation in tomato cultivation for the fresh market. The authors designed and tested four irrigation scheduling methods. The results obtained by the authors show that such a system can be used for precise and automatic irrigation of horticultural crops. It allows for minimizing both energy and water consumption.

In [77] authors presented a hybrid body-worn sensor network system for IoT-related safety and health monitoring applications. The purpose of the system developed by the authors of the paper is to improve safety in the outdoor workplace. The communication of this system is based on LPWAN and wearable body area network (WBAN). The sensors in the WBAN are used to measure the environmental conditions around the subject and to monitor the subject's vital signs.

C. Popularity of LPWAN

From the maps provided by the TTN platform, you can see that Europe is currently the one with the most LPWAN technology in use (Fig. 7). TTN Mapper is a tool that collects the actual location data of registered gateways on TTN/TTS, Helium, and ChirpStack platforms [94].

In Europe alone, the Netherlands and the United Kingdom lead the way in the use of the LPWAN technology (Fig. 8). Unsurprisingly, Amsterdam is a world leader in implementing low-energy IoT solutions, creating a green Smart City to make life easier for residents and protect the environment [95].

Legend to maps:

- green - small number of devices,
- yellow - medium number of devices,
- orange - medium number of devices,
- red - high number of devices.

Figure 8 shows the section of Europe with the highest concentration of gates. The area with few or no gates has been omitted.

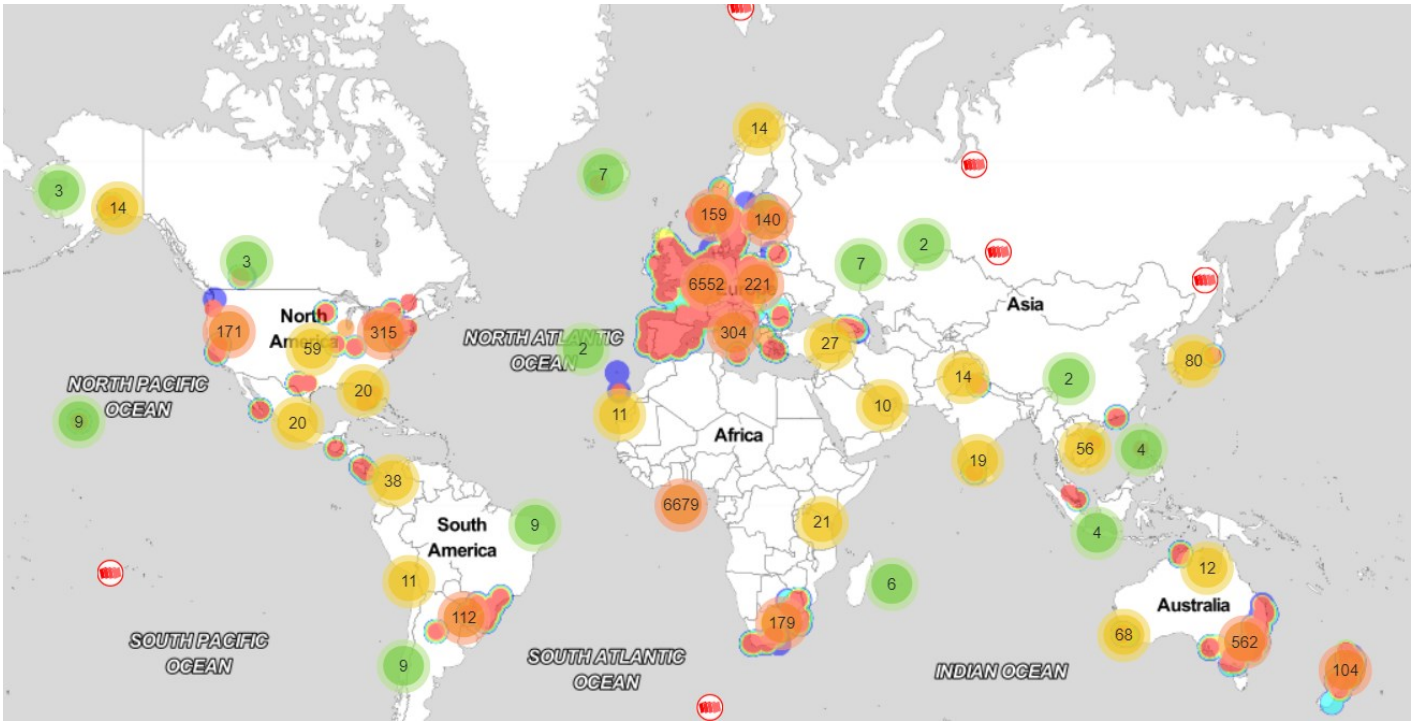

Fig. 7. Distribution of LPWAN gateways in the world [94].

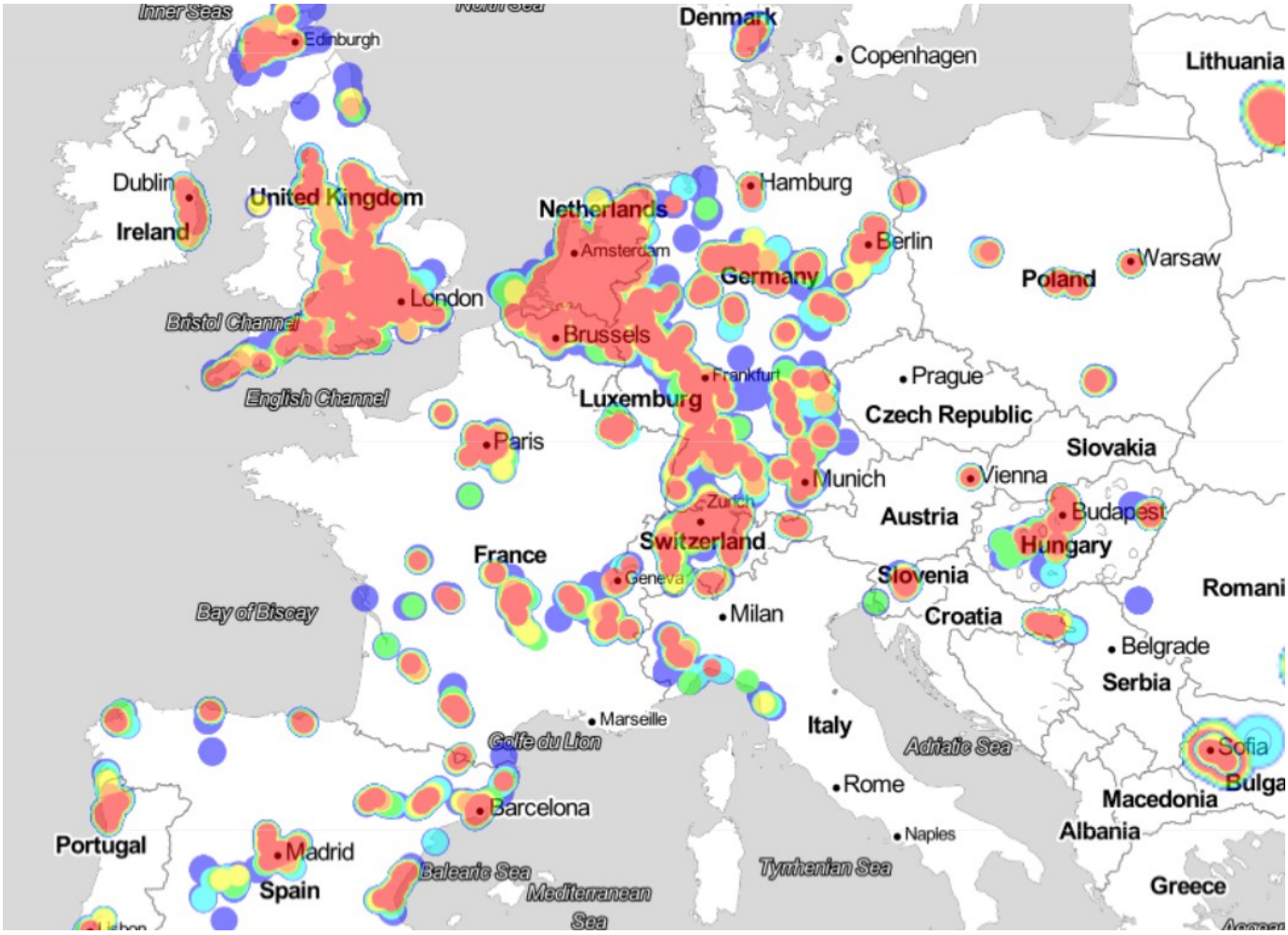

Fig. 8. Distribution of LPWAN gateways in Europe [94].

IV. NETWORK SERVERS FOR LORAWAN SOLUTIONS

In this chapter, a selection of the most popular cloud solutions is characterized, allowing the implementation of proprietary solutions, using communication in LPWAN networks, as well as platforms that allow processing and analysis of data collected on network servers.

LoRaWAN is one of the protocols of LPWANs - low-energy long-range networks. The LoRaWAN standard allows two-way communication in the unlicensed ISM band, at 868 MHz (for Europe). As a result, the use of LoRa-WAN wireless technology is becoming increasingly popular in solutions for IoT and sensor networks [61, 63, 67].

TTN (TTS).

The Things Network service migrated to The Things Stack Community Edition in 2021. The Things Stack is a LoRaWAN network server that enables the design of various deployment scenarios, supports all existing LoRaWAN versions (including the latest 1.1), all A, B and C modes of operation, and all regional parameters issued by the LoRa Alliance. TTS allows users to run their own server and use dedicated solutions or web applications. These capabilities make TTS a very good solution for beginners as well as experienced users.

Originally, the implementation of proprietary solutions on the TTN platform allowed an average of one device to transmit uplink messages every 30 seconds, per 24 hours, and up to ten messages in downlink transmissions, per 24 hours. The process of migrating The Things Networks service to The Thing Stack, meant that the possible number of transmittable messages in a downlink increased. In the TTN service, it was possible to send 10 messages in downlink transmission per day, while the TTS service allows 10,000 downlink messages in 24 go-hours [82-83].

Chirpstack

Chirpstack is an open-source platform that provides functionality for LoRaWAN networks. It requires running a server on a so-called gateway, where you can then use a local version of the interface to manage your devices. The running ser- vice also allows integration with platforms for data analysis and visualization. The Chirp-stack solution allows commercial use of its functionalities and has support for devices of all classes in the LoRaWAN standard and supports all versions of LoRa [85].

Openstack

Openstack is a cloud server that allows the deployment of proprietary solutions in the IoT area using LoRaWAN standard communication [86].

Thethings.io

Another platform used in LoRa is Thethings.io. It has a simple API (Ap-plication Programming Interface) that allows users to implement proprietary solutions. The Thethings.io platform also allows integration with TTS via HTTPS and MQTT protocols [87].

Based on the analysis of the parameters summarized in Table II, it is reasonable to choose the TTN (TTS) platform.

The presented platforms, in addition to LoRaWAN communication, allow easy integration with popular platforms for data processing, analysis and visualization, such as Thingspeack, Arduino IoT Cloud, AWS IoT, Azure IoT Hub, Google Cloud and Node-Red.

TABLE III
CHARACTERISTICS OF PLATFORMS USED WITH LORA. SOURCE: [82, 97]

	TTN (TTS)	**Chirpstack**	**Open-Stack**	**Thethings.io**
Ease of implementing custom solutions	Easy configuration. Huge community using this platform, making it easy to find help. Open source code.	Moderately advanced configuration. Requires the ability to work with scripts.	The need for specialized skills and knowledge.	Intermediate configuration.
Cost	Free for personal use. For commercial use: €190 / $230 per month.	Free for private and commercial use.	Cost calculated based on a combination of service level and infrastructure.	Fee depends on the number of devices and maintenance of the platform. Free trial for 15 days.
Supported protocols	TCP/IP, UDP, DHCP, MQTT, HTTP, Websockets, AMQP, gRPC	MQTT, HTTP, DHCP, Protobuf Websockets, AMQP, gRPC	TCP/IP, UDP, ICMP, DHCP, ARP	MQTT, HTTP, Websockets, CoAP

A. System description

At the Department of Computer Science and Telecommunications, Poznan University of Technology, an experimental system has been implemented to conduct research on the degree of complexity of the selected network server, dedicated to solutions benefiting from communication in the LoRaWAN standard.

Equipment and technologies used

The implementation of the system under study used a LoRa gateway - Lorank 8, the specification of which is shown in Table IV, Arduino Uno Rev 3 platform and RFM95W transmitter (transmitter specification in Table V). The Arduino platform together with the transmitter is responsible for sending test messages to the TTS service.

The RFM95W transmitter is equipped with a LoRa module, which enables long-range communication with high immunity to interference and low power consumption.

To implement the connection of the end device to the TTS via a LoRa gateway, the LMiC library (loRaMAC in C) was used, which can be found on the github platform [101].
Figure 2 shows the location of the eperimental system, which is located in the CWiBT (Lecture Center and Technical Library) building of Poznan University of Technology, at Piotrowo Street 2. The project uses one gateway and one terminal device. Ultimately, the experimental set will consist of about 10 terminal devices with sensors to control the microclimate in the rooms of the said building.

Table IV
Parameters of the gate used [88]

Frequency bandwidth	868 MHz
Sensitivity	-138 dBm
Maximum power	+27 dBm (500mW)
LoRa demodulators	49
Parallel channels	8
Max nodes connected	~60 thousand (assuming that nodes send data once an hour. In other cases, the number of nodes that can handle about 10-20 thousand)
Processor	1GHz, ARM Cortex A8
OS	Debian / Angstrom Linux
Wi-Fi	Optional (via USB)
Current intensity	1A
Max USB current	500mA
AC adapter	5VDC, 2A

Table V
Key parameters of the RFN95W transmitter 0

Maximum link budget	168 dB
Modulation	FSK, GFSK, MSK, GMSK, LoRa™ i OOK
Programmable bit rate	up to 300 kbps
Immunity to interference	IIP3 = -12,5 dBm
High sensitivity	-148 dBm
Built-in sensors	Temperature sensor and low battery indicator
Constant RF (radio frequency) output power depending on supply voltage	+20 dBm - 100 mW
Power amplifier efficiency	+14 dBm
Low RX current (measured resistance)	10,3 mA

Figure 9 shows a schematic of the Arduino Uno R3 platform with the RFM95W transmitter and Fig. 10 shows the location of the test site.

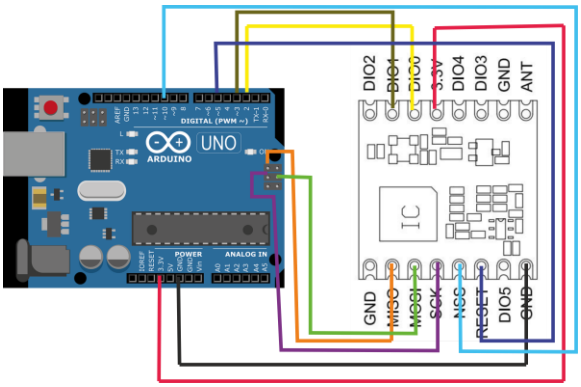

Fig. 9. Schematic of the Arduino's connection to the RFM95W. Source: own elaboration based on: [89]

We start the configuration on the web server by adding a gateway. In order to add a gateway to the TTS network, you need to download the gateway's ID information - Gateway ID. The key part of configuring the gateway's connection to the web server, is to download the global_conf.json file (Fig. 11).

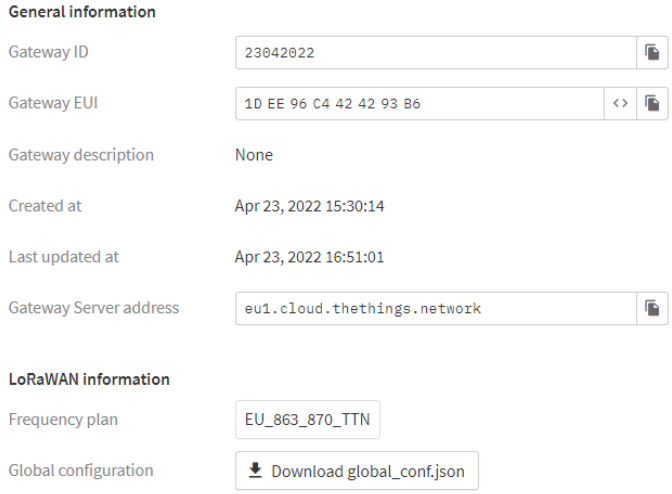

Fig. 11. Gateway configuration data on the TTS platform. Source: the screenshot is from the administration panel on the TTS platform

In the case of the gateway used in the project, there was a problem with differentiating the size of the signifiers for the Gateway ID. It was necessary to change the Gateway ID parameter in the local_conf.json file. The second problem was that the gateway's system clock was out of sync with the server's clock. The solution to this problem was to install the NTP (Network Time Protocol) package.
After adding a gateway in the service, you need to define the end device. To do this, first add an application in the service and in the created application add the configured devices. You can add them from the LoRaWAN repository or enter the configuration data manually (Fig. 12).

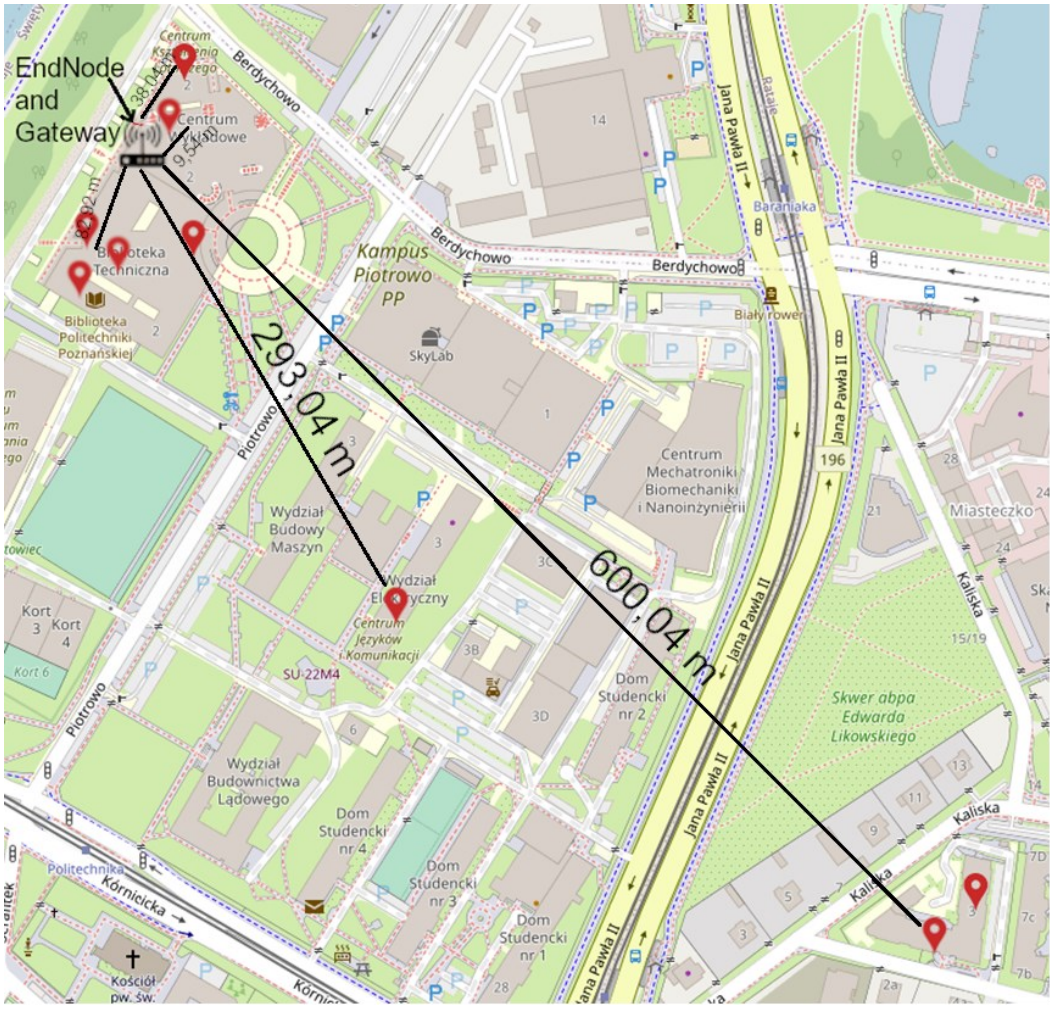

Fig. 10. Location of the experimental set. Source: own work.

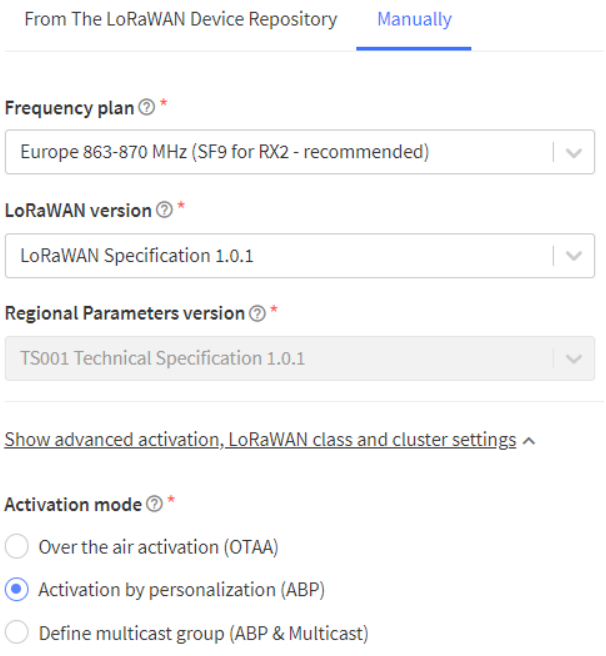

Fig. 12. Configuration data when defining an end device on the TTS platform. Source: screenshot is from the TTS platform administration panel

When adding devices, select the activation method. By default, the OTAA way is selected, which is recommended and better than ABP, since session keys are assigned dynamically and change with each new session. However, the ABP activation method allows for better control over the device, so this method was selected during the prototyping stage [102].

V. Communication Security in LPWAN Networks

Although LPWAN technology is very attractive for IoT solutions, it poses the threat of attacks. Despite LoRaWAN's security features, LoRa devices are subject to security assaults. LoRa modulation, for example, requires 900 milliseconds to 1.2 seconds for each LoRa broadcast. Attackers have a lot of options with such a large trans-mission window [103].

LPWAN security remains a serious challenge because the end devices in the network have limited resources (computing memory, battery), so the use of state-of-the-art cryptographic algorithms with high computing power is not possible. LPWAN technologies use the AES128 symmetric encryption method, which generates two keys for message encryption and decryption using Appkey. However, despite encryption and decryption, the message is always of the same length, which can make it easy for an attacker to decrypt the key. Despite this mechanism, LPWAN devices are vulnerable to jamming attacks, device, and network key compromise, and replay at-

tacks. Radio modules connected with the microcontroller also do not provide support for cryptographic algorithms, which causes problems in recognizing whether commands are sent by the microcontroller or the attacker [63, 69, 104].

Jamming The jamming attack technique is a popular problem when IoT solutions are deployed. It is characterized by transmitting a strong radio signal in the proximity of measurement devices to interfere with transmissions. In [103], it is shown that it is possible to jam LoRa devices using LoRa. More precisely, simultaneous LoRa transmissions on the same frequency can interfere with each other. An Arduino runtime platform with a LoRa radio module is sufficient to perform this attack. This research shows that it is an easy and inexpensive way to interfere with and harm LoRa transmissions.

In addition to message encryption, it is important to choose how to activate the end devices used in the deployed connection. We distinguish between OTAA (Over-The-Air-Activation) and ABP (Activation By Personalization). The OTAA method is recommended and is more secure than the ABP method because, in the OTAA method, session keys are assigned dynamically and change with each session. On the other hand, the advantage of the ABP method is better to control of the device primarily at the prototyping stage. The ABP way makes the end device connected to one selected network all the time until we manually change it. In addition, the ABP method is less secure than OTAA [82].

In LoRaWAN networks, there is one more feature that is an advantage on the one hand and a disadvantage on the other. LoRaWAN networks have ADR (Adaptive Data Rate). ADR adjusts the SF and baud rate according to the distance between the end de-vices and the gateway. This makes the end devices that are closer to the gateway can get faster data transmission than those that are far away. However, this makes the devices that are farther away take longer to complete the transmission, which gives a potential attacker more time to launch an attack [27, 105].

The authors of [104] performed security research on recent attack vectors on IoT applications leveraging LPWANs. The findings revealed that LPWAN communication methods have security flaws that can cause irrevocable damage to IoT applications. The authors were able to identify the most relevant sorts of assaults, post-dates, risks, and possible responses with regard toto about LPWAN technology through their research. Some of these assaults have been identified separately, along with extensive descriptions of how they are employed and carried out. After determining the key points of the severity of discovered threats, they conducted research to uncover potential ways to defend, mitigate, or even eradicate these security flaws.

The authors of [66] analyzed the security mechanisms and vulnerabilities of LPWANs (for the LoRa, Sigfox, NB-IoT, and DASH7 standards), presenting that each solution has advantages and downsides for IoT solutions. It was demonstrated that, despite security protections, LoRa devices are vulnerable to a variety of assaults.

In [106], the authors pointed out that the security of packet transmission is affected by the spreading factor - the smaller the factor, the longer the transmission time over the air. This makes our packets vulnerable, especially at the physical layer and the link layer. This leads to the fact that it is not possible to have one fixed set of rules, because everyone has a different level of vulnerability. The authors also conducted an analysis of analyzed current security approaches and found that some of them may not be effective, hence the need for secure communication arises. They proposed the use of Machine Learning with reinforcement.

In [69], the authors described existing security solutions in LPWANs, identified vulnerabilities that need to be addressed, and compared security with other types of wireless communication. The authors also presented the possibility of using Soft-ware-Defined Networking (SDN) in LPWAN security for IoT solutions, and the challenges associated with SDN implementation.

In [107], the authors proposed the use of PHYSEC-based key management, which is based on physical layer security in LoRaWAN. The authors' research showed that it can be a good solution to current key management solutions, while having low energy consumption cost costs when compared to other key management methods.

VI. Conclusions

This article presents an overview on wireless networks used in Smart Buildings and Smart Cities, especially LPWANs, and an analysis of network servers for LoRaWAN communications and how to configure the built experimental system on a selected network server, using readily available and inexpensive hardware and open-source software. The experimental system will be expanded in the future and used for research in the field of Intelligent Buildings and in the field of LPWAN communication security.

The use of LPWANs is becoming increasingly desirable due to the low-power nature of this communication. This allows us to reduce greenhouse gas emissions to some extent and make our devices and operations greener. However, an important aspect is the security of communications. The number of IoT devices using LPWAN communications is growing and expanding every day, which makes the transmitted data attractive to malicious attackers. Therefore, it is important to strengthen this communication. Despite its advantages, LPWAN communication has security issues. This creates a need for further research and new solutions to enhance the security of LPWAN communications. The authors' next step will be to practically test current LPWAN security solutions and propose an author's way to secure this communication.

Abbreviations

ABP	Activation By Personalization
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
BLE	Bluetooth Low-Energy
CSS	Chirp Spread Spectrum
DL	Downlink
EU	European Union
GB	Gigabytes
Gbps	Gigabytes Per Second
LoRa	Long-Range
LoRaWAN	Long-Range Wide-Area Network
LPWAN	Low-Power Wide-Area Network
IoT	Internet of Things
ISM	Industrial, Scientific, Medical
Kbps	Kilobytes Per Second
kbps	Kilobits Per Second

km	Kilometers
kWh	Kilowatt hour
LTE	Long Term Evolution
Mbps	Megabytes Per Second
MHz	Megahertz
NB-IoT	Narrowband Internet of Things
OTAA	Over-The-Air-Activation
SDN	Software-Defined Networking
SF	Spreading Factor
TTN	The Things Network
TTS	The ThingStack
UNB	Ultra NarrowBand
UL	Uplink
V2G	Vehicle-to-grid
V2X	Vehicle-to-everything
Wi-Fi	Wireless Fidelity
WNS	Wireless Sensor Network

REFERENCES

[1] Greenhouse gas emissions in the European Union. Available online: https://www.europarl.europa.eu/ news/pl/headlines/priorities/zmiana-klimatu/ 20180301STO98928/infografika-emisje-gazow-cieplarnianych-w-unii-europejskiej (accessed on 10.10.2022).

[2] ICT's potential to reduce greenhouse gas emissions in 2030. Available online: https://www.ericsson.com /en/reports-and-papers/ research-papers/exploring-the-effects-of-ict-solutions-on-ghg-emissions-in-2030 (accessed on 10.10.2022).

[3] Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors 2022, 22, 2087. https://doi.org/10.3390/s22062087

[4] Future of Industry Ecosystems: Shared Data and Insights. Available online: https://blogs.idc.com/2021/ 01/06/future-of-industry-ecosystems-shared-data-and-insights/ (accessed on 10.10.2022).

[5] Energy minimization in mobile networks. Orange report. https://biuroprasowe.orange.pl/blog/siec-komorkowa-moze-byc-bardziej-energooszczedna-w-orange-polska-zuzywany-duzo-mnie-pradu-w-przeliczeniu-na-przeslany-gigabajt/ (accessed on 10.10.2022).

[6] F. U. Khan, M. Awais, M. B. Rasheed, B. Masood and Y. Ghadi, "A Comparison of Wireless Standards in IoT for Indoor Lo-calization Using LoPy," in IEEE Access, vol. 9, pp. 65925-65933, 2021, https://doi.org/10.1109/ACCESS.2021.3076371

[7] Xiang Li, Daqing Zhang, Jie Xiong, Yue Zhang, Shengjie Li, Yasha Wang, and Hong Mei. 2018. Training-Free Human Vitality Monitoring Using Commodity Wi-Fi Devices. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 3, Article 121 (Sep-tember 2018), 25 pages. https://doi.org/10.1145/3264931

[8] Wang Y., Wu K., Ni L.M.: 'WiFall: device-free fall detection by wireless networks', IEEE Trans. Mob. Comput., 2017, 16, (2), pp. 581 –594

[9] Wang X., Yang C., Mao S.: 'TensorBeat: tensor decomposition for monitoring multi-person breathing beats with commodity WiFi', arXiv:1702.02046, 2017

[10] Yigitler H., Kaltiokallio O. J., Hostettler R. et al.: 'RSS models for respiration rate monitoring', IEEE Trans. Mob. Comput., 2019, Early Access

[11] Zhang F., Zhang D., Xiong J. et al.: 'From Fresnel diffraction model to fine-grained human respiration sensing with commodity Wi-Fi devices'. Proc. ACM Interactive, Mobile, Wearable and Ubiquitous Technology, Singapore, Singapore, 2018

[12] Kun Qian, Chenshu Wu, Yi Zhang, Guidong Zhang, Zheng Yang, and Yunhao Liu. 2018. Widar2.0: Passive Human Tracking with a Single Wi-Fi Link. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '18). Association for Computing Machinery, New York, NY, USA, 350–361. https://doi.org/10.1145/3210240.3210314

[13] H. Li, K. Ota, M. Dong and M. Guo, "Learning Human Activities through Wi-Fi Channel State Information with Multiple Access Points," in IEEE Communications Magazine, vol. 56, no. 5, pp. 124-129, May 2018, https://doi.org/10.1109/MCOM.2018.1700083

[14] M. Soni, A. Jain and T. Patel, "Human Movement Identification Using Wi-Fi Signals," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 422-427, https://doi.org/10.1109/ICICT43934.2018.9034451

[15] Hasmath Farhana Thariq Ahmed, Hafisoh Ahmad, Aravind C.V., Device free human gesture recognition using Wi-Fi CSI: A survey, Engineering Applications of Artificial Intelligence, Volume 87, 2020, 103281, ISSN 0952-1976, https://doi.org/10.1016/j.engappai.2019.103281

[16] Venkatnarayan R.H., Page G., Shahzad M.: 'Multi-user gesture recognition using Wi-Fi'. Proc. 16th Annual Int. Conf. on Mobile Systems, Applications, and Services, Munich Germany, June 2018, pp. 401 –413

[17] Haseeb M.A., Parasuraman R.: 'Wisture: touch-less hand gesture classification in unmodified smartphones using Wi-Fi signals', IEEE Sens. J., 2019, 19, (1), pp. 257 –267

[18] Xu Q., Chen Y., Wang B. et al.: 'TRIEDS: wireless events detection through the wall', IEEE Internet Things J., 2017, 4, pp. 723 –735

[19] Wu X., Chu Z., Yang P. et al.: 'TW-See: human activity recognition through the wall with commodity Wi-Fi devices', IEEE Trans. Veh. Technol., 2019, 68, (1), pp. 306 –319

[20] M. Sikandar, H. Khiyal, A. Khan and E. Shehzadi, SMS Based Wireless Home Appliance Control System (HACS) for Auto-mating Appliances and Security Preliminaries Home Appliance Control System (HACS), vol. 6, 2009.

[21] Depatla S., Muralidharan A., Mostofi Y., 'Occupancy estimation using only WiFi power measurements', IEEE J. Sel. Areas Commun., 2015, 33, (7), pp. 1381 –1393

[22] Zheng X., Wang J., Shangguan L. et al.: 'Design and implementation of a CSI-based ubiquitous smoking detection system', IEEE/ACM Trans. Netw., 2017, 25, (6), pp. 3781 –3793

[23] J. Bhatt and H. K. Verma, "Design and Development of Wired Building Automation Systems", Energy Build., vol. 103, pp. 396-413, 2015.

[24] Maternaghan et al., "Home automation system using a wireless network", IEEE Transactions on Consumer Electronics, vol. 44, no. 4, pp. 153-171, 2014.

[25] S. Jakovljev, M. Subotic and I. Papp, "Realisation of a Smart Plug device based on Wi-Fi technology for use in home automation systems", 2017 IEEE Int. Conf. Consum. Electron. ICCE 2017, pp. 327-328, 2017.

[26] Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the Energy Sector. Energies 2020, 13, 494. https://doi.org/10.3390/en13020494

[27] Zanaj, E.; Caso, G.; De Nardis, L.; Mohammadpour, A.; Alay, Ö.; Di Benedetto, M.-G. Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey. Technologies 2021, 9, 22. https://doi.org/10.3390/technologies9010022

[28] K. E. Jeon, J. She, P. Soonsawad and P. C. Ng, "BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 811-828, April 2018, https://doi.org/10.1109/JIOT.2017.2788449

[29] P. Spachos and K. N. Plataniotis, "BLE Beacons for Indoor Positioning at an Interactive IoT-Based Smart Museum," in IEEE Systems Journal, vol. 14, no. 3, pp. 3483-3493, Sept. 2020, https://doi.org/10.1109/JSYST.2020.2969088

[30] P. Spachos and K. Plataniotis, "BLE Beacons in the Smart City: Applications, Challenges, and Research Opportunities," in IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 14-18, March 2020, https://doi.org/10.1109/IOTM.0001.1900073

[31] Ke, C.; Wu, M.; Chan, Y.; Lu, K. Developing a BLE Beacon-Based Location System Using Location Fingerprint Positioning for Smart Home Power Management. Energies 2018, 11, 3464. https://doi.org/10.3390/en11123464

[32] Alfian, G.; Syafrudin, M.; Ijaz, M.F.; Syaekhoni, M.A.; Fitriyani, N.L.; Rhee, J. A Personalized Healthcare Monitoring System for Diabetic Patients by Utilizing BLE-Based Sensors and Real-Time Data Processing. Sensors 2018, 18, 2183. https://doi.org/10.3390/s18072183

[33] Hasan, M.K.; Shahjalal, M.; Chowdhury, M.Z.; Jang, Y.M. Real-Time Healthcare Data Transmission for Remote Patient Monitoring in Patch-Based Hybrid OCC/BLE Networks. Sensors 2019, 19, 1208. https://doi.org/10.3390/s19051208

[34] Montoliu, R.; Sansano, E.; Gascó, A.; Belmonte, O.; Caballer, A. Indoor Positioning for Monitoring Older Adults at Home: Wi-Fi and BLE Technologies in Real Scenarios. Electronics 2020, 9, 728. https://doi.org/10.3390/electronics9050728

[35] Chaari Fourati, L., Said, S. (2020). Remote Health Monitoring Systems Based on Bluetooth Low Energy (BLE) Communication Systems. In: Jmaiel, M., Mokhtari, M., Abdulrazak, B., Aloulou, H., Kallel, S. (eds) The Impact of Digital Technologies on Public Health in Developed and Developing Countries. ICOST 2020. Lecture Notes in Computer Science(), vol 12157. Springer, Cham. https://doi.org/10.1007/978-3-030-51517-1_4

[36] S. Das, S. Ganguly, S. Ghosh, R. Sarker and D. Sengupta, A Bluetooth Based Sophisticated Home Automation System Using Smartphone, pp. 236-240, 2016.

[37] M. Asadullah and K. Ullah, "Smart home automation system using Bluetooth technology", ICIEECT 2017 - Int. Conf. Innov. Electr. Eng. Comput. Technol. 2017 Proc., 2017.

[38] K. Khanchuea and R. Siripokarpirom, "A Multi-Protocol IoT Gateway and WiFi/BLE Sensor Nodes for Smart Home and Building Automation: Design and Implementation," 2019 10th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES), 2019, pp. 1-6, https://doi.org/10.1109/ICTEmSys.2019.8695968

[39] Chellappa, M., Madasamy, S., Prabakaran, R. (2011). Study on ZigBee technology. 297-301. https://doi.org/10.1109/ICECTECH.2011.5942102

[40] Jie Xiao, Jing Tao Li, Design and Implementation of Intelligent Temperature and Humidity Monitoring System Based on ZigBee and WiFi, Procedia Computer Science, Volume 166, 2020, Pages 419-422, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.02.072

[41] K. Xia, J. Ni, Y. Ye, P. Xu and Y. Wang, "A real-time monitoring system based on ZigBee and 4G communications for photo-voltaic generation," in CSEE Journal of Power and Energy Systems, vol. 6, no. 1, pp. 52-63, March 2020, https://doi.org/10.17775/CSEEJPES.2019.01610

[42] Liang, C.B., Tabassum, M., Kashem, S.B.A., Zama, Z., Suresh, P., Saravanakumar, U. (2021). Smart Home Security System Based on Zigbee. In: Suresh, P., Saravanakumar, U., Hussein Al Salameh, M. (eds) Advances in Smart System Technologies. Advances in Intelligent Systems and Computing, vol 1163. Springer, Singapore. https://doi.org/10.1007/978-981-15-5029-4_71

[43] Allahham, Alaa & Rahman, Md Arafatur. (2018). A SMART MONITORING SYSTEM FOR CAMPUS USING ZIGBEE WIRELESS SENSOR NETWORKS. International Journal of Software Engineering and Computer Systems. 4. 1-14. https://doi.org/10.15282/ijsecs.4.1.2018.1.0034

[44] Z. Qadir, F. Al-Turjman, M. A. Khan and T. Nesimoglu, "ZIGBEE Based Time and Energy Efficient Smart Parking System Using IOT," 2018 18th Mediterranean Microwave Symposium (MMS), 2018, pp. 295-298, https://doi.org/10.1109/MMS.2018.8611810

[45] V. Aswin Raaju, J. Mappilllai Meeran, M. Sasidharan and K. Premkumar, "IOT Based Smart Garbage Monitoring System Using ZigBee," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 2019, pp. 1-7, https://doi.org/10.1109/ICSCAN.2019.8878742

[46] I. Ali, S. Z. Partal, S. Kepke and H. P. Partal, "ZigBee and LoRa based Wireless Sensors for Smart Environment and IoT Applications," 2019 1st Global Power, Energy and Communication Conference (GPECOM), 2019, pp. 19-23, https://doi.org/10.1109/GPECOM.2019.8778505

[47] Z-Wave Alliance website. Available online: https://z-wavealliance.org/z-wave-global-regions/ (accessed on 10.10.2022).

[48] Luchian, A. Taut, I. Ivanciu, G. Lazar and V. Dobrota, "Z-Wave-Based Vehicular Blackbox with Automatic Emergency Assistance," 2018 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2018, pp. 85-90, https://doi.org/10.1109/LANMAN.2018.8475110

[49] Wei, Y. Chen, C. Chang and C. Yu, "The Implementation of Smart Electronic Locking System Based on Z-Wave and In-ternet," 2015 IEEE International Conference on Systems, Man, and Cybernetics, 2015, pp. 2015-2017, https://doi.org/10.1109/SMC.2015.351

[50] M. B. Yassein, W. Mardini and A. Khalil, "Smart homes automation using Z-wave protocol," 2016 International Conference on Engineering & MIS (ICEMIS), 2016, pp. 1-6, https://doi.org/10.1109/ICEMIS.2016.7745306

[51] Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. Sensors 2021, 21, 8087. https://doi.org/10.3390/s21238087

[52] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang and C. -H. Youn, "5G-Smart Diabetes: Toward Personalized Diabetes Diagnosis with Healthcare Big Data Clouds," in IEEE Communications Magazine, vol. 56, no. 4, pp. 16-23, April 2018, https://doi.org/10.1109/MCOM.2018.1700788

[53] Adhikari, A. Hetherington and S. Sur, "mmFlow: Facilitating At-Home Spirometry with 5G Smart Devices," 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2021, pp. 1-9, https://doi.org/10.1109/SECON52354.2021.9491616.

[54] Ahad, A.; Tahir, M.; Aman Sheikh, M.; Ahmed, K.I.; Mughees, A.; Numani, A. Technologies Trend towards 5G Network for Smart Health-Care Using IoT: A Review. Sensors 2020, 20, 4047. https://doi.org/10.3390/s20144047

[55] Ahad, M. Tahir and K. -L. A. Yau, "5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions," in IEEE Access, vol. 7, pp. 100747-100762, 2019, https://doi.org/10.1109/ACCESS.2019.2930628

[56] Dua, A. Dutta, N. Zaman and N. Kumar, "Blockchain-based E-waste Management in 5G Smart Communities," IEEE IN-FOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 195-200, https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162845

[57] Shen, Y.; Fang, W.; Ye, F.; Kadoch, M. EV Charging Behavior Analysis Using Hybrid Intelligence for 5G Smart Grid. Electronics 2020, 9, 80. https://doi.org/10.3390/electronics9010080

[58] Guevara, L.; Auat Cheein, F. The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. Sustainability 2020, 12, 6469. https://doi.org/10.3390/su12166469

[59] Sroka, P. and Kliks, A. (2022). 5G for V2X. In Wiley 5G Ref (eds R. Tafazolli, C.-L. Wang and P. Chatzimisios). https://doi.org/10.1002/9781119471509.w5GRef232

[60] Ai, A. F. Molisch, M. Rupp and Z. -D. Zhong, "5G Key Technologies for Smart Railways," in Proceedings of the IEEE, vol. 108, no. 6, pp. 856-893, June 2020, https://doi.org/10.1109/JPROC.2020.2988595

[61] LoRa Alliance website. Available online: https://lora-alliance.org/about-lorawan/ (accessed on 20 April 2022).

[62] Nowak, M., Koperski, B., Szymborska, A. (2016). Wykorzystanie standardu LoRaWAN do budowy bezprzewodowych sieci sensorowych w inteligentnych budynkach. Napędy i Sterowanie, nr 6, 120-123.

[63] Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. Sensors 2020, 20, 5800. https://doi.org/10.3390/s20205800

[64] Butun, I., Pereira, N.S., & Gidlund, M. (2019). Security Risk Analysis of LoRaWAN and Future Directions. Future Internet, 11, 3.

[65] Foubert, B.; Mitton, N. Long-Range Wireless Radio Technologies: A Survey. Future Internet 2020, 12, 13. https://doi.org/10.3390/fi12010013

[66] Chacko, S., Job, M.D. (2018). Security mechanisms and Vulnerabilities in LPWAN. IOP Conference Series: Materials Science and Engineering.

[67] Nowak, M.; Derbis, P.; Kurowski, K.; Rózycki, R.; Waligóra, G. LPWAN Networks for Energy Meters Reading and Monitoring Power Supply Network in Intelligent Buildings. Energies 2021, 14, 7924. https://doi.org/10.3390/en14237924

[68] Sinha S.R., Wei Y., Hwang S.: A survey on LPWA technology: LoRa and NB-IoT, Division of Electronics and Electrical Engineering, Dongguk University – Seul, Korea 2017.

[69] Pathak, G.; Gutierrez, J.; Rehman, S.U. Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions. Electronics 2020, 9, 1195. https://doi.org/10.3390/electronics9081195

[70] Basford, P.J.; Bulot, F.M.J.; Apetroaie-Cristea, M.; Cox, S.J.; Ossont, S.J. LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation. Sensors 2020, 20, 648. https://doi.org/10.3390/s20030648

[71] Nowak, M. (2016). Nowe rozwiązania informatyczne wspierające systemy sterowania, monitorowania i wizualizacji w gospodarce wodno-ściekowej. [w:] Zaopatrzenie w wodę, jakość i ochrona wód. ISBN: 9788364959455

[72] Cappelli, I.; Parrino, S.; Pozzebon, A.; Salta, A. Providing Energy Self-Sufficiency to LoRaWAN Nodes by Means of Thermo-electric Generators (TEGs)-Based Energy Harvesting. Energies 2021, 14, 7322. https://doi.org/10.3390/en14217322

[73] Bäumker, E.; Conrad, L.; Comella, L.M.; Woias, P. A Fully Featured Thermal Energy Harvesting Tracker for Wild-life. Energies 2021, 14, 6363. https://doi.org/10.3390/en14196363

[74] Rinaldi, S.; Pasetti, M.; Sisinni, E.; Bonafini, F.; Ferrari, P.; Rizzi, M.; Flammini, A. On the Mobile Communication Requirements for the Demand-Side Management of Electric Vehicles. Energies 2018, 11, 1220. https://doi.org/10.3390/en11051220

[75] Sharma, V.; You, I.; Pau, G.; Collotta, M.; Lim, J.D.; Kim, J.N. LoRaWAN-Based Energy-Efficient Surveillance by Drones for Intelligent Transportation Systems. Energies 2018, 11, 573. https://doi.org/10.3390/en11030573

[76] Haozhe Zhang, H. Zhang, Long He, L. He, Francesco Di Gioia, F. Di Gioia, Daeun Choi, D. Choi, Antonio Elia, A. Elia, & Paul Heinemann, P. Heinemann. (0000). LoRaWAN based internet of things (IoT) system for precision irrigation in plasticulture fresh-market tomato. Smart agricultural technology, 2, 100053. https://doi.org/10.1016/j.atech.2022.100053

[77] Wu, F.; Wu, T.; Yuce, M.R. An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications. Sensors 2019, 19, 21. https://doi.org/10.3390/s19010021

[78] Liang, R.; Zhao, L.; Wang, P. Performance Evaluations of LoRa Wireless Communication in Building Environments. Sensors 2020, 20, 3828. https://doi.org/10.3390/s20143828

[79] Pereira, F.; Correia, R.; Pinho, P.; Lopes, S.I.; Carvalho, N.B. Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment. Sensors 2020, 20, 6420. https://doi.org/10.3390/s20226420

[80] Minhas, N.; Kumar, Dr. (2018). Performance Analysis of ISM Band Antennas: A Survey. International Journal of Advanced Computer Research.

[81] Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. Sensors 2018, 18, 3995. https://doi.org/10.3390/s18113995

[82] The ThingNetwork website. Available online: https://www.thethingsnetwork.org/docs/quick-start (accessed on 10.10.2022).

[83] The ThingStack website. Available online: https://www.thethingsindustries.com/docs/ (accessed on 10.10.2022).

[84] Thingspeak website. Available online: https://thingspeak.com (accessed on 10.10.2022).

[85] OpenStack website. Available online: https://www.openstack.org/community/ (accessed on 10.10.2022).

[86] Chirpstack website. Available online: https://www.chirpstack.io (accessed on 10.10.2022).

[87] TheThings.io website. Available online: https://thethings.io (accessed on 10.10.2022).

[88] Lorank Gateway User's Guide 8. https://github.com/Ideetron/Larank/blob/master/lorank8v1/manual.pdf ((accessed on 10.10.2022).

RFM95W radio module documentation. https://www.hoperf.com/modules/lora/RFM95.html (accessed on 10.10.2022).

[89] A guide to interfacing an Arduino and RFM95W-based terminal device with a TTN.

https://www.mobilefish.com/developer/lorawan/lorawan_quickguide_build_lora_node_rfm95_arduino_uno.html (accessed on 10.10.2022).

[90] Arduino IoT Cloud documentation. Available online: https://docs.arduino.cc/cloud/iot- cloud/tutorials/cloud-lora-getting-started (accessed on 10.10.2022).

[91] Peruzzi, G.; Pozzebon, A. A Review of Energy Harvesting Techniques for Low Power Wide Area Networks (LPWANs). Energies 2020, 13, 3433. https://doi.org/10.3390/en13133433

[92] Polonelli, T.; Brunelli, D.; Marzocchi, A.; Benini, L. Slotted ALOHA on LoRaWAN-Design, Analysis, and Deployment. Sensors 2019, 19, 838. https://doi.org/10.3390/s19040838

[93] Bouguera, T.; Diouris, J.-F.; Chaillout, J.-J.; Jaouadi, R.; Andrieux, G. Energy Consumption Model for Sensor Nodes Based on LoRa and LoRaWAN. Sensors 2018, 18, 2104. https://doi.org/10.3390/s18072104

[94] Almuhaya, M.A.M.; Jabbar, W.A.; Sulaiman, N.; Abdulmalek, S. A Survey on LoRaWAN Technology: Recent Trends, Opportunities, Simulation Tools and Future Directions. Electronics 2022, 11, 164. https://doi.org/10.3390/electronics11010164

[95] Ismail, D., Rahman, M., & Saifullah, A. (2018). Low-power wide-area networks: opportunities, challenges, and directions. Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking.

[96] TTN Mapper. Available online: https://ttnmapper.org/heatmap/ (accessed on 10.10.2022).

[97] Amsterdam Smart City. Available online: https://amsterdamsmartcity.com/about (accessed on 10.10.2022).

[98] Gassara Mouna & Elleuchi Manel, Abid Mohamed. 2021. “Cloud-based platforms for LoRa internet of things: a survey”. International Journal of Informatics and Communication Technology (IJ-ICT). 10. 54. https://doi.org/10.11591/ijict.v10i1.pp54-64

[99] So Jaeyoung, Kim Daehwan, Kim Hongseok, Lee Hyunseok, Park Suwon. 2016. "LoRaCloud: LoRa platform on OpenStack". IEEE NetSoft Conference and Workshops (NetSoft), pp. 431-434.

[100] LMiC Bilblioteka. https://github.com/mcci-catena/arduino-lmic (accessed on 10.10.2022).

[101] OTAA and ABP activation - differences. https://www.thethingsindustries.com/docs/devices/abp-vs-otaa/ 3 (dostęp 20.04.2022).

[102] Aras, E., Ramachandran, G.S., Lawrence, P.W., & Hughes, D. (2017). Exploring the Security Vulnerabilities of LoRa. 2017 3rd IEEE International Conference on Cybernetics (CYBCON), 1-6.

[103] Torres, N.; Pinto, P.; Lopes, S.I. Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem. Appl. Sci. 2021, 11, 3176. https://doi.org/10.3390/app11073176

[104] Kufakunesu, R.; Hancke, G.P.; Abu-Mahfouz, A.M. A Survey on Adaptive Data Rate Optimization in LoRaWAN: Recent Solutions and Major Challenges. Sensors 2020, 20, 5044. https://doi.org/10.3390/s20185044

[105] Basu, D., Gu, T., & Mohapatra, P. (2020). Security Issues of Low Power Wide Area Networks in the Context of LoRa Networks. ArXiv, abs/2006.16554.

[106] Weinand A.; de la Fuente A. G.; Lipps C.; Karrenbauer M. Physical Layer Security based Key Management for LoRaWAN, in the 2020 Workshop on Next Generation Networks and Applications (NGNA), Kaiserslautern, Germany, December 2020.