**The IOT communication technologies and applications**

**[1] Mrs.R.Sasikala,[2] Mrs.K.Susheela, [1],[2]Assistant Professor**

 **[1],[2] Department of Computer Science and Engineering(Data Science)** **Email:[1]rsgh7780@gmail.com**, **[2]ksusheela473@gmail.com**

**Abstract: Now a days T**he IOT (Internet of Things) has great importance, which results in the evolution of communication technologies to meet the needs of IoT applications. This Chapter describes the details of the communication technologies in IoT and the common domains of their application.

## Introduction

 The International Telecommunications Union defined the Internet of Things as that involving far-reaching technological and social implications to form a global infrastructure of the information society[1]. IoT uses information and communication technologies to make physical and / or virtual objects interconnect in order to provide advanced services in our professional life and daily activities[1]. The IoT is increasingly integrated in many application domains.

 The IoT environments contain many types of sensors that measure the physical parameters of the environment and transform into electrical signals and then digital messages. Furthermore, they produce a variety of data in different formats. Therefore the new technologies and new approaches must be introduced and integrated to manage efficiently these amounts of data.

 The communication technologies are evolving in order to meet the needs of the IoT Thus, a wide variety of IoT applications has been recently developed and deployed to significantly affect our daily and professional lives[2] .Despite of its success, the IoT still faces many challenges and problems. The major issues are: the management of Big Data (collection, transmission and analysis), the security and confidentiality of these data and the interoperability between the used heterogeneous technologies

 This Chapter provides an overview of the Internet of Things (IoT) by focusing on: The used communications technologies, the most popular application domains of the IoT and This Chapter is organized as follows. Section 2 lists the emerging communications technologies used in the IoT networks. In Section 3 describes a variety of application domains of the IoT and Finally, Section 4 concludes this Chapter.

## Communication technologies for the IoT

##  Mainly The IOT communication Technologies are broadly categorized into 2 types:

## Wired technologies

## Wireless technologies

### Wired technologies

 According to (Dong et al., 2019) and (Alparslan et al., 2020), the wired communication technologies that are used in the IoT networks are:

1. Ethernet,
2. HomePlug GP,
3. HomePNA,
4. HomeGrid/G.hn and
5. MoCA.

These technologies are summarized in Table 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Technology** | **Ethernet** | **HomePlug PG** | **HomePNA** | **HomeGrid/G.hn** | **MOCA** |
| Used infrastructure | Ethernet cables and jacks | Electrical wiring and power outlets | Telephone and coaxial cables, phone jacks | Power lines, coaxial cables and phone linesplastic optical fibers | Coaxial cables and jacks |
| Frequencies | - | 24 - 500kHz | 12 - 44MHz | Power lines: 100MHzCoaxial cables: 200MHz Phone Lines: 200MHz | 500 - 1650MHz |
| Range | 100 m | 300m | 300m | 100m | 90m |
| Data rate | 400 Gb/s | between 4 Mbps and 200Mbps | 320Mbps | 1 Gbps over power lines1.7Gbps over phone lines and coaxial cables | 10 Gbps |
| Latest version | 802.3cv-2021 | HomePlug GP 1.1 | HomePNA 4.0 | G.hn Wave-2 | MoCA 3.0 |
| Common Use Cases | smart home, smart offices | smart homes and offices, smart grid applications, electric vehicles | smart homes and offices | smart homes and offices, industrial applications | smart homes, buildings, hospitals, hotels and schools |

 **2.1.1.Ethernet**

 Ethernet (IEEE 802.3): It is one of the common local area network (LAN) technologies used in real life. Ethernet links several machines through twisted pair cables. The physical cabling makes this technology more secure and less vulnerable to disturbances In (Jiabul et al., 2020), Ethernet was defined as a wired technologies that can be used in Smart Homes by providing reliable and secure transmissions[3]. Besides, it is a low-cost technology with a high data rate (from 10 Mbps to several Gbps. Indeed, the latest versions of Ethernet (802.3cu-2021 and 802.3cv-2021) offer up to 400 Gb/s on single-mode fiber (IEEE et al., 2021). On the other hand, its range is limited to 100m (Jiabul et al., 2020)[3] for each cable linking two active elements (hub and switch). described the transition to the use of Ethernet in the IoT. detailed the cases where Ethernet is used in IoT applications.) presented a performance evaluation of the use of Ethernet in an industrial IoT environment.

 **2.1.2 HomePlug Green PHY (GP):**

 HomePlug Green PHY (GP): it is a power-line communication (PLC) technology. This technology uses the existing electrical wiring in a building to connect network devices. HomePlug employs powerline adapters that plugs into a power outlets and use Ethernet cables to be connected to other devices. It can be utilized, for example, with an existing Ethernet network to connect equipment in a remote room without using wireless technology. The most important advantage of the HomePlug GP[5] is its economical energy consumption[4] (Dr. Yusuf et al., 2019). Besides, it offers a data rate between 4 Mbps and 200Mbps. Its range is close to 300m (Jiabul et al., 2020). It is characterized by security, reliability, compatibility with existing infrastructure and interoperability with IEEE 1901 devices (Md. Liton, 2020). Other characteristics of this technology are represented in Table1. HomePlug GP is designed for the IoT applications, mainly in Smart Homes and smart grid applications (Dr. Yusuf et al., 2019). In addition, due to the new power management and features offered by HomePlug GP 1.1, it has been a promising alternative for green communications for electric vehicles (Pallander, 2021).

**2.13 HomePNA (Home Phone Networking Alliance):**

 It is a technology applied in home networks by reusing telephone and coaxial cables. Indeed, HomePNA networks use phone jacks, HPNA adapters and bridges with coaxial cables and telephone wiring to connect devices. Using the existing cables does not interrupt voice or television services since different frequencies are used (Table 1). HomePNA is mainly employed in Smart Homes with a range close to 300m (Jiabul et al., 2020). HomePNA, described in Table 1, offers a data rate up to 320 Mbps (HPNA 3.1) (Gianfranco et al., 2018). 4.0 version of HomePNA includes support for the G.hn standard, which makes all connections possible regardless of the type of wiring.

**2.1.4 HomeGrid/G.hn:**

 It is a technology that utilizes the existing types of domestic cabling (electrical cabling (PLC), coaxial cable and telephone lines) and plastic optical fibers , which makes it very cost effective. Indeed, a G.hn network uses adapters to connect its devices. It can be used in Smart Homes (Jiabul et al., 2020) and offices as well as in industrial applications (Zeng, 2020). It is more beneficial than HomePNA as it provides a higher data rate (1 Gbps over power lines and 1.7 Gbps over phone lines and coaxial cables) with more robust performance. However, its range is limited to 100m (Phatrakit et al., 2019). Other characteristics of G.hn are represented in Table1.

 2.1.5 **MoCA (Multimedia over Coax Alliance):**

 It is a technology that uses coaxial cables (Jiabul et al., 2020) and can be employed in Smart Homes with a very high reliability, security and data rate (Dragos et al., 2018). Its characteristics are described in Table 1. Its latest version MoCA 3.0 offers a data rate of 10 Gbps. Its range is close to 90m. On the other side, MoCA network can utilize 16 adapters simultaneously, which makes it useable in buildings, hospitals, hotels and schools. Its combination with Wi-Fi repeaters increases the Wi-Fi range in a reliable way (without loss of data rate).

**2.2Wireless technologies**

 The most widely used wireless communication technologies in the IoT networks are :

* + - 1. *RFID*
			2. *NFC*
			3. *BLE*
			4. *ZigBee*
			5. *Z-Wave*

 ***2.2.1 RFID*(Radio Frequency Identification):**

 It is used in retail applications and asset as well as in inventory tracking. It can also be used in an industrial environment to identify, in a simple and an efficient way, some measurements and information (physical location, offset measurements, identification and control of raw materials, etc.).

There are three versions of the RFID technology: 1) a passive version: It is the most economical version where the tags use the energy generated by the waves of the RFID readers since they are not equipped with an internal battery; 2) an active version where the tags are powered by their own energy sources; 3) a semi-passive version in which the tags utilize their own energy sources and the energy generated by the RFID readers.

**Figure1. (a)** RFID Systems Architectures

**2.2.2.NFC((Near Field Communication):**

It is a communication technology in which two devices can exchange information (Figure 1(b)) by a wireless link at a short distance equal to 4 centimeters. Its basic structure components are the same as that of RFID. In fact, an end node in an NFC system can be: i) an NFC tag: a transponder that stocks data and sends it after receiving a signal from a reader, ii) an NFC Reader: atransceiver that reads data from tags, or iii) a device that combines both an NFC reader and an NFC tag. The proximity between the devices that communicate with the NFC reduces the risk of hacking. For this reason, the NFC is commonly used in electronic payments and tickets. This technology is also supported by several devices that use Android and IOS systems.

***2.2.3* BLE (Bluetooth Low Energy):**

 It is a short-range wireless network technology employed in Personal Area Networks (PAN). BLE is a version of Bluetooth standard designed to transmit / receive small amounts of data while consuming extremely low amounts of energy. Its possible architectures and end nodes (devices equipped with BLE technology) are represented in Figure 2. The first possible architecture, called Point-to-Point (Figure 2(a)), creates direct communications between two BLE nodes. In a star architecture (Figure 2(b)), the BLE network includes a number of end nodes connected to the BLE Central Master. It can represent a bridge to the outside of the network. In a mesh architecture (Figure 2(c)), the network contains full-interconnected BLE end nodes.

In fact, the BLE is supported by several operating systems (Linux, Windows, macOS, Android and IOS). Thanks to the simplicity of its implementation, it is widely used to transmit sensor data. This technology is essentially applied in Smart Home, smart wearable devices, smart health and retail. Indeed, it makes it possible to transmit data from portable devices (fitness, medical, Smart Home, etc.) to smartphones. Table 2 presents the characteristics of BLE.

**2.2.4 ZigBee (IEEE802.15.4):**

 It is a medium range technology designed for economical wireless networks with a low power consumption. This technology can put objects in a dormant state if necessary. ZigBee is used mainly in Smart Homes since it connects the nodes that are nearby the medium range. Its architecture is represented in Figure 3. Its main components are: i) ZigBee Coordinator, ii) ZigBee end nodes (which are devices equipped with ZigBee technology) and iii) ZigBee Routers that act as intermediates between end devices and the coordinator. The ZigBee Coordinator is the only device that can form and start the network. Other devices can join the network after sending requests. In addition, the coordinator may function as a bridge to other networks. Zigbee network must have one coordinator

 ZigBee offers robust and highly secure operations and facilitates the addition or removal of network objects. However, adding a new device requires checking its compatibility with the current components of the network. As the ZigBee is available in an open source, it can be modified to be adapted to particular devices although the latter cannot communicate with other network components. Another disadvantage of the ZigBee is the signal disturbances since it uses a frequency that includes other technologies and equipment in the same environment (e.g. WiFi, Bluetooth, microwaves, etc.). The Zigbee Alliance announced its most recent IP standard, Matter, to simplify and harmonize the IoT. It is a secure connectivity standard that solves the problem of interoperability in Smart Homes. Indeed, the objective of this standard consists in making a greater number of connected objects interoperable by creating an IP-based interoperability layer at the application layer.

**2.2.5 Z-Wave**

 it is a communication technology designed primarily to automate home. Indeed, it can make objects communicate effectively with one another with low energy consumption. Moreover, Z-Wave facilitates the addition of a new compatible device since it adds another mesh to the network. Unlike the ZigBee, the Z- Wave is less disturbed by other devices since it uses a frequency of 868 MHz. The Z-Wave architecture is shown in Figure . It contains two types of components: i) Z-Wave slaves (which are the end devices equipped with ZigBee technology using the network to communicate) and ii) Z-Wave controller (which is the component that organizes the network and controls all other devices to work together).

**Characteristics of Wireless Technologies:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Technology** | **BLE** | **NFC** | **RFID** | **Z-Wave** | **ZigBee** |
| Category | WPAN | Near Field | Near Field | WPAN | WPAN |
| Frequency | 2.4 Ghz | 13.56 MHz | 13.56 MHz | 868 MHz | 868 MHz (EU), 2.4 GHz |
| Power Consumption | Very low | Very low | Very low | Low | Low |
| Range | From 50 to 150 m (70m typical) | 10 cm (4cm is the optimal range) | 100m (active tags), 25m (passive tags) | 100m | From 10 to 100m |
| Data rate | 1 Mb/s | 100-420 kbps | 500 Kbps | 100 oKbps | 20 kbps (868 MHz), 250kbps (2.4 GHz) |
| Maximum Transmission Unit | 251 bytes |  | 16-64 Kbps | 255 bits | 100 bytes |
| Bidirectional Communication | yes | yes | yes | yes | Yes |
| Topology | Point to point , star and mesh (Bluetooth MESH) | Point to point | Point to point, star | Mesh | Mesh |
| Scalability (devices) | 5917, 50 (mesh) | 2 | limited | 232 | 65 000 |
| Mobility Support | yes | yes | yes | yes | Yes |
| Direct Internet Access | no | no | no | no | No |
| Common Use Cases | Smart home, smart wearable devices, smart health, retail | Electronic payments and tickets | Retail applications, asset and inventory tracking | Medium-range IoT applications whose nodes are nearby. For example: home automation | Medium-range IoT applications whose nodes are nearby. For example: home automation |

**The Other Communication technologies in an IOT are given below:**

**WiFi (Wireless Fidelity):** It is widely used since it makes objects connect to each other or directly to the Internet. The Figure exposes the architecture of a use case of WiFi in an IoT network. The components represented in the figure are: i) End nodes (WiFi devices that ensure communication); ii) WiFi Mesh Routers (the routers that transmit data between end nodes and the gateway to another network (Internet). These routers can communicate with each other in a mesh topology); and iii) WiFi Mesh Router with Gateway (a router that acts also as a gateway to other networks). WiFi is efficiently used to transfer files thanks to its ability to handle large amounts of data. It is mainly characterized by its fast transfer speed[1]. However, it has limits in terms of range and power consumption. Its best use cases are Smart Home and smart retai

.

**LoRaWAN**: It is a LPWAN (Low-Power Wide Area Networks) technology that provides long-range communications with low power consumption. LPWAN technologies are adequately used in applications that do not require high data rate and are not time sensitive. They are generally employed in [6]large industrial and commercial environments. They are also utilized in smart city, building and agriculture applications. LoRaWAN is a technology that transfers data from terminal nodes to the central server, via gateways, by a single hop. It is developed to support LoRa over the Internet. Its architecture is shown in Figure where the typical system architecture of a LPWAN is represented. Its main components are: i) end nodes (the end devices that communicate data); ii) network server (the central point of the network that aggregates data and acts as an intermediate with application servers); iii) LPWAN gateways (the devices that communicate data between terminal nodes and the central server); and iv) application servers (the servers that run applications using the network data).



* Sigfox: It is an LPWAN technology that ensures the transmission of small amounts of data. Initially, Sigfox supports communications from terminal nodes to base stations. However, it is not efficient for communications in the opposite direction (from base stations to terminal nodes). Later versions support two- way communication between terminal nodes and base stations. The architecture of Sigfox is the same as that of a general LPWAN
* . **NB-IoT (Narrowband IoT):** It is an LPWAN cellular technology designed specifically for IoT networks. It efficiently connects the IoT devices over mobile networks by processing small amounts of bidirectional data in a secure and reliable manner. It is optimized to exchange small amounts of data in networks using a large number of devices and over long periods. NB-IoT architecture is depicted in Figure 7. Its main components are: i) end nodes (the end devices that generate data to be sent to the base stations and can receive data from them); ii) evolved base stations (the base stations that control the end devices, communicate with them and relay data to IoT Evolved Packet Core);IoT Evolved Packet Core (EPC) (the component that connects the network with IoT platform and application server); (iv) application server which is the server that hosts and runs applications; and v) IoT platform (a set of components that facilitate the interactions between the IoT EPCs and the application server and orchestrates the data movements). 
	+ **NB-Fi (Narrowband fidelity):** It is an LPWAN technology designed for bidirectional communications between machines (M2M). It is characterized by low power consumption. NBi-Fi provides robust and reliable communications and uses artificial intelligence techniques to improve its performance and to avoid interference. NB-Fi network has the same architecture of a LPWAN .
	+ **DASH7**: It is an extension of the RFID. It offers communications with low latency and high flexibility. DASH7 provides multi-hop communications and supports object mobility up to 2 km range. The DASH7 architecture, which is similar to LoRaWAN, is represented in Figure 6. Table 4 includes the characteristics of DASH7.
	+ **Cellular (3G/4G/5G)**: These technologies provide high data rate and reliable communications over long distances. Moreover, they require very high operating costs and energy requirements. An example of the architecture based on 5G used in the IoT is presented in Figure 8. It is composed of : i) end nodes (the end devices equipped with 5G technology; ii) Gateways (the devices that connect the 5G network to other IoT networks); and iii) 5G Base Station which is the component that connects other devices (end nodes and gateways) to the Internet. Table 4 enumerates the characteristics of the 5G. Although the 5G offers several advantages (e.g. considerable improvement of the data rate and the reduction of latency). The next version (the 6G) was developed to introduce a communication standard of new generation with more advantages and enhanced capacities.

****

* **LiFi (Light Fidelity):** It is a visible light (VLC) wireless communication technology that uses visible light to transmit data. LiFi is a promising technology for the IoT networks since it makes the latter meet their requirements (a high data rate, high power efficiency, high security, no interference, more reliability, low cost, etc.) even with a large number of connected devices (Ahmad et al., 2020) (Qusay et al., 2020). In fact, it avoids the negative impact of radio frequency (RF) on the human health and reduces carbon emissions. In addition, it can be used simultaneously for communication and lighting. However, this technology suffers from limited range and high vulnerability to interruptions (light cannot pass through obstacles). Therefore, it cannot be used in environments where there are other light sources. For this reason, the LiFi technology can be used only in specific fields where it coexists with other technologies since it cannot completely replace them (Ahmad et al., 2020). Figure 9 presents a scenario that combines both the WiFi and the LiFi technologies. This network is composed of: i) end nodes (the end devices that communicate data); ii) Relay/Amplification devices (the components that relay data between end devices and the LiFi Access Point and can amplify the signals while transmitting the data); iii) LiFi Access Point (the device that aggregates data from LiFi devices and transmits it to WiFi Access Point); and WiFi Access Point (the device that connects other devices to a public network).

****

**Comparision Between wired and wireless technologies**

This comparison demonstrates that wired technologies are characterized by lower power consumption and ensure faster and more secure transmissions, comparedto the wireless technologies[8]. Indeed, the use of wires makes it possible to create connections with high data rate and more reliability. However, wireless technologies reduce the data rate and can cause reliability problems in real time because of the errors caused by interference, noise and collisions. In addition, they are highly sensitive to intrusion and hacking, which makes wired technologies more secure. Despite these disadvantages, wireless technologies have some advantages. For instance, they create networks with longer ranges, compared to the wired technologies. These wireless networks are also more scalable and more flexible since new objects and mobile devices can be easily added and a greater number of connected objects can be supported using these technologies In addition, they are less expensive and time-saving since they do not require the installation of many equipment and because of their easy remote maintenance. Moreover, without wires, the risk of failures and dangers can be minimized since their use can sometimes be dangerous, especially in high-temperature environments. All these advantages make wireless technologies[9] a good choice for IoT networks. According to (Dong et al., 2019), wireless communication technologies were behind the development of the IoT since they improve its system flexibility and scalability by providing long-range and low-power communications.

 In the below table Comparison between wired and wireless communications technologies ("+" means "more advantageous" and "-" means "less advantageous")

|  |  |  |
| --- | --- | --- |
| **Criterion** | **Wired technologies** | **Wireless technologies** |
| **Range** | **-** | **+** |
| **Data rate** | **+** | **-** |
| **Management of mobile nodes** | **-** | **+** |
| **Power consumption** | **+** | **-** |
| **Reliability** | **+** | **-** |
| **Security** | **+** | **-** |
| **Costs** | **-** | **+** |
| **Scalability** | **-** | **+** |
| **Flexibility** | **-** | **+** |
| **Speed of installation** | **-** | **+** |
| **Ease of maintenance and reconfiguration** | **-** | **+** |
| **Risk of failures** | **-** | **+** |
| *Danger of use* | **-** | **+** |

From the above-presented comparisons we can deduce that wireless communications technologies are better suited for IoT environment.

## Application domains of the IoT

## we will present the most popular application domains of the IoT [10]and their most important challenges

* Smart City: is used in many domains such as public safety, greening the environment, smart lighting, traffic management, private and public transport traffic, efficient management of waste, etc. Thanks to this development, cities become smarter by offering more high-quality services and reducing their expenses (Dr. Yusuf et al., 2019).
* Smart Home: Authors, in (Dr. Yusuf et al., 2019), defined Smart Home as a residence equipped with IoT technologies. Its equipment is connected to the Internet in order to control continuously and remotely the various activities of the residents based on data collected from the deployed sensors. Indeed, it offers a better quality of life with more safety and comfort.
* Smart Building: The IoT can make buildings smart by benefiting from its solutions in terms of monitoring and management. Moreover, the integration of the IoT allows reducing the operating and maintenance costs of the buildings to better satisfy the occupants by guaranteeing their safety and minimizing the environmental impact of the buildings in terms of energy, water consumption and waste production.
* The Educational Internet of Things (EIoT): It is used to apply IoT technologies in education and learning. In fact, carrying out the learning process via the IoT makes it possible to build intelligent educational environments (intelligent technologies, intelligent objects and intelligent pedagogy) to make it more productive and more efficient.
* The Agricultural Internet of Things: Recently, the agriculture has become more industrialized to improve production quality and quantity by integrating the Agricultural Internet of Things (AIoT) that consists in using the IoT technologies to modernize and enhance the various application fields of the agricultural sector. AIoT can improve the agricultural productivity and minimize the human intervention and workforce.
* The Industrial Internet of Things (IIoT): It consists in using the IoT technologies in an industrial environment. It is employed to equip the industry with sensors and actuators in order to obtain automated intelligent objects that detect and communicate real-time events (Wazir et al., 2019), receive orders and act by applying the recommended actions.
* The Medical Internet of things (MIoT): It is based on integrating the IoT technologies in the healthcare sector. In this context, (Fadi et al., 2020) defined the MIoT network as a network of people and medical devices that interchange health data through wireless communication. Therefore, the MIoT improves the quality of medical treatment, reduces healthcare costs and creates more efficient medical systems (Mohan, 2020) (Fadi et al., 2020).

The Energy Internet of Things (EIoT): It applies the IoT technologies in energy distribution networks. In a smart and efficient way, the IoT facilitates the collection, exchange and use of data. It accelerates the integration of renewable energy. In fact, an efficient localization method should be applied in this type of networks

* The Internet of Battlefield Things (IoBT): It consists in applying the IoT in the military domain. In other words, devices used in the world of defence and military battles become intelligent as they can communicate with each other. As a result, they become more efficient as they improve the operational efficiency of military applications.
* The Commercial Internet of Things: (Henner et al., 2020) defined the CIoT as the use of IoT devices to purchase products and services online in order to give new opportunities to retail customers. In fact, the IoT affects all stages of the buying process during the interactions between the client and the seller or manufacturer.
* The Social Internet of Things (SIoT): It is the combination of social networks with the IoT technologies. In fact, the SIoT networks include intelligent objects considered social as they mimic the human behavior in social networks. Therefore, these objects can create their social networks (Mozhgan et al., 2020) by making relations and, thus, constructing social structure.
* The Green Internet of Things (GIoT): It is a version of the IoT that involves energy efficient features and environmental conservation activities. It ensures greener and healthier environment. First, the GIoT aims at reducing energy waste and minimizing energy consumption (Rafeeq, 2019). The GIoT technologies are also employed to significantly decrease the emissions of toxic pollutants such as carbon dioxide (CO2)) and the greenhouse effect caused by the IoT systems (Albreem et al., 2021).

The common challenges and application issues[11] for the different versions of the IoT can be summarized as follows:

* Management of large amounts of generated and communicated data by collecting, analyzing and transmitting them.
* Security and confidentiality of the transmitted and stored data: consist in protecting IoT environments against possible threats.
* Considering the heterogeneity of the used technologies: The hardware and software installations implemented must guarantee compatibility and interoperability between the many used technologies.
* The scalability and connectivity of the IoT networks: are ensured by implementing scalable solutions to meet the future needs of networks where the number of connected objects is growing exponentially.
* Optimization of energy consumption: The deployed solutions and the used technologies must consume these resources in an optimized manner.

## Conclusion

The success and benefits of the IoT lead to its rapid emergence in our domestic and professional life. Therefore, research works and technological innovations has recently evolved in order to address the different application domains. In fact, this paper presented a review describing the communication technologies used in the IoT networks. These technologies and their common use cases were compared. Subsequently, a variety of IoT application domains were listed. Moreover, each IoT application domain was depicted and examples of its use cases as well as its common challenges and problems were illustrated. Moreover, some recent research studies dealing with the IoT were summarized. We noticed that these application areas have the same challenges which consist in the management of Big Data (collection, transmission and analysis) as well as the security and confidentiality of these data and the interoperability between the heterogeneous used technologies. In this context, numerous intelligent methods can be applied to solve these problems. In fact, numerous intelligent and hybrid artificial intelligence-based methods were introduced and investigated the resolution of engineering real-world problems, especially IoT applications and issues (Mnasri et al., 2017) (Mouhammd et al., 2015) (MNASRI et al., 2020) (Hassanat, 2018) (Tarawneh et al., 2018) (MNASRI et al., 2018) (Hassanat et al., 2015). Most of these studies confirmed the complexity of IoT problems and highlighted the need for innovative methods to resolve IoT related challenges. As a continuation of this work, we will focus on the challenges and the unsolved problems of the IoT in order to explain them and propose promising ideas to find solutions.

**References**

[1] . Mnasri S., Adrien van den Bossche, Nejah Nasri, Thierry Val. The 3D Redeployment of Nodes in Wireless Sensor Networks with Real Testbed Prototyping. International Conference on Ad Hoc Networks and Wireless (AdHoc-Now 2017), Sep 2017, Messina, Italy

[2]. Alparslan S., Alexios L., and Ismail B. Industrial Networks and IIoT: Now and Future Trends, pages 3–55. 07 2020.

[3] Jiabul Hoque and Md Ahmed. Smart home: An empirical analysis of communication technological challenges. European Journal of Engineering Research and Science, 5:571 – 575, 05 2020.

[4] Gianfranco C., Giovanni M., Gaetano P., Bruno R., and Luigi S. Chapter 4 - iot and sensor networks security. Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, Intelligent Data-Centric Systems, pages 77–101. Academic Press, 2018.

 [5] Dr. Yusuf P., Majzoob O., Osama S., Hani H., and Mohammed A. The future of internet of things (iot) and its empowering technology. Volume 9: Pages 20192 – 20203, 03 2019.

 [6] Md. Liton, H. 2020. « Control of a Multilevel Inverter for Wind Energy Conversion System with Energy Storage and Condition Monitoring Options. ». Doctoral thesis, Curtin University.

 [7] Pallander, R. (2021). Implementation of HomePlug Green Phy standard (ISO15118) into Electric Vehicle Supply Equipment (Dissertation). Doctoral thesis, Lulea University of Technology.

 [8] Phatrakit P., Watchara W., Bunyawat V., and Chatkaew C. Review of the lightning electromagnetic impulse protection measure for smart home and building in smart grid system in thailand. volume 14, 2019.

 [9] Zeng, Tony. (7 February 2020). Use of G.hn in Industrial Applications (1). International Telecommunication Union. https:/[/www](http://www.itu.int/pub/T-TUT-HOME-2020-1).[itu.int/pub/T-TUT-HOME-2020-1](http://www.itu.int/pub/T-TUT-HOME-2020-1)

 [10] Dragos Mocrii, Yuxiang Chen, and Petr Musilek. Iot-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1- 2:81–98, 2018.

[11] Rafeeq Ahmed. Green iot - issues and challenges. 02 2019. Albreem M. A., A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M.

[12] N. Mohd Yasin. Green internet of things (giot): Applications, practices, awareness, and challenges. IEEE Access, 9:38833– 38858, 2021.

[13]MNASRI S., N. NASRI, A. VAN DEN BOSSCHE and T. VAL,

"3D indoor redeployment in IoT collection networks: a real prototyping using a hybrid PI-NSGA-III-VF," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018, pp. 780-785, doi: 10.1109/IWCMC.2018.8450372.

[14] Hassanat A. B. A., M. Alkasassbeh, M. Al-awadi and E. A. A. Alhasanat, "Colour- based lips segmentation method using artificial neural networks," 2015 6th International Conference on Information and Communication Systems (ICICS), 2015, pp. 188-193, doi: 10.1109/IACS.2015.7103225