Multidiszciplináris tudományok, 12. kötet. (2022) 4 sz. pp. 15-24 **https://doi.org/10.35925/j.multi.2022.4.2**

COMMUNICATION SOLUTIONS FOR SMART BUILDINGS

Szilárd Szopkó
research assistant, University of Miskolc, Research Institute of Applied Earth Science
3515 Miskolc, Miskolc-Egyetemváros, e-mail: szopko@afki.hu

Ildi Bölkény
research associate, University of Miskolc, Advanced Materials and Intelligent Technologies Higher Education and Industrial Cooperation Centre, EIKI
3515 Miskolc, Miskolc-Egyetemváros, Building of IT, I/100., e-mail: bolkeny@eiki.hu

Abstract
Building energy is a priority in the European Union's energy efficiency directives. In line with this, the EnerOptima module implemented within the framework of the Earth Energy Competence Center Project aims to optimize the building energy of existing buildings. The selection of the communication of the measuring and control modules to be implemented in the project requires great care, as it determines the quality of the IoT network. The article deals with the communication options used in different building energetics and their comparison. The purpose of this article is to compare communication protocols that are well-suited to the project and to select the optimal one for the project.

Keywords: *smart building, communication, IoT*

1. Introduction

Reducing energy consumption and waste is becoming increasingly important for the European Union. EU leaders set a target in 2007 to reduce the EU's annual energy consumption by 20% by 2020. In 2018, as part of the Clean Energy for All Europe package, a new target of reducing energy consumption by at least 32.5% by 2030 has been set. In line with this, the EnerOptima module implemented within the framework of the Earth Energy Competence Center Project aims to optimize the building energy of existing buildings. (Ciucci, 2021)

To increase the energy efficiency of buildings, the goal is to develop an efficient, self-assessing and predictive decision-making method and model system that can be parameterized for a specific building and optimizes the energy use of the building based on the coordinated operation of the three main components (feeding, consumption and storage) of building energy. One of the three sub-tasks of the module is to minimize energy consumption while ensuring the needs for comfort and user habits.

Smart home, smart grid, smart heating, smart devices for energy efficiency are one of the most popular and steeply evolving markets today. There are millions of tools to buy. To the best of our knowledge, however, there is still a lack of coordinated metering-control-optimization systems that are prepared for the technological and commercial changes that will pose future energy challenges. The aim of the project is to research and develop a modular family of energy efficiency tools that can be integrated into an existing BEMS, that can be easily parameterized to local conditions and that optimizes the energy used according to the needs and investment opportunities of the building operator.

The selection of the communication of the measuring and control modules to be implemented in the project requires great care, as it determines the quality of the IoT network. The following chapter

provides a brief overview of similar completed projects. Then it deals with the communication options used in different building energetics and compares them. The purpose of this article is to compare communication protocols that are well-suited to the project and to select the optimal one for the project.

2. Similar projects

Smart Build, Improving the Energy Efficiency in Public Buildings project was already completed. For analysing the potential for energy savings nine public demonstration sites in three different European countries, namely Italy, Greece and Slovenia were equipped with Information and Communication Technology devices. The system has three levels. Level of collect information from the buildings and spaces in real time using sensors, counters and meters. Level of send the data to the remote server and level of aggregate and elaborate data for energy analysis and energy efficiency and saving actions scheduling. All three levels communicate with each other, and especially in the first level, individual devices also communicate or can communicate with each other. The presentation of the project does not cover the communication system used. (smartbuild.eu)

According to the news of 2021 smart buildings are getting even smarter with the help of an investment from the U.S. Department of Energy (DOE). The DOE announced 10 pilot projects that will equip more than 7,000 buildings with smart technology to reduce energy use, costs, and emissions. Connected communities of grid-interactive efficient buildings use smart controls, sensors, and analytics to communicate with power grid, reducing the amount of energy they require during periods of peak demand. This capability is used to optimize buildings and distribute energy resources to maintain the comfort of the building occupants, lowers utility bills, and reduces grid system costs. The 10 pilot projects represent a cross-section of the buildings industry that include utilities, local governments, homebuilders, and end-users. (energy.gov)

The 'Pilot project for smart building services technology' project tests new smart technology solutions in a pilot environment in Otaniemi. With sensible building services technology the lifetime costs of a building and manage to improve its utilisation ratio can be cuted. The aim is to develop the facilities so that they can be altered according to the situation at hand. Items installed in the facilities include: Control system for lighting, building automation, security and access monitoring, camera surveillance, indoor positioning, and IoT sensors. The pilot project is part of the Aalto Industrial Internet Campus (AIIC), which brings together the research activities of the Aalto Internet of things and industrial digitalisation for the creation of shared research platforms and experimental set-ups, in areas such as manufacturing the process industry, as well as construction and building management. Although the project was completed in 2018, the communication protocols used were not published. (aalto.fi)

3. Communication

There are many wireless communication technologies. These include those that are in competition with each other and some that do not occur because they have been developed for a specific target area. The point is that whatever these networks are, they have characteristics that make them more suitable for this or that task than their peers. To decide this, we usually need to know only a few characteristics of the given system: range, transmission speed, number of devices (how many devices can be connected to the network at one time…), operating frequency (affects transmission speed…), energy consumption (together with operating frequency affects the range…), security, cost, etc. Four wireless communication technologies were examined, especially considering their applicability in the field of building automation.

3.1. Wi-Fi

Wireless communication technology based on microwaves (more precisely radio waves…). It allows you to use various devices such as computers, tablets, smartphones, mobile phones, etc. connecting to the Internet (World Wide Web…). It can be used to implement wireless networks in homes, offices and public places (airport, train station, cafe, restaurant, hotel, etc.) through which different users can connect to the Internet with their own computer. (Geier, 2021; Gast, 2021)

Wi-Fi networks can be public, open networks, private networks, public but closed networks, public but only partially closed networks, and there are commercial, so-called HotSpot providers as well. Anyone can connect to public, open networks without any restrictions. Private networks are password protected, only if you know this will the user be able to connect. Public but closed networks can only be used for a limited time by users who know the password and access to the network is managed by a separate program. HotSpot providers provide limited access to the network and the entire Internet for a fee. Public but partially closed networks are a transition between public, open networks and private networks. A small portion of the available bandwidth can be used by anyone, but a larger portion provides password access for a smaller group. In doing so, they are trying to restrict the activities of people who abuse free internet use.

Table 1. *Key features of Wi-Fi standards (Geier, 2021; Gast, 2021)*

Standard	Frequency [GHz]	General speed [Mbit/sec]	Maximum speed [Mbit/sec]	Indoor range [m]	Outdoor range [m]
802.11	2.4	0.9	2	20	100
802.11a	5	23	54	35	120
802.11b	2.4	4.3	11	38	140
802.11g	2.4	19	54	38	140
802.11y	23	23	54	50	5000
802.11n	2.4/5	74	600	70	250
802.11ac	2.4	500	1300	140	360
802.11ax	2.4/5	-	9600	-	-

Standards related to Wi-Fi technology include 802.11 (original…), 802.11a (Wi-Fi 2), 802.11b (Wi-Fi 1), 802.11g (Wi-Fi 3), 802.11y, 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6). The most important data for each standard are summarized in the Table 1.

Wi-Fi devices mostly operate on two frequencies, 2.4 GHz and 5 GHz. Usually only one frequency is used, but nowadays there are more and more commercially available devices that can handle both frequencies. A lower frequency usually means a lower transmission speed, but this is coupled with a longer range. If transmission speed is required when building a Wi-Fi network, 5 GHz is the clear winner, but the more limited range should also be considered here. (Geier, 2021; Gast, 2021)

WEP (Wired Equivalent Privacy…) was the first encryption standard in Wi-Fi. It also has a version based on 64, 128, 256 and 512 bit keys, but even with the right settings it can be cracked in minutes. Although it provides a basic level of protection for users, but it gives a false sense of security and is therefore not widely used today. The WPA (Wi-Fi Protected Access…) encryption method is now supported by all devices, essentially created to replace WEP anno. WPA uses an RC4 (Rivest Cipher 4…) encryption algorithm called TKIP (Temporal Key Integrity Protocol…) to protect data. The main

advantage of TKIP is that it generates a new key after the set time or the amount of data transmitted. WPA only provides real security if you work with a password that is long and complex enough. The IEEE 802.11i-2004 encryption method is now supported by all devices and provides the best protection for users. The method is also known as WPA2. WPA3 is version 3 of Wi-Fi's current favorite encryption algorithm, not yet so widespread, only a few devices support its use. The most important innovation lies in the recognition of password guessing. (Geier, 2021; Gast, 2021)

3.2. Bluetooth

Bluetooth is a wireless communication method for transmitting large amounts of information (high data-rate…) over a short range beetween devices with low-cost and low power. It is a radio frequency cable replacement technology designed primarily for the exchange of data between fixed and mobile devices, but also allows for easy file sharing and the connection of various devices to the Internet.

In Bluetooth communication, the energy available to the transmitter determines how far the Bluetooth device can operate. Based on this, the assets can be divided into 3 groups. Class 1 devices have the most power and can therefore operate up to a distance of 100 m. The class 2 group includes the most commonly used Bluetooth devices with a maximum operating distance of 10 m. Devices in class 3 have the least energy and can therefore only operate up to a distance of 1 m.

Bluetooth devices can connect to a network in two ways (topology…), piconet and scatternet. Bluetooth is a master / slave comm unication technology where one (single piconet…) or multiple (multiple piconet…) slaves are connected to a master in a piconet topology. Due to its design, the piconet topology is most reminiscent of a point-to-point communication relationship. Communication is always initiated by the master on the network and also determines when which slave can communicate. It is not possible to communicate directly between two slave devices. In a piconet network maximum of 7 slaves can be connected to a master, so a total of 8 devices can form a buletooth network. The structure of the piconet topology can be studied in the following figures. (Townsend, 2014)

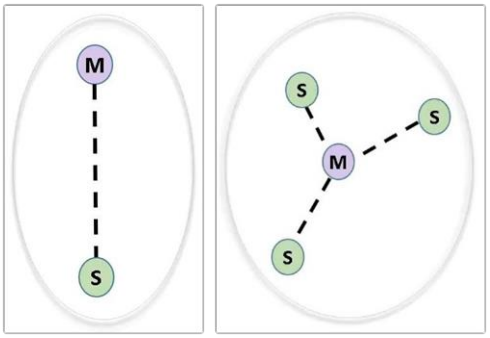

Figure 1. *Structure of a Bluetooth network with single piconet topology and with multiple piconet topology (Townsend, 2014)*

Bluetooth networks with scatternet topology are essentially connections of Bluetooth networks with piconet topology. Each subnet with piconet topology can be connected in the form of a master-slave or a master-master, where, of course, the individual connection points cannot be on the same subnet. The structure of the scatternet topology can be studied in the following figure.

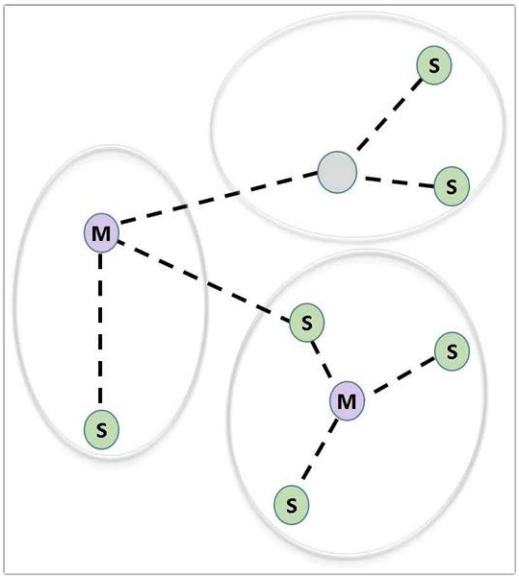

Figure 2. *Structure of a Bluetooth network with scatternet topology (Townsend, 2014)*

Bluetooth uses the band around 2.4 GHz for communications, which is essentially a frequency range that can be used for industrial, scientific, and medical purposes (ISM frequency band…). The area bounded by the minimum frequencies 2402 MHz and the maximum frequencies 2483.5 MHz is divided into 79 channels with a bandwidth of 1 MHz. When a message is sent, the transmitter bounces randomly between channels so fast that up to 1,600 hops occur in 1 second. The system always selects a non-interfering channel for communication under the given conditions. The information flows between the transmitter and the receiver in packets, where each packet is transmitted on a different channel (the choice is made according to the frequency hoping method…), so if 1600 packets are transmitted in 1 second, this requires a transmission time of 625 μsec. Random hopping on channels minimizes the potential for interference with devices that also use the ISM band for communication. (Townsend, 2014)

3.3. ZigBee

ZigBee is a cost-effective wireless communication method for the short range transmission of little data (low data-rate…) between low power devices. ZigBee is a communication standard designed specifically for sensor networks. Perhaps the most widely used method of communication in the world of IoT (Internet of Things…). An open source method, which is maintained, updated and made available by a separate international organization (ZigBee Alliance…). The most important areas of its use are building automation, medical data collection and industrial control systems. (Wang et al., 2014)

Due to the power requirements of Wi-Fi and due to the limited number of devices of Bluetooth, they are not really suitable for collecting medical data. However in ZigBee it is possible to process information provided by up to hundreds of sensors.

Due to its low power consumption, a ZigBee device can remain operational for up to several years on a single battery charge. When a ZigBee device is not communicating, it is able to wait in sleep mode. A low rate means a minimum transfer rate of 20 kbps and a maximum transfer rate of 250 kbps, wich is low compared to Wi-Fi or Bluetooth. The distance of the communication is not too significant, indoors it is only 75-100 m, but in the case of direct view it can be up to 300 m. The network join time for a new

device is 30 mses, which is quite good compared to Wi-Fi or Bluetooth. ZigBee is suitable for both small and large networks, as it allows up to 65,000 devices to be connected to a network, but experience has shown that it is not advisable to string more than 240 devices to a network. However, this number is still better than the maximum allowed for Wi-Fi and Bluetooth. (Wang et al., 2014)

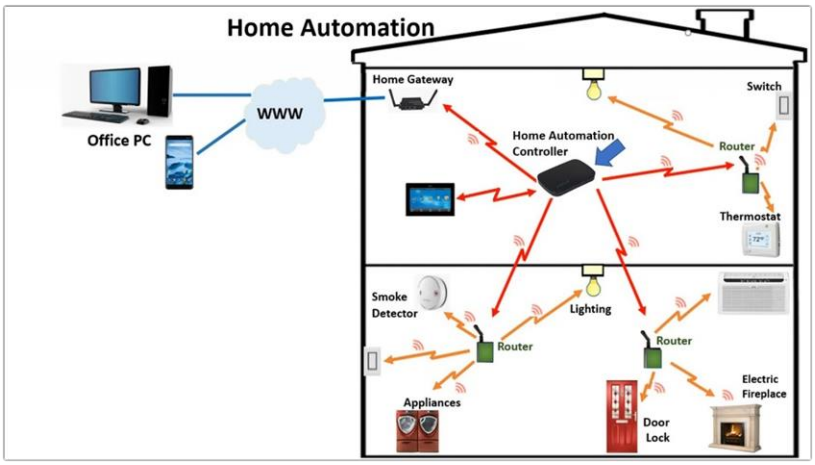

Figure 3. *Building automation (home automation…) with ZigBee devices (Wang et al., 2014)*

The ZigBee communication method uses 3 frequency bands, one in Europe, one in the Americas and Australia, and one worldwide. The frequency band used in Europe is around 868 MHz, which allows only one channel (channel 0…) to be created. The area around 915 MHz (902-928 MHz…) used in the Americas and Australia is already divided into 10 channels (channels 1-10…), the distance between each channel being 2 MHz. The worldwide used frequency band around 2.4 GHz has enough space to set up 16 channels (channel 11 26…), the distance between each channel is 5 GHz.

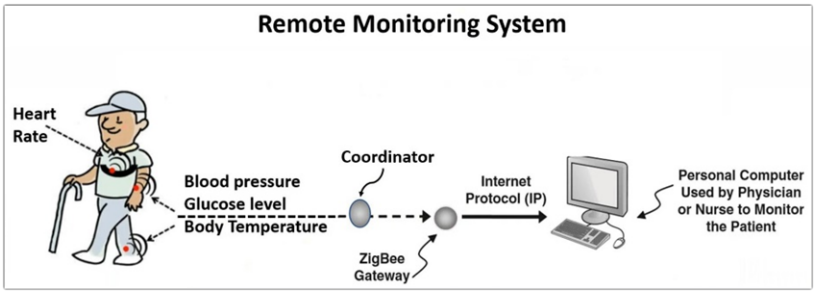

Figure 4. *Collecting medical data with ZigBee devices (Wang et al., 2014)*

There are 3 types of ZigBee devices, there is a coordinator, a router and an end device end. Each ZigBee network can have only one coordinator. The coordinator is the most important element and starting point of the network. The coordinator is responsible for selecting the appropriate channel and assigning a unique ID to the network and allocating a unique address to each device connected to the network. The coordinator is also responsible for initiating and processing messages between elements of the network. Routers act as an intermediate node between the coordinator and the end devices,

directing data traffic between the different nodes. They receive and store messages for end devices and allow other routers and end devices to connect to that network. If the appropriate information is available for the end device, it is forwarded to a node or directly to a coordinator, or it can be in sleep mode to save power. All data to the end device is first sent to the node of the end device and essentially the end device is also responsible for requesting and sending messages from the node.

ZigBee devices can be connected to each other in the form of a star topology, a mesh topology or a tree topology. Star topology is the simplest and most cost-effective form. In case of star connection, there is no router in the network, the end devices are connected directly to the coordinator. There is no possibility for two end devices to communicate directly, in the event of a coordinator failure, the entire network will announce the boring and the distance of the communication will be greatly influenced by what the coordinator is capable of. (Wang et al., 2014; Elahi and Gschwender, 2015)

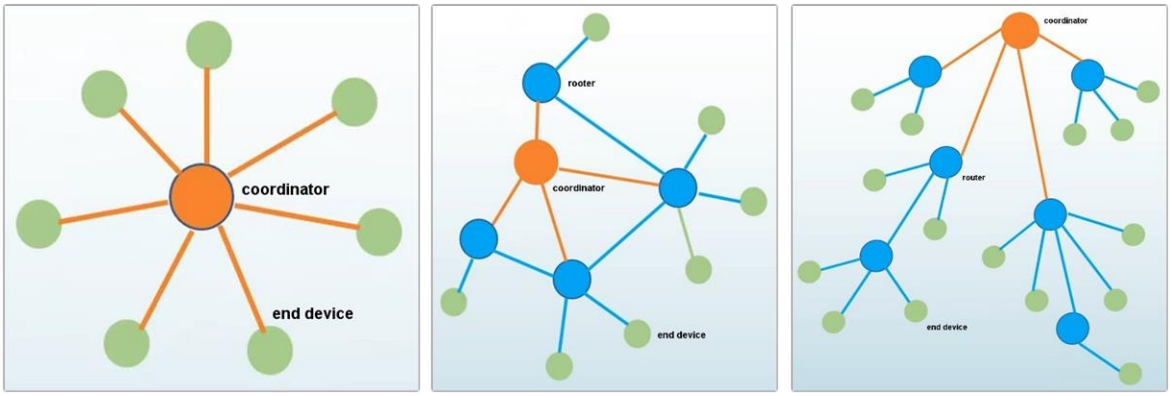

Figure 5. *Structure of a ZigBee network with star topology, with a mesh topology and with a tree topology (Wang et al., 2014; Elahi and Gschwender, 2015)*

In the case of a mesh topology, there are several nodes in the network, where adjacent nodes are in communication with each other and the end devices are also connected to these nodes, but so that one end device cannot be connected to another end device or another node. In the event of a node losing communication, the system will be able to find a new route to ensure uninterrupted communication. The tree connection is not very different from the network connection, only here a node cannot be connected to more than one node, of course an intermediate node can receive several end devices.

The ZigBee communication method uses an AES encryption algorithm to protect general data and authorization information. AES is one of the most secure and robust encryption methods used by even government agencies to prevent unauthorized access to information. (Wang et al., 2014; Elahi and Gschwender, 2015)

3.4. LoRa

LoRa is a cost-effective wireless communication method for transmitting little information over a wide range between low power devices. It uses a wide range of modulation techniques to transmit information over fairly long distances (up to more than 10 km…) with low energy consumption. The LoRa standard is maintained and made available by an international organization (LoRa Alliance…). Due to its energy savings, like ZigBee, LoRa is very suitable for implementing of IoT systems. (Gehlot et al., 2020)

LoRa uses different frequencies in different parts of the world to transmit information. The frequency range around 868 MHz (867-869 MHz…) in Europe, 915 MHz (902-928 MHz…) in America and 433

MHz in Asia. Non-high frequency means low transmission speeds, so the maximum communication speed can be 250 bps to 50 kbps in Europe and 980 bps to 21.9 kbps in America, which is quite low compared to several Mbps for other communication methods. The frequencies used by LoRa networks are described in more detail in the following list:

- EU: 863 - 870 MHz
- EU: 433 MHz
- USA: 902 - 928 MHz
- Australia: 915 - 928 MHz
- China: 779 - 787 MHz
- China: 470 - 510 MHz
- Asia: 923 MHz
- Korea: 920 - 926 MHz
- Indonesia: 865 - 869 MHz

The data is transferred asynchronously between the elements of the LoRa network only if the information is available. Data from end devices or end nodes is sent to a LoRa gateway. A device can even connect to multiple gateways within reach. The data is sent from the gateways to the server (LoRa server program…) via a normal Internet connection, which performs filtering on duplicate packets, performs security checks and is also responsible for managing the LoRa network itself. The operation and stability of the LoRa network is excellent at lower loads, but in case of higher loads there may be problems with sending confirmations.

LoRa devices can be divided into 3 groups. Class A devices are battery powered devices. In that case the device wants to send data to the server, it is also ready to receive a command from the server in parallel. The server must wait completely with sending a command to the device until the next time data sending of the device, if there was nothing to tell the device at that time. Class B devices are also battery powered devices. Compared to class A devices, they can also receive commands from the server at specified intervals. Of course, this is only possible by synchronizing with the server. Class C devices have a direct power supply and are able to receive commands from the server at all times.

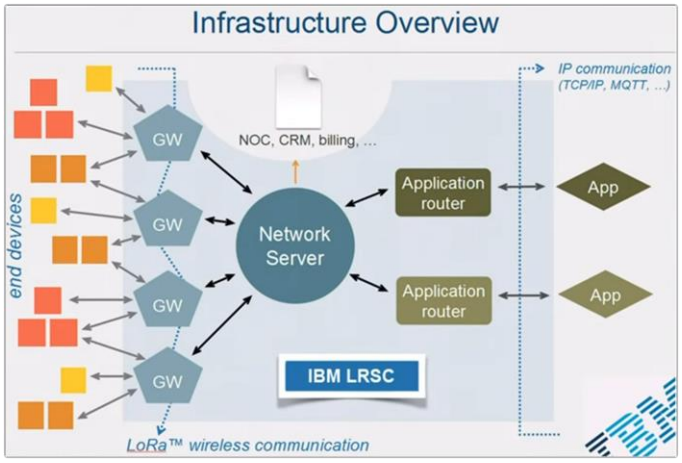

Figure 6. *Structure of a LoRa network (Gehlot et al., 2020)*

LoRa uses two keys to encrypt data to ensure communication. These keys are unique to each LoRa device. NwkSkey ensures the integrity of messages during data transfer between the device and the

network server, and AppSkey is used for data transfer between the device and the application server for AES-128 encryption. LoRa devices can connect to the network in two ways. The OTAA (Over-rhe-Air Activation…) method allows the device to request the server to generate new AppSkey and NwkSkey keys with its own AppSkey key, and these keys are used to encrypt communication between the device and the server. During the ABP (Activation by Personalization…) method, the user is responsible for managing the keys. (Gehlot et al., 2020)

4. Comparison

In the process of building automation, little information flows between the sensors and the central computer at not a high speeds, and little information is passed between the central computer and the intervening devices during decision-making again at not a high speed in the world too. Decision-making is mostly based on information provided by a lot of sensors and, of course it is also worth considering the cost of creating a building automation system. This is especially true for individuals who want to make a smart home from their flats by automating the operation of their apartemnt.

Wi-Fi and Bluetooth technologies allow only a limited number of accesses. The maximum number of devices connected to the network is 32 for Wi-Fi and 7 for Bluetooth. When automating a smaller home, 32 devices may still be enough, but there are not many possibilities for expanding the system. In terms of device numbers, the use of ZigBee, or LoRa technology, is much more advantageous because they are capable of receiving data from a larger amount of sensors, as they are IoT technologies. Due to their role in IoT, it is also due to the fact that LoRa and ZigBee devices are very energy- and cost-efficient, although LoRa performs slightly better in energy efficiency. Energy efficiency goes hand in hand with lower communication rates and longer operating ranges. However, a longer operating range makes it easier for unauthorized accessers and more difficult to identify those who steal the data.

Table 2. *Key parameters of wireless communication technologies (Geier, 2021; Townsend, 2014; Wang et al., 2014; Gehlot et al., 2020)*

Technology	**Device**	**Frequency**	**Speed**	**Range**
Wi-Fi	32	2.4/5 GHz	Even more Mbit/sec	Few m
Bluetooth	7	2.4 GHz	1 Mbit/sec 3 Mbit/sec	Cable replacement technology Few m (around the table)
ZigBee	240 (mostly) 65000 (theoretical)	868 MHz 915 MHz	20 – 250 kbps	Few 10 m
LoRa	Moire 100	868 MHz 915 MHz 433 MHz	50 kbps, or less	Few 10 km

5. Conclusion

Based on what has been described so far, we must distinguish whether the building automation system is intended to regulate the operation of a private house or a building that functions as a workplace. For

a system that operates a private house, a ZigBee network can clearly be the winner. Based on the number of devices, the transmission speed and the maximum communication range, we can say that when building a smart home, it is best to create a ZigBee network for building automation purposes, taking into account cost and security considerations.

It may also be useful to use a ZigBee network to automate a building that functions as a workplace, but this is more complicated. A workplace certainly has a complete, built-in computer network. This is an Internet communication network consisting of UTP cables and switches that allow star connection. In this case, you may want to consider using the internal network for building automation purposes as well. Of course, this requires Wi-Fi routers and devices capable of Wi-Fi communication, which will likely incur the cost of building the system, but will be offset by higher transfer rates and greater security. The building automation system has the possibility of using a physically isolated subnet protected by a firewall, and the range of a few meters from Wi-Fi routers makes it difficult to gain unauthorized access to the system. Of course, it is still possible to create ZigBee-based subnets and create a hybrid system.

6. Acknowledgement

Project 2019-1.3.1-KK-2019-00001 was implemented with the support of the Ministry of Innovation and Technology from the National Research Development and Innovation Fund, in the financing of the 2019-1.3.1-KK tender program.

References

[1] Ciucci, M. (2021). *Energiahatékonyság*. https://www.europarl.europa.eu/
[2] Smart Build Project. https://www.smartbuild.eu/
[3] Department of Energy (2021). *DOE invests $61 million for smart buildings that accelerate renewable energy adoption and grid resilience*. https://www.energy.gov/
[4] Aalto University (2017). *Pilot project for smart building services technology investigates the functionality of building services technology in the future in an everyday environment*. https://www.aalto.fi/
[5] Geier, J. (2021). *Designing and deploying 802.11 wireless networks: A practical guide to implementing 802.11n and 802.11ac wireless networks for enterprise-based applications*. (Networking Technology), 2nd Edition, ISBN-13: 978-1587144301
[6] Gast, M. S. (2021). *802.11 wireless networks: The definitive guide*. Second Edition 2nd Edition, ISBN-13: 978-0596100520
[7] Townsend, K. (2014). *Getting started with bluetooth low energy*. ISBN13 (EAN): 9781491949511
[8] Wang, C., Jiang, T., Zhang, Q. (2014). *ZigBee® Network protocols and applications*. 1st Edition, ISBN 9780367378783
[9] Elahi, A., Gschwender, A. (2015). *ZigBee wireless sensor and control network*. 1st Edition, Kindle Edition, ISBN-13: 978-0137134854
[10] Gehlot, A., Sharma, K. K., Singh, R., Sharma, R. K. (2020). *LoRA and IoT Networks for applications in Industry 4.0*