Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 29, S. 231-236, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 29, pp. 231-236, December 2021

Research Article

Wireless Communication Protocols for Project Developers in IoT Applications

Fatih Topaloğlu[1*]

[1*] Malatya Turgut Özal University, Faculty of Engineering and Natural Sciences, Departmant of Computer Engineering, Malatya, Turkey, (ORCID: 0000-0002-2089-5214), fatih.topaloglu@ozal.edu.tr

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2021 – 21-23 October 2021)

(**DOI:** 10.31590/ejosat.1018644)

ATIF/REFERENCE: Topaloğlu, F. (2021). Wireless Communication Protocols for Project Developers in IoT Applications. *European Journal of Science and Technology*, (29), 231-236.

Abstract

The effective use of network technologies in IoT applications necessitates the determination and use of the most efficient wireless network protocols according to the application area and scope. A project developed with IoT systems uses network technology and protocol structure that includes many protocols according to its purpose and scope. The protocols used include the communication of hardware, data communication and standards of how this communication starts and ends in IoT applications. Choosing the most suitable connection for project and application developer engineers in the product line covering IoT applications is of great importance for the efficient operation of the system. In the study, the most effective wireless network protocols for IoT applications were researched, explained and comparisons were made.

Keywords: IoT, Wireless communication, Wireless network protocols.

IoT Uygulamalarında Proje Geliştiriciler için Kablosuz İletişim Protokolleri

Öz

IoT uygulamalarında ağ teknolojilerinin etkin bir şekilde kullanılmaya başlanması uygulama alanı ve kapsamına göre en verimli kablosuz ağ protokollerinin belirlenmesini ve kullanılmasını gerekli kılmaktadır. IoT sistemleri ile geliştirilen bir proje, amaç ve kapsamına göre bir çok iletişim kuralları içeren ağ teknolojisini ve protokolü yapısında kullanmaktadır. Kullanılan protokoller IoT uygulamalarında donanımların haberleşmesi, veri iletişimi ve bu iletişimin nasıl başlayıp nasıl biteceğinin standartlarını içermektedir. IoT uygulamalarını kapsayan ürün bandında proje ve uygulama geliştirici mühendisler için en uygun bağlantıyı seçmek sistemin verimli bir şekilde çalışmasında büyük öneme sahiptir. Yapılan çalışmada IoT uygulamaları için en etkin kablosuz ağ protokolleri araştırılmış, açıklanmış ve kıyaslamalar yapılmıştır.

Anahtar Kelimeler: IoT, Kablosuz iletişim, Kablosuz ağ protokolleri.

[*] Corresponding Author: fatih.topaloglu@ozal.edu.tr

1. Introduction

The Internet of Things (IoT) aims to connect every device to the Internet so that these devices can be accessed anytime, anywhere and from any network (Nour et al., 2019). This concept has been defined as a new communication system where the Internet is connected to the physical world via wireless devices. This system has become an indispensable part of our daily life. On the other hand, its products and services offer many benefits that have not been thought of before, emerge as they are used and cannot be given up easily.

With the increase in smart technologies and the introduction of automation into buildings and cities, new network options have been developed for different applications.However, wireless devices with different communication standards and hardware limitations need to work in harmony with each other and with existing internet protocols (Castellani et al., 2010). Depending on the application, the most suitable network option is determined by considering factors such as data requirement, power demand, security and battery life, and application development continues in this way.

Wireless network technologies are widely preferred in IoT projects and applications because of their small size data exchange, low cost, minimum power consumption principle, and easy and flexible installation. Thanks to these technologies, it is possible to establish complex network structures, expand them and enable these structures to communicate with other technologies.

While human beings are able to handle most of their operations with the help of technology, technology manufacturers face problems in meeting the energy and battery demand of the technology used. Therefore, one of the conditions sought for every technology produced is low power consumption. Foreseeing this, engineers have developed a large number of wireless communication modules. In the study, the most effective wireless network protocols were determined by considering the features needed in IoT projects, they were explained with examples according to their application areas and comparisons were made.

The remainder of the work is organized as follows. In the second part, the analysis, application areas and examples of the determined wireless communication protocols are explained. In the third section, comparisons of the proposed protocols are made. In the last section, the study is summarized.

2. Proposed Wireless Network Protocols

Protocols are network languages or rule frames that are used in inter-device communication and determine the protocols. Network protocols generally define physical interfaces, signal levels and encoding, network addresses, connection establishment/disconnection, size and structure of network data units, error checking, successful acknowledgment, flow control mechanisms, database fields and formats, application-specific meanings. In addition, standardization studies have been carried out so that wireless sensors with different hardware/communication sources can be used in large-scale applications (Sheng et al., 2013; Atzori et al., 2010; Tagami & Arumaithurai, 2016; Chen, 2017; Lin et al., 2017).

People sometimes even refer to any wireless technology they use as a wireless network “Wi-Fi”. While it may seem ideal for wireless devices all over the world to use a common network protocol such as Wi-Fi, networks available today instead support a wide variety of protocols. Because no existing protocol provides the optimal solution for the different wireless uses that people want. Some offer faster speeds or more reliable and longer distance connections, while others offer better optimized options for battery saving on mobile devices. Due to the lossy nature of the wireless transmission environment and the resource constraints of the devices in the environment, communication protocols are designed differently from existing internet protocols (Akyildiz, Su, Sankarasubramaniam & Cayirci, 2002). The following wireless networking protocols have proven particularly useful in IoT applications and projects.

2.1. Radio Frequency Identification (RFID)

RFID is a method of recognizing objects individually and automatically using radio frequency. In line with the developing technology, in line with the increasing demands in IoT applications, it has now become a necessity to use RFID technology in information collection, product controls, counting and regulations in the face of complexity in business integrity. It provides benefits at many points such as facilitating business life, reducing costs, accelerating the workflow, increasing efficiency and profitability.

Scope of application; Tracking and Identification (Supply chain management, inventory control, retail payment, recycling, cargo tracking, etc.) (Cho et al., 2007), Payment and Storage (Electronic access systems, contactless credit cards, bus and subway passes, concert tickets etc.), Access Control (Building access cards, concert tickets, vehicle contact systems etc.), Anti-Forgery (Paper coins, game tokens, prescription drugs etc.).

The RFID system includes a tag, a reader, and an antenna. The reader sends a polling signal to the tag via the antenna and the tag responds with its unique information. The antenna sends the incoming data to the computer environment digitally. Thanks to the support software, these data are read and transactions are made. RFID tags can be placed directly on or inside all objects to be identified in an RFID system. In this way, it is ensured that the product is recognized when it enters the coverage area, and the information recorded on the label is easily obtained. In RFID technology, tags are divided into three as active, passive and semi-passive. A detailed comparison of the features of RFID tags is given in Table 1.

Table 1. Features of tags in RFID technology

Label Type	**Passive**	**Active**	**Semi-Passive**
Power source	over RF	Battery	Battery
Communication	Response	Initiation and Response	Response
Max. Range	10 M	>100 M	>100 M
Cost	Cheap	Expensive	Average
Usage Area	Proximity Cards	Valuable Property Tracking	Pallet Tracking

Active RFID tags contain their own power source that allows broadcasting with a reading range of up to 100 meters. Long read ranges make active RFID tags ideal for many IoT applications where asset location and other improvements in logistics are important. Passive RFID tags do not have their own power source. Because the radio waves must be strong enough to power the tags, passive RFID tags provide a read range of up to 10 meters from close contact. Semi-Passive RFID tags As with active RFID tags, semi-passive tags also have an internal power supply. But in order to initiate communication, it must receive a warning from the RFID reader; For this reason, it is called a semi-passive tag. Due to its internal power supply, it provides a longer read range than passive tags.

2.2. Near Field Communication (NFC)

NFC is a short range wireless RFID communication technology. NFC, a contactless technology, is a network technology used to provide instant access to all digital data and information on your mobile device. In this technology, data transmission takes place in short distance, high frequency and low bandwidth. NFC is designed as a secure form of data exchange and NFC device can be both NFC reader and NFC tag. The most important device that performs this function in the market is smart phones. NFC devices in smart phones can work as both readers and tags.

The structure of the NFC Tag is quite simple. NFC readers send a signal to the tag via the antenna. The tag sends the unique information contained in it to the antenna of the reader. The antenna receives the incoming data and transfers it to digital media. An NFC device can act as both a reader and a tag. This unique capability has made it a popular choice for contactless payment by actors in the mobile industry in their decision to incorporate NFC into new smart phones.

NFC, a contactless technology, is a network technology used to provide instant access to all digital data and information on your mobile device. In this technology, data transmission takes place in short distance, high frequency and low bandwidth. This process takes place in 3 different ways. The first is The Host Card Emulation mode, where a mobile terminal acts as a smart contactless chip. The second is The Peer-to-peer mode of data exchange, which works in both directions between two mobile devices communicating with each other via NFC. The third is The Reader mode, which allows you to read information or trigger actions by closely touching or bringing the phone close to an NFC tag.

NFC is used as a payment method, it is often confused with QR code application. However, NFC technology is very different from QR code as it is a connection method and there are huge differences between the two systems. Near Range Communication stores data via a microchip and is therefore digital in nature. QR code, on the other hand, stores data in an image and does not carry a digital identity on its own. While the QR code becomes active with the optical reader on digital devices, NFC establishes a wireless connection with the opposite device. QR code can be found in digital or physical media, and codes in physical media can simply be deformed. NFC, on the other hand, is only available in the digital environment and does not deform as long as the devices are not damaged.

2.3. Bluetooth

Bluetooh is a wireless technology that works with radio waves and its main purpose is to provide data communication between different devices. The Bluetooth standard is accepted as the basis of the IEEE 802.15 family of standards created by IEEE to develop communication standards for wireless private area networks (Bisdikian, 2001). Bluetooth opens the doors of wireless data and voice communication with a technique that is low power consumption, cheap, reliable, fast and allows to be integrated into all devices (Shepherd, 2001). Bluetooth networks transmit data in the form of low-power radio waves. It communicates at a frequency of 2.45 gigahertz. This frequency band is reserved for the use of industrial, scientific and medical devices by international agreements.

With Bluetooth 2.1, energy saving has been improved by 5 times. With Bluetooth 3.0, the data transmission rate has increased up to 24 Mbps, allowing users to share files and play games to a more comfortable level. With Bluetooth 4.0, power consumption has been further reduced, enabling the use of equipment such as fitness, heartbeat and step counters on phones. The most important Bluetooth version, known to those who are interested in IoT, especially as a low-energy protocol, is 4.0. Because in this version, energy consumption has been reduced even more and it has become available for use in IoT systems.

The Bluetooth 5.0 version caters specifically to IoT applications. The most important feature of this version is that it can pass through walls more effectively and can be used more effectively indoors such as home and office. With Bluetooth 5.0, the range distance has been increased 4 times, the data transmission rate has been doubled and the connectionless data transmission capacity has been increased 8 times. While doing these, its low power consumption has made it an indispensable protocol for IoT.

2.4. Wireless

The widespread use of Wi-Fi connection in the home and office environment has the biggest factor in the preference of Wireless technology in IoT. With this network protocol, processing and transmission of big data is carried out quickly. Wi-Fi technology is the same as the working principle of transistor radios and wireless network systems work with radio frequencies. In order for a Wi-Fi connection to take place, a device such as a modem that transmits the signal and another device, such as a smartphone, that can receive and convert these signals into data is required.

Wi-Fi is a compatibility indicator that indicates that technological devices can provide wireless connection. All technological devices that can communicate over a wireless network have one of the IEEE 802.11 standards. Network connection is performed at a radio frequency of 2.4 GHz or 5 GHz, depending on the IEEE 802.11 standard, which wireless access points and devices jointly support. Wireless connection standards; It is designated as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac. Wireless connection standards specifications are given in Table 2.

Table 2. IEEE 802.11 Wi-Fi protocol summary

Protocol	Frequency	Channel Width	MIMO	Max data rate
802.11ac wave2	5 GHz	20, 40, 80, 160 MHz	Multi User	1,73 Gbps
802.11ac wave1	5 GHz	20, 40, 80 MHz	Single User	866,7 Mb/sn
802.11n	2,4 -5 GHz	20, 40 MHz	Single User	450 Mb/sn
802.11g	2,4 GHz	20 MHz	No	54 Mb/sn
802.11a	5 GHz	20 MHz	No	54 Mb/sn
802.11b	2,4 GHz	20 MHz	No	11 Mb/sn

Some applications that can be done with wireless technology; With wireless devices placed in the human body, vital values can be constantly checked, the patient's medications can be controlled, whether the patient takes the right medication at the right time, and information such as general health information, benefits, harms, manufacturer, distributor of the product can be accessed via the internet thanks to the wireless device used on foods. With the wireless device placed in the cars, the driver can be warned against vehicle activities or creatures that may cause traffic accidents by controlling the mobility around a vehicle, where the bus is, how long it will arrive, the intensity in the bus can be instantaneous by using the camera and wireless systems placed in the public transportation vehicles and the mobile phone. possible to follow.

2.5. Long Term Evolution -Advanced (LTE-A)

LTE-A, a cellular communication protocol, enables the development of IoT applications that will operate over longer distances. LTE-A, LTE-Advanced and LTE+ are the names of the same service. LTE-A technology is an advanced or upgraded version of LTE technology, which is faster, more stable, and has higher bandwidth than normal LTE. This technology is closest to the connection speeds offered by real 4G technology.

The prominent advantages of LTE-Advanced are the ability to take advantage of advanced topology networks and optimize multi-origin networks by mixing macro cells and low power nodes. At this point, 4.5G stands out with its carrier aggregation feature. Thanks to this feature, it can access the internet with two connections at the same time. Another advantage is that it can use mobile network and Wi-Fi at the same time.

LTE-A provides high-speed transmission of big data. Of course, technologies such as GSM or 3G can be used instead. However, in places where remote data communication is required, using the 4G (LTE-A) band will enable the IoT application to perform faster. Sending big data in this way is both expensive and causes high power consumption. However, in cases such as fast transmission of smaller data, using this protocol will make transactions faster. In summary, it is necessary to take advantage of cellular network technologies such as LTE to receive data over long distances or to control devices.

2.6. ZigBee

Another important IoT communication protocol is Zigbee. Zigbee are low power consumption wireless technologies designed to move small amounts of data over short to medium distances. With its compatibility in wireless control and sensor networks, it has an important role in M2M and IoT applications. Zigbee technology is mesh network. Each node in the system acts as both a wireless data source and a repeater. Information from a single sensor node passes from node to node until it reaches the transmission gateway.

It uses the IEEE 802.15.4 low speed personal area network protocol for the unified physical layer in Zigbee technology. The data rate is 250 kbps Zigbee, and the wireless communication range varies between 10-100 meters. The most striking feature of ZigBee technology is its very low power consumption and long battery life, ranging from 6 months to 2 years depending on the application (Leung, 2002). Unlike Bluetooth, it can actively communicate with 30-40 units at the same time, which is 8 in Bluetooth (Bahl, Heile, & Naeve, 2002). Among the IoT system developers, Zigbee has a large user base with all these features.As can be seen in Table 3, Zigbee is one of the favorites of IoT developers because it can establish networks with high reliability, low cost, energy efficiency, support for a large number of nodes, and for monitoring and management purposes.

Table 3. Zigbee basic characteristic

Property	Value
Data Rate	868 MHz-20kb/s, 915 MHz-40kb/s, 2.4 GHz-250kb/s
Number of Units / Network	255
Distance	10-100 m
Complexity	Less complex than current standards
Battery Life	6 Months-2 Years
Number of Channels	868, 915 MHz – 11 Kanal, 2.4 GHz – 16 Channel
Address	8bit-64bit

This technology security systems (security alarm, fire-gas-water detector systems, entrance-exit controls), urban smart grid control devices, HVAC (heating, ventilation and air conditioning) control systems, health (monitoring and controlling body functions of patients and athletes), vehicles (monitoring tire pressure in places where cables cannot reach, for example), agriculture (humidity, It is widely used in local area sensor data networks such as water, temperature data monitoring), industry (production control, energy management, control of industrial devices), home automation and lighting controls.

2.7. Z - Wave

Based on low-power RF communication technology, Z - Wave is a wireless communication protocol. In addition, it is a globally accepted home and building automation standard (ITU-T G.9959) that allows devices in the home and office to communicate with each other and the user easily and wirelessly. Z-Wawe technology increases efficiency by controlling energy consumption, which is one of the main purposes of smart home systems (Shrouf, & Miragliotta, 2015; AlFaris, Juaidi, & Manzano-Agugliaro, 2017). Being wireless easy to install and controlling almost all kinds of electrical equipment has made Z-Wave the first choice in IoT applications.

Z-Wave technology provides a very powerful mechanism to communicate with all members in the networks, which makes the system more reliable (Withanage, Ashok, Yuen, & Otto, 2014). With its high scalability, it can control up to 232 devices. Its biggest advantage is that it is independent and compatible with teamwork. For example, by turning on the office lights, the temperature in the office can be adjusted to the predetermined set value. Table 4 describes the features of Z-Wave technology.

Table 4. Features of Z-Wave technology

Property	Explanation
Simple	All devices communicate with each other easily and in a very short time, without complicated programming and new wiring.
Strong	Points where it is too far from the control unit or behind a thick wall are also easily accessible.
Bidirectional Communication	It allows all points connected to the Z-Wave network to be controlled from anywhere with internet and devices such as mobile phones and tablets, and the current status can be monitored.
Smart	Devices in the network can work independently of each other as well as as a team.
Safe	It is extremely safe thanks to its very low electromagnetic wave emission.

Z-Wave devices are programmed according to the country of residence. Since it works over radio frequency, it does not work when moved to a different region. However, the 2.4 GHz band is subject to heavy interference from WiFi and Bluetooth systems. Zig-Bee operates on the 2.4 GHz band, which is the same as Bluetooth and Wi-Fi. Therefore, the more devices on the same frequency, the higher the interference.

Sub GHz bands using Z-Wave do not face the same interference issues. Z-Wave is a closed standard of silicon labs. However, as a closed system it should generally not change protocols and specific device hubs should not be required. Z-Wave provides additional security for easy identification by requiring each device to use a unique ID to communicate with the hub.

3. Discussion and Suggestions

The huge interconnected device ecosystem, called IoT, has been expanding rapidly around the world in recent years. Today, many devices around us have the ability to send information to other devices or applications, collect information and analyze information.

The invisible language that allows billions of devices in this ecosystem to talk to each other are IoT standards and protocols. Protocols used for personal devices that we use in daily life may not be suitable for meeting the requirements in IoT-based applications. Many wireless network protocols have been developed as a solution to this problem. Developed wireless network protocols offer the advantages of traditional LAN technologies without cable limit.

Table 5. Comparison of wireless communication standards.

Standard	Zigbee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM
Apps	Monitoring and Control	Instead of Cable	Web, E-mail, Video	Wide area voice and data
System Resource	4kb-32kb	250kb+	1 Mb+	16 Mb+
Network Size	256/65k+	7	30	1000
Band width (Kbps)	20-250	720	11000+	64-128
Range	1-75+	1-10+	1-100	1000+
Areas of Success	Durability, Cost	Cost, Convenience	Speed, flexibility	Accessibility, Quality

There are many options and alternatives when looking at the features of IoT wireless protocols, standards and technologies. Choosing the right protocol is a difficult task because each protocol has its own advantages and disadvantages (Reinisch, Kastner, & Granzer, 2007). In Table 5, the standards and technologies defined in the study and some comparisons of the most popular ones are also presented in tabular form.

Here are some requirements that application developer engineers should consider for IoT wireless networks; real-time data transfer, minimum millisecond delay, data flow protection and high security for applications, billions of heterogeneous machine connections, Monitoring and traffic control of devices in the Network, cost-effectiveness and application configuration capability. In addition, high-speed and high-capacity communication, wide coverage extension, low power consumption and cost, low latency, reliable communication, wide connection and detection capabilities offered by 5G technology, ultra-reliable and low-latency and massive object communication features, The project will offer important privileges for developers.

4. Conclusion

Today, access to information everywhere, quickly and freely has become important, and wireless network systems have gained great importance. Wireless network systems are a technology that will not lose its importance in the future, as it is today, and even a huge investment will be made on it. The wireless environment gives engineers and practitioners the freedom to work wirelessly without sacrificing connectivity. In addition, devices connected to other wireless devices provide mobile workers with more uninterrupted working methods. Wireless environment makes work more effective and efficient, while helping to ease the network in in-house applications.

Some of the devices used in IoT applications serve only as receivers, some only as transmitters, and some as both receivers and transmitters. Almost all of them use different communication protocols. So there are many connection options available to engineers. With the study, the most effective wireless communication protocols from many standards and technologies to be used in IoT applications are defined.

References

Akyildiz, I., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks*, 38(4), 393–422. doi: 10.1016/s1389-1286(01)00302-4

AlFaris, F., Juaidi, A., Manzano-Agugliaro, F. (2017). Intelligent homes' technologies to optimize the energy performance for the net zero energy home. *Energy and Buildings Journal*, 153, 262–274. doi:10.1016/J.ENBUILD.2017.07.089

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. doi: 10.1016/j.comnet.2010.05.010

Bahl, V., Heile, B., & Naeve, M. (2002). Home Networking with IEEE 802.15.4: A Developing Standard for Low–Wireless Personal Area Networks. *IEEE Communications Magazine*, 40(8), 70–77. doi: 10.1109/MCOM.2002.1024418

Bayilmis, C., Erturk, I., & Ceken, C. (2003). Bluetooth Kablosuz Haberleşme Tekniği Kullanarak Veri Transferi Uygulaması. *3. International Advanced Technologies Symposium*, 305–313.

Bisdikian, C. (2001). An Overview of the Bluetooth Wireless Technology. *IEEE Communications Magazine*, 86–94. doi: 10.1109/35.968817

Castellani, A. P., Bui, N., Casari, P., Rossi, M., Shelby, Z., & Zorzi, M. (2010). Architecture and protocols for the Internet of Things: A case study. 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 678–683. doi: 10.1109/percomw.2010.5470520

Chen, E. T. (2017). The Internet of Things. *The Internet of Things in the Modern Business Environment Advances in E-Business Research*, 167–187. doi: 10.4018/978-1-5225-2104-4.ch009

Cho, J., Shim, Y., Kwon, T., Choi, Y., & Kim, S. (2007). SARIF: A novel framework for integrating wireless sensor and RFID networks. *IEEE Wireless Communications*, 14(6), 50–56. doi: 10.1109/mwc.2007.4407227

ITU G.9959, 2012. ITU Recommendation G.9959: short range narrow-band digital radio communication transceivers – PHY and MAC layer specifications.

Leung, E. (2002). ZigBee: A New Era of Wireless Communications. *China Wireless Communications*.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5), 1125–1142. doi: 10.1109/jiot.2017.2683200

Nour, B., Sharif, K., Li, F., Biswas, S., Moungla, H., Guizani, M., & Wang, Y. (2019). A survey of Internet of Things communication using ICN: A use case perspective. *Computer Communications*, 142-143, 95–123. doi: 10.1016/j.comcom.2019.05.010

Reinisch, C., Kastner, W., & Granzer, W. (2007).Wireless Technologies in Home and Building Automation. *2007 5th IEEE International Conference on Industrial Informatics*, 2, 93-98. doi: 10.1109/INDIN.2007.4384737

Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communications*, 20(6), 91–98. doi: 10.1109/mwc.2013.6704479

Shepherd, R. (2001). Bluetooth Wireless Technology in the Home. *Electronics & Communication Engineering Journal*, 195–203. doi:10.1049/ecej:20010501

Shrouf, F, & Miragliotta, G. (2015). Energy management based on Internet of Things: practices and framework for adoption in production management. *Journal of Cleaner Production*, 100, 235-246. doi: 10.1016/j.jclepro.2015.03.055

Tagami, A., & Arumaithurai, M. (2016). GreenICN Project: Architecture and Applications of Green Information Centric Networking. *IEICE Transactions on Communications*, E99.B(12), 2470–2476. doi: 10.1587/transcom.2016cni0001

Withanage, C., Ashok, R., Yuen, C., & Otto, K. (2014) A comparison of the popular home automation technologies. *2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, 600–605. doi:10.1109/ISGT-ASIA.2014.6873860