Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi
International Journal of Engineering Research and Development
UMAGD, (2023) 15(1), 333-343.
10.29137/umagd.1063036
Cilt/Volume:15 Sayı/Issue:1 Ocak/January 2023
Araştırma Makalesi / Research Article

Comparison of IoT Protocols with OSI and TCP/IP Architecture

Füsun Yavuzer Aslan[1], Bora Aslan [1*]

[1] *Department of Software Engineering, Kırklareli University Kırklareli, TÜRKİYE*

***Başvuru/Received**: 25/01/2022* ***Kabul / Accepted**: 14/11/2022* ***Çevrimiçi Basım / Published Online:** 31/01/2023*
***Son Versiyon/Final Version**: 31/01/2023*

Abstract
ARPANET, which was created in 1969 with the idea of having only a few systems connected at the beginning, has today become a vast separate world where billions of computers and systems come together. Internet speed, capacity and traffic have grown exponentially. Today, the mobile devices that almost everyone carries in their pockets have had superior capabilities than the supercomputers of 20 years ago. Now, human beings can make almost all devices smart thanks to microsensors and smart chips. With smart phones, cars and heating systems have become easily controllable and programmable. Every year, new devices in different forms with increasing talent and intelligence are introduced and adopted. An increasing number of M2M applications, such as smart meters, healthcare monitoring, transportation and packaging, or asset tracking, make a significant contribution to the growth of devices and connections.

In this research, which takes into account newly developed technologies, interoperability and compliance with standards are examined. IoT architectures are examined and the currently accepted five-layer architecture method is compared with OSI and TCP/IP architecture. In addition, IoT protocols are mapped with OSI and TCP/IP architecture. Furthermore, technologies used in the context of the IoT are combined with OSI and TCP/IP architecture, to provide an integrated view.

Key Words
"Architecture, IoT, Network, OSI, Protocols, TCP/IP"

**** Corresponding Author:** bora.aslan@klu.edu.tr*

1. Introduction

With the development of sensor and communication technologies in the last decade, applications built within the framework of IoT (Internet of Things) have begun to take place in our lives discreetly and slowly. The number of objects classified as devices and connections is growing worldwide faster than the world's population. Smart meters, healthcare monitoring, shipping and packing, and asset tracking are just a few of the M2M (machine-to-machine) applications that contribute to the expansion of devices and connectivity. IoT is a network of devices that share information and communicate through various communication protocols. Many sources state that IoT is a system that uses information and communication technologies to facilitate more effective and interactive use of vital infrastructure and services such as education, health, security and transportation. Current applications that we can increase the possibilities in all areas of our lives with the Internet of Things include a wide industrial area, starting from smart homes, cities, factories, and applications in different health and agriculture fields (Ercan & Kutay, 2016).

IoT applications are rapidly moving towards becoming indispensable objects of our lives. Figure 1 shows the distribution of 1414 IoT projects launched on the market in 2020 per sector. Looking at the graph, we can see that most new products related to industrial manufacturing, transportation, energy, retail, and urban planning applications (Scully, 2020).

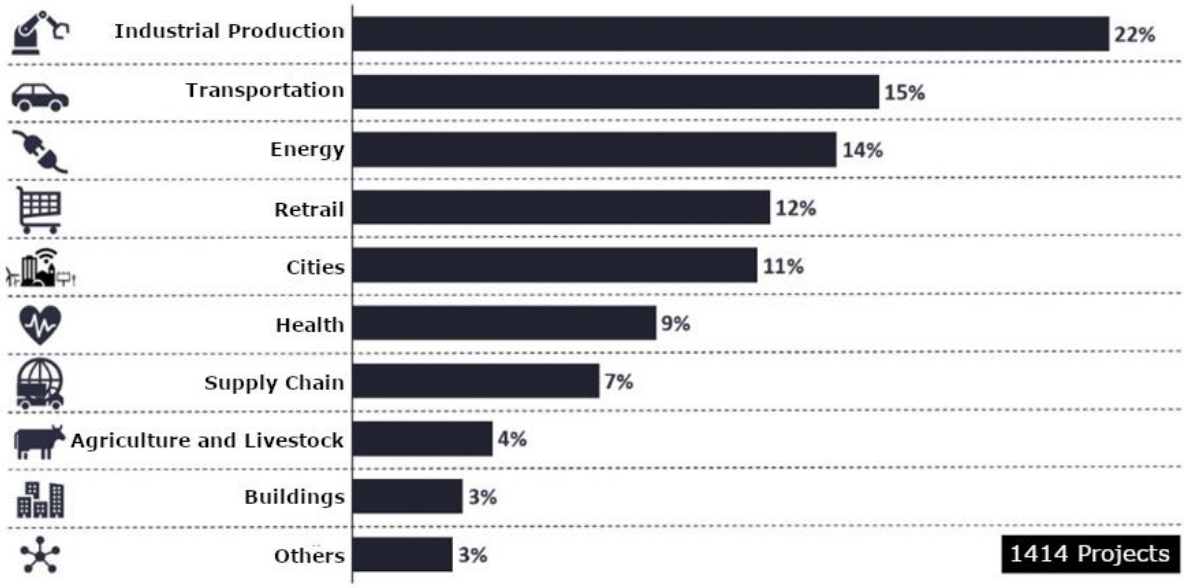

Figure 1. Sectoral distribution of IoT projects in 2020

The manufacturing industry is undergoing a significant transformation led by IoT applications. Satya Nadella, a Microsoft executive, suggested that IoT applications transform manufacturing rules, accelerate the development of digital factories, and improve operational performance (Forbes, 2018). In line with available data, autonomous vehicles equipped with IoT technology dominate the transportation sector. Furthermore, battery monitoring, tire pressure tracking, driver surveillance, and fleet management are widely used applications in this field. According to Martin Lundstedt, a Volvo executive, solutions connected with IoT applications improve safety for drivers, operators, and other users while lowering carbon dioxide emissions worldwide (TU Automotive, 2019). Energy-related projects focused on smart energy distribution, grid optimization, remote asset management and monitoring, maintenance forecasts, and increasing consumer transparency.

IoT solutions applied in the retail sector include in-store digital signage, customer tracking and feedback, product tracking and inventory management, smart vending machines as well as smart shelves, and lastly, self-checkout markets. Smart cities are one of the most promising areas for IoT applications, as they immediately impact the lives of millions of people. Smart parking, traffic management, smart garbage collection systems, smart lighting, public safety measures, and air pollution control systems are examples of applications in this area. The IMD (International Institute for Management Development) Smart City Index 2019 report includes smart cities, focusing on people's perceptions of balancing the economic and technological aspects of their cities with humanitarian elements. As stated in the report, the top 10 cities are Singapore, Zurich, Oslo, Geneva, Copenhagen, Auckland, Taipei, Helsinki, Bilbao and Dusseldorf, respectively (Bris, 2019). IoT applications in healthcare have started to attract attention recently. Various applications, such as remote health monitoring, digital diagnostics, and robotic assistance are becoming increasingly popular in this field. In addition, end-user products classified as health products are growing in several fields, such as sports and personal care. Overall, these products are aimed at improving the quality of life. One of the new trends in healthcare is monitoring the pandemic through IoT applications during the COVID-19 era (World Medical Innovation Forum, 2020). Logistics providers are increasingly utilizing interconnected digital solutions to overcome complexity while performing supply chain procedures. Since the establishment of the first IoT applications as

product tracking systems via RFID systems, the supply chain and logistics sectors have been enriched in various IoT applications. Asset tracking, cold chain tracking, status monitoring, inventory and warehouse management, and autonomous vehicles are projects in this field. Creating smart agriculture technology is very important since humanity will need more food as the world population increases. IoT applications can help farmers make decisions that result in higher yields and quality and more cost-effective farming by reducing the use of fertilizers and pesticides (I-CIO, 2018). Precision agriculture, livestock tracking, irrigation management, smart mapping, smart spraying systems, and the use of unmanned aerial vehicles are examples of smart agriculture initiatives. Smart buildings and home automation are two examples of long-standing and widely used IoT applications. Smart lighting, elevator monitoring, smart smoke and fire extinguishers, facility automation for building security, and building monitoring systems are examples of common building or residential projects. Big companies like Google, Amazon, and Microsoft offer smart home control systems that are among the most popular products on the market.

Regardless of the success and rise it has achieved in recent years, as in every concept, the concept of IoT also contains some fundamental and conceptual problems in terms of performance and management (Erdal & Ergüzen, 2020). IoT applications are creating a whole slew of new issues in such a vast and unpredictable ecosystem. The issues that the emerging computing world is facing are listed and briefly explained below (Kim & Solomon, 2016).

- *Security issues:* The more people, businesses, and countries become more dependent on IoT applications, more hackers and malicious actors aim to access and steal information.
- *Privacy issues:* The majority of IoT applications collect and process data to improve people's lives. Privacy issues arise as most of this data can be classified as personal information.
- *Interoperability and standards problems:* While the Internet uses TCP/IP infrastructure and a server/client architecture, various non-standard protocols have been established in IoT applications for low-processing-capacity objects to improve their communication and efficiency of their data transfers. The diversity of standards leads to interoperability problems.
- *Legal issues:* Legal regulations have lately surfaced in order to address issues with data ownership acquired by IoT applications. National studies of countries on this subject may be insufficient for global IoT applications.
- *Economic development problems:* IoT applications and accompanying technologies are drastically changing the economy. Dark factories, unmanned transportation, and means of transportation are believed to pose serious development challenges. These technologies reduce the need for labor, in other words, increase unemployment or pave the way for new business sectors.

2. IOT Architectures

Reviewing the literature, there is no widely validated architecture for IoT, such as TCP/IP or the OSI reference model. Different researchers have proposed different architectural models (Sethi & Sarangi, 2017). Accordingly, the proposed architectural models are given in Figure 2. We can see the perception and network layer at the lowest layer of all proposed approaches, and the application layer at the upper layers. These layers have similar general characteristics and functions. A support layer has been proposed between the application and the network layer in a four-layer architecture. In the five-layer architecture, a middle layer has been added between the network and application layers, and the business layer has been added as the top layer.

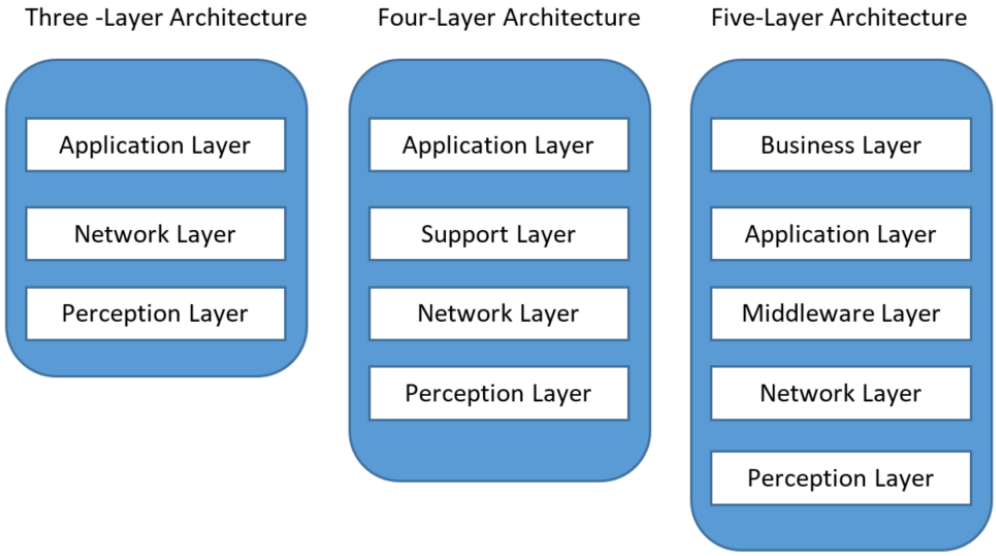

Figure 2. IoT architectures in the literature

Three-Layer Architecture is a simple model from which certain core IoT solutions can be developed. It has perception, network and application layers to collect, transmit and process data. However, in some sectors, such as healthcare, this simplistic approach cannot achieve the required level of reliability and safety. This architecture was discovered early in the IoT research process. It has three layers: perception, network and application (Wu et al., 2010). The perception layer is physical and contains sensors that detect and collect data about the surroundings. For this reason, it's also known as the device layer in some sources. Its primary purpose is to identify the object and collect data. Barcode labels, data matrix codes, and associated readers, RFID tags and reader/writers, camera, GPS, sensors, terminals, and sensor networks are all part of the Perception Layer. Data gathered by sensor type and application can be object information, location details, humidity, temperature, motion, acceleration, vibration, direction, changes in the air, etc. After that, the data is sent to the network layer for further processing. The perception layer works basically the same for the three models given in Figure 2. The network layer's primary task is to transfer and process information collected from the perception layer. For this reason, it is also called the transmission layer. Information transfer occurs at this layer using infrastructure including the internet, mobile communication networks, satellite networks, and wireless networks. Another responsibility of this layer is to interconnect other things, network devices and servers. While transferring data, it is possible to work on data too. The transmission medium can be wired or wireless. Besides, depending on the sensor structures, 4G, UMTS (Universal Mobile Telecommunications System), Wi-Fi, Bluetooth, Infrared, ZigBee etc., communication mediums can be used. The network layer divides the message into packets and uses IPv4 and IPv6 addressing techniques to route the packets from source to destination. The network layer fundamentally functions fully in the three models given in Figure 2. The application layer is responsible for providing IoT application-specific services. Different protocols may be required for each application. As a result, proprietary and non-standard protocols on the application layer are application-specific.

Layers in the four-layer architecture approach are perception, network, support, and application. Compared to the three-layer architecture, a support layer has been added between the network and application layer to enable cloud computing technologies. Also, this layer aims to process data and provide partial security. The perception layer consists of physical objects as in a three-layer architecture and functions for the same purposes. The network layer's main job is to transmit and process information collected from the perception layer; therefore, its role is identical to that of the three-layer architecture. The support layer is being used to ensure that data is transmitted between the application and the network layer more safely and dependably. Objects are typically supported at this stage by cloud and edge computing technologies. The data is processed and sent to the lower or upper layer. Devices of IoT applications utilize UDP throughout the communication. UDP is a faster but unreliable protocol than TCP. The support layer usually has a DTLS-based security mechanism. The application layer is responsible for providing IoT application-specific services. Different protocols may be required for each application. As a result, proprietary and non-standard protocols on the application layer are application-specific.

Layers in the five-layer architecture approach are perception, network, middleware, application and business. In this approach, the data processing workload of the system has been shifted from the application layer to the middleware layer, which is added between the network and application layers. Data can be processed before or after transmission through the network in this way. The business layer has been added to the top layer of the five-layer architecture. Operations such as IoT application scalability, interoperability, data flow control, and data analysis for further interpretation can all be performed using this layer. The big data generated by IoT devices can be addressed in this way. The role and content of the perception and network layers are the same in this architectural approach as they are in the three and four-layer architecture models. The middleware layer is also known as the intermediate layer. Different types of services can be provided by devices utilized in IoT applications. Devices may only interact and communicate with other devices that provide the same service type in some instances. Large volumes of data from the transport layer can be stored or processed using middleware layer technology. In this layer, one can also administer and provide a variety of services. This layer can use various technologies, including databases, cloud computing, and big data processing modules. The purpose of this layer is to send meaningful data to higher layers and organize data from the upper layers so it can be sent to lower layers. The application layer is in charge of offering IoT application-specific services. Different protocols may be required for each application. As a consequence, custom and non-standard protocols on the application layer work for the application specifically. The business layer is in charge of managing the IoT system in general. Different business models, graphs, flow charts, and specifications for direct application management are created by planning based on data obtained from the lower layers. Sound business models, as well as protocols and technologies, are required for the real success of IoT technology. Data and results may be analyzed, and future actions and business plans can be defined, thanks to the systems that will be developed in this layer.

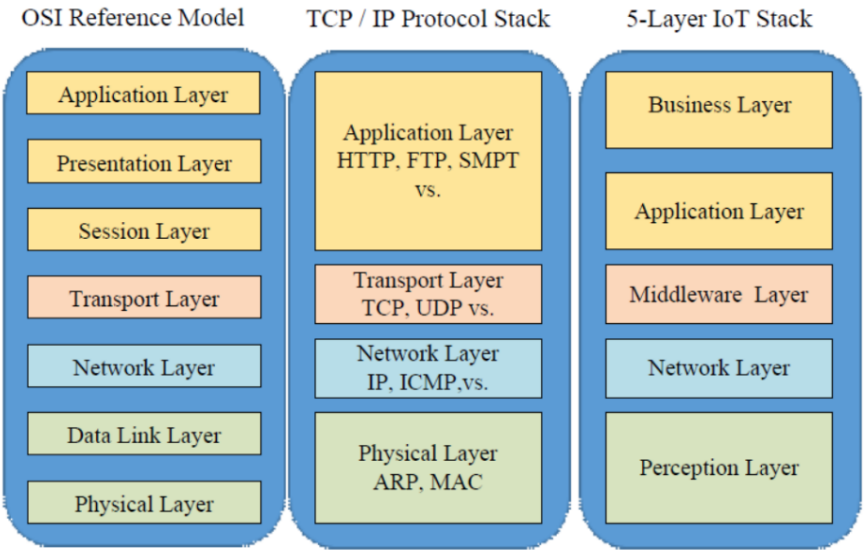

Figure 3. Comparison of OSI, TCP/IP and five-layer architecture

The OSI reference model was first established in the late 1970s and has been the standard since 1984. TCP/IP architecture was created in 1973 and declared as the ARPANET standard protocol in 1983. These two architectures are still used as the internet's primary protocol today. The quest for architecture in this domain persists, with both the growth of IoT applications and the development in the number of devices connected to the internet or network, yet, no standard has been established. The five-layer architecture and the rise of the IoT ecosystem have been acknowledged as the generated data being classified as big data. In Figure 3, a comparison of the OSI model, TCP/IP architecture and five-layer architecture is given. Hereunder, the following expressions can be stated:

- The physical layer in TCP/IP corresponds to the perception layer in IoT architecture, which performs similar functions.
- Considering general characteristics, the network layer in all models conducts similar tasks,
- Although the transport layer corresponds to the middleware layer, there are some differences. The essential distinction is that you can process and transmit data in IoT applications, particularly at the beginning of data transfer,
- The DTLS and TLS protocols provide security for TCP and UDP packets in a five-layer IoT architecture, exactly as they do for TCP/IP.
- In addition to the application layer, the business layer has been added to the top layer of TCP/IP.

3. Protocols in IOT Applications

In IoT applications, many technologies such as IPv6, 6LowPAN, ZigBee, Bluetooth, Wi-Fi, LoRaWAN, Z-Wave, NFC, and Sigfox are used for devices to communicate with each other. Most of the technologies described are found in IoT architectures' network layer. In fact, in IoT applications, some technologies that are immediately related to computer networks naturally attract attention. However, these technologies can fall short of IoT components. In the next five years, this scenario will lead to the introduction and standardization of many protocols and technologies ideal for IoT applications. The protocols utilized in IoT applications are explained in this section of the study to give a broad perspective, and then OSI and TCP are compared.

3.1. IEEE 802.15.4

IEEE 802.15.4 is known as a standard protocol built for LR-WPAN (Low-Rate Wireless Personal Area Network). LR-WPAN is a form of network used in IoT applications to transfer data between devices. The capacity to function in short distance communication at low power and data rates wirelessly is the most crucial attribute that differentiates it from other LAN and WAN technologies (Chen et al., 2010). IEEE 802.15.4 offers a low-cost communication network for low-power, low-speed devices, and also provides simple and easy setup, accurate data transmission, relatively low cost, and long battery life. In the 2.4 GHz ISM band, the IEEE 802.15.4 protocol permits transmission at a speed of 250 kbps across 16 channels.

Most of the IoT protocols discussed in this section of the article employ IEEE 802.15.4 as their physical layer. IEEE 802.15.4 has a 2-layer structure as physical and data link layers. The physical (PHY) layer is responsible for signal transmission to the MAC sublayer. This layer performs bitwise actions, including wireless signal channel changes, bit modulation, and packet synchronization. Connecting and disconnecting devices from the network, overseeing access control to shared channels, and transferring data to the upper layer and lower layer properly are among the main responsibilities of the MAC sublayer. The MAC sublayer and the LLC sublayer are combined together and called the data link layer. LLC is common to all IEEE 802 standards. LLC, on the other hand, may be overlooked when developing IEEE 802.15.4-based applications.

3.2. 6LoWPAN

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is an open-source protocol not designed to send data through LR-WPAN to IPv6-enabled devices produced by IETF. Theoretically, the goal of the production is to connect small devices that have limited processing power and low energy consumption to the internet (Shelby & Bormann, 2011). A device with 6LoWPAN support can connect directly to the internet. Within the 6LoWPAN protocol, each device on the network should have an IPv6 address. It is ideal for applications that need a low-data-rate wireless internet connection. 6LoWPAN operates in a frequency range of 868 MHz to 2.4 GHz and a data-signaling rate of 250 kbps. Hence, it provides a connection range of 10 to 100 meters. Data transmission is performed over nodes using routers in an optimized manner. 6LoWPAN can be integrated with other WAN and LAN networks. 6LoWPAN is quite new in the industry. It is, therefore, particularly well-suited to systems such as home automation, street lighting tracking and management, residential lighting, smart metering, and common internet-connected device applications (Mulligan, 2007).

In a typical 6LoWPAN network, there are two types of devices, namely the router and the end device. As the name suggests, routers primarily route data to another node in the 6LoWPAN network in the shortest way possible. On the other hand, end devices send the data they gather from sensors to the router device to which they are connected when it is required. Only when there is a request, these devices switch from sleep mode to active mode. As a result, energy usage will be minimal regardless of network size.

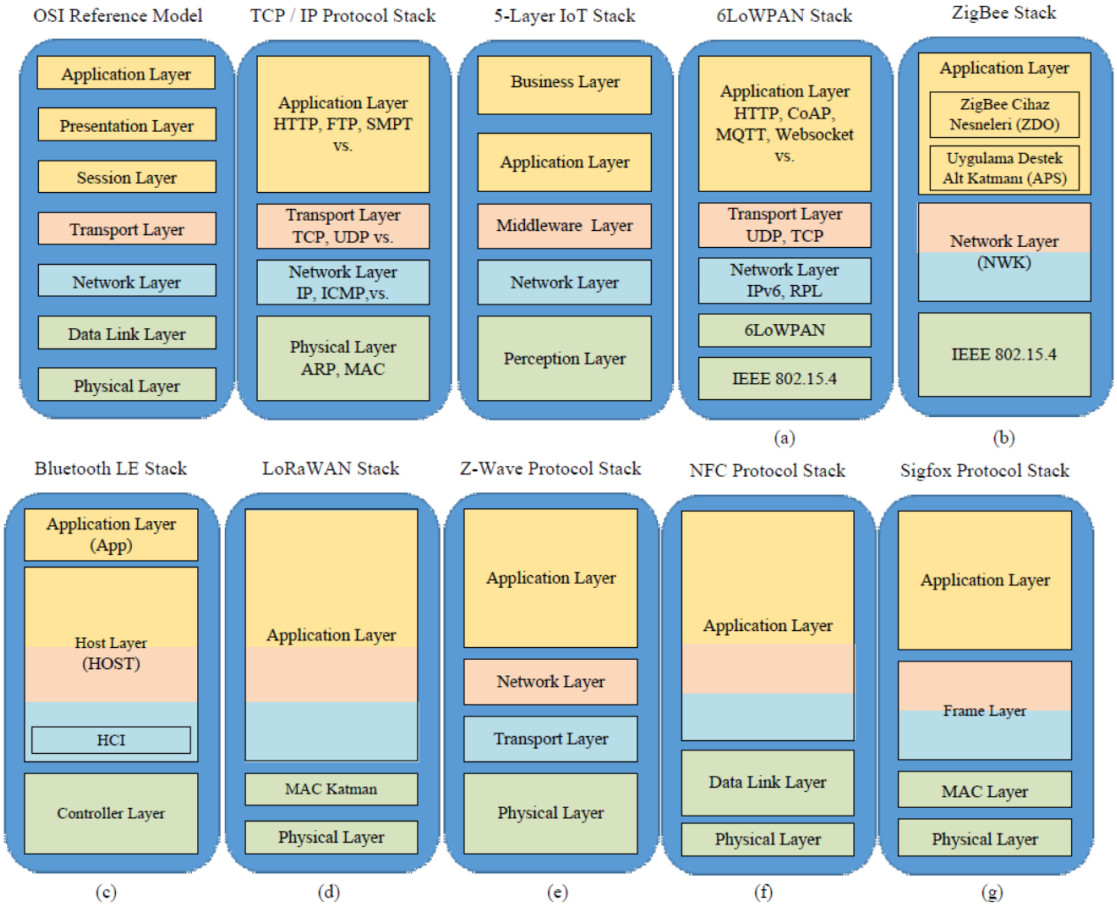

Figure 4. Comparison and mapping of OSI, TCP/IP and IoT Protocols

The layer structures of the OSI reference model, the TCP/IP protocol stack and the 6LoWPAN protocol stack are shown in Figure 4 (a). In parallel, the physical layer of the 6LoWPAN protocol stack converts data bits into wireless signals leveraging IEEE 802.15.4. By identifying and fixing problems in the physical layer during data communication, the data link layer seeks to maintain healthy communication. Protocols such as MAC, CSMA-CD (carrier-sense multiple access with collision detection) used in OSI and TCP / IP are provided by IEEE 802.15.4 for 6LoWPAN. In addition, 6LoWPAN adaptation was performed via a protocol and layer named 6LoWPAN to control devices in the network and route the data. The network and transport layers technically work with the same principle. However, the UDP protocol is generally used throughout data transmission for 6LoWPAN. Hence, the establishment of faster communication becomes possible. At the application layer, the HTTP protocol is commonly used in TCP/IP communication. Although there is an HTTP protocol for 6LoWPAN, application-level communication is commonly done using the CoAP (Constrained Application Protocol) or MQTT (Message Queuing Telemetry Transport) protocols, which are best fitted to IoT devices (Yalçınkaya, 2020).

3.3. ZigBee

ZigBee is a wireless network technology that is highly interoperable and standards-based, and it is used to connect IoT applications. ZigBee, founded on the IEEE 802.15.4 standard, was developed to address the need for a low-cost wireless network solution that enables low data rates, low power consumption, security, and reliability. ZigBee has a self-optimizing network structure. It is accomplished by allowing other nodes to explore new routes across the network if a node's data transfer path fails. Due to its decentralized network structure, it is employed as a powerful wireless solution in the IoT business (Farahani, 2011).

ZigBee is specifically designed for wireless sensor networks. Any monitoring and control application that needs a wireless connection can benefit from it. It is mostly employed in smart home and building automation, home security, smart cities, logistics and asset management and tracking, and patient tracking systems.

ZigBee operates at a speed of 20 kbps at 868 MHz, 40 kbps at 915 MHz and 250 kbps at 2.4 GHz. It is best used in applications involving battery-powered devices when a low data rate, reduced cost, and long battery life are desired. Since it spends most of the time in power-saving mode, also known as sleep mode, the wireless device's total time in processes like receiving or sending data is quite limited in many ZigBee applications. That is why devices can run for several years without battery replacements.

The layer structures of The OSI reference model, the TCP/IP protocol stack and the ZigBee protocol stack are given in Figure 4 (b). Consequently, all processes at the physical layer are carried out per the IEEE 802.15.4 protocol. The ZigBee network layer (NWK) is mainly responsible for creating a new network. This layer performs the following tasks: connecting and disconnecting a network, configuring network when a new device connects to a network, assigning an address to a new device, organizing all coordinator and router operations. Therefore, we can say that this layer defines some of the network and transport layer roles in the TCP/IP cluster. The Application Layer consists of the Application Support sublayer (APS) and the ZigBee Device Objects sublayer (ZDO). It includes applications defined by the manufacturer. The APS sublayer is responsible for the discovery and binding services. Discovery is used to determine devices running on the network, while the binding is used to match two or more devices and transmit messages between these connected devices. The ZigBee Device Objects sublayer (ZDO) performs local and wireless management of the network. Up to 240 separate application objects can be defined in the application layer, each with a unique endpoint address ranging from 1 to 240.

3.4. Bluetooth

Ericsson Mobile created Bluetooth technology in 1994. Bluetooth technology was later developed by the Bluetooth Special Interest Group, which was founded in 1998. Bluetooth, which is common in many products, has been standardized with IEEE 802.15.1. Bluetooth technology was created to allow short-distance communication between mobile or fixed devices without the use of cables. Its advantages include low cost, low power consumption, and the ability to communicate in a reliably (Miller et al., 2000).

Bluetooth is a wireless technology that transmits digitized voice and data over the 2.4 GHz ISM band, which is license-free. The devices do not need to see one another directly since it operates using radio waves. Bluetooth operates between 2.400 - 2.483 GHz with a 1 MHz band.

Bluetooth devices can be dual-mode, supporting both BR/EDR (Bluetooth Basic Rate/Enhanced Data Rate) and BLE (Bluetooth Low Energy), or single-mode, supporting solely Bluetooth limited power. Due to high-energy economy of BLE, many Bluetooth devices are used in IoT applications.

The protocol stack for the single-mode BLE device is planned in three layers, as shown in Figure 4 (c). These are controller, host, and application. Each of these basic building blocks is separated into multiple sub-layers in the protocol stack, which together provide the necessary functionality.

- *Application Layer*: The application layer, like all other systems, is the top layer that includes the reasoning for everything relevant to the use purpose, the user interface, and data processing.
- *Host Layer*: It includes the layers of Generic Access Profile (GAP), Generic Attribute Profile (GATT), Logical Link Control and Adaptation Protocol (L2CAP), Attribute Protocol (ATT), Security Manager Protocol (SMP), Host Controller Interface (HCI). The host control interface (HCI) is a method for reaching the hardware functions of Bluetooth devices that are not part of the protocol stack. By obtaining information such as baseband commands, connection manager commands, hardware status logs, control logs, and incident logs, HCI firmware enables Bluetooth hardware to function effectively.
- *Controller*: It includes Host Controller Interface (HCI), Link Layer (LL), and Physical Layer (PHY). The physical layer comprises analog communication circuits that can modulate, demodulate, and transform analog signals into digital symbols. The Link Layer combines specialized hardware and software that directly creates an interface with the PHY. It is also the real-time layer of the entire protocol stack, as it is in charge of adhering to all of the rules' timing requirements. This layer specifies operations including data entry, framing access address and signaling protocol, CRC (Cyclic Redundancy Check) generation and verification, data whitening, random number creation, and AES (Advanced Encryption Standard) encryption.

3.5. LoRaWAN

LoRaWAN (Long-Range Wide Area Network) is an open-source technology that is associated with low power usage for wide area networks. The battery life of a node is critical for IoT applications in terms of the network's capacity, service quality, and security. LoRaWAN networks are structured in a star topology where gateways transmit messages between end-devices and back-end centralized network servers. It offers data signaling at speeds ranging from 0.3 to 50 kbps, depending on the environment. Communication with LoRaWAN has a range of 2 to 5 km in the city and up to 15 km outside the city. LoRaWAN can be used in a variety of applications, including smart city applications, smart agriculture, and smart factories. In order to create a full range with LoRaWAN in Amsterdam, an IoT data network has been established using 10 gateways as an example for smart cities. The city of Amsterdam is the first to implement a comprehensive LoRaWAN application (Adelantado et al., 2017).

LoRaWAN operates in an unlicensed radio spectrum. As a result, radio frequencies can be utilized in the application without paying a license fee. The system, which is similar to Wi-Fi in that it uses the 2.4 GHz and 5 GHz ISM bands worldwide, allows anyone to set up Wi-Fi routers and send or receive Wi-Fi signals without requiring a license or permission. LoRaWAN supports bands from 902 to 928 MHz in the United States, 863 to 870 MHz in the EU, and 779 to 787 MHz in China, and typically transmits on the 868 MHz band in Europe and 900 MHz in the United States.

LoRaWAN can be mapped to the second and third layers of the OSI model. LoRaWAN protocols are defined by a group named LoRa Alliance. LoRaWAN stack layers are shown in Figure 4 (d).

3.6. Z-Wave

Z-Wave is a low-power MAC protocol designed for smart home applications. It is suitable for IoT applications, small applications such as light control, energy control, and fitness trackers and provides approximately 30 meters of point-to-point communication range. The ITU developed the Z-Wave protocol, which is now endorsed by the Z-Wave Alliance, a collection of over 300 worldwide firms. Batteries power many Z-Wave devices without the need for direct electrical energy. Because Z-Wave devices are only active during data transmission, they have low energy consumption. It is known that there are more than 35 million Z-Wave products in the world (Paetz, 2018).

Z-Wave technology operates at different frequencies while below the 1 GHz band, depending on the country. In Europe, it uses the frequencies 868.4 MHz and 869.85 MHz, while in the United States; it uses the frequencies 908.4 MHz and 916 MHz. It does not interfere with technologies such as Wi-Fi broadcasting in the 2.4 GHz band because it broadcasts at these frequencies. Besides, since the broadcasts are at quite low frequencies, they lose relatively less power when passing through obstacles like walls, etc. Z-Wave protocol provides communication up to 100 kbps speed. It also can function with IPv6 and multi-channel support, which are both significant advantages.

As shown in Figure 4 (e), the Z-Wave protocol stack consists of four layers: physical layer (PHY / MAC), transport layer, network layer and application layer. The physical layer is responsible for modulation and RF channel assignment, as well as adding headers at the transmitter and then synchronizing them at the receiver using the header. At the same time, the MAC layer is responsible for HomeID and NodeID, as well as controlling the medium between nodes using the anti-collision and withdrawal algorithms. The transport layer governs frame transmission and reception, as well as retransmission, ACK packet transmission, and verification. The network layer manages packet routing, topology scanning, and routing table updates. The application layer is in charge of application-oriented tasks in received or sent packets.

3.7. NFC

NFC (Near Field Communication) allows phones, tablets, laptops, and other devices to transfer data over short distances with other NFC-enabled devices. It was developed on RFID technology. The communication range is up to 10 cm. NFC operates in the 13.56 MHz ISM band and supports different data signaling rates such as 106 KBS, 212 KBS and 424 KBS (Coskun et al., 2012). Products using the NFC protocol are utilized in many applications due to their functionality. Mobile payment, authentication and access control, data transfer between devices, and reading digital information are common uses.

NFC communication system includes a reader or a writer device and a tag. The tag is a passive device with an antenna and a small bit of memory that works through a magnetic field. Tag memory can be in several forms such as read-only, rewritable or write-once. The reader is an active device that sends radio signals to the tag for interaction. In passive communication mode, the reader passively charges the device and allows data to be read.

NFC devices support active and passive communication types. During active mode, target and initializer devices take over their power sources, and can communicate with each other via alternative signal transmission. While in the passive mode, the initiating device generates radio signals, and target device receives its power from this electromagnetic field. The target device responds to the initializer by modulating the current electromagnetic field.

Figure 4 (f) shows the mapping of P2P based NFC device stack to the OSI reference model and TCP/IP protocol stack. As seen here, the application layer, data connection layer, and physical layer make up the NFC protocol stack. The application layer determines the

data format to be exchanged between NFC devices or between the NFC device and tags. The physical layer focuses on modulation, coding, and RF-related characteristics like frequency and power, whereas the data link layer deals with different operation modes and anti-collision mechanisms.

3.8. Sigfox

Sigfox is a French company founded in 2009 that builds wireless networks to keep low power devices such as electricity meters, smartwatches and washing machines always on and emit low amounts of data. The company's trademark system is a cellular-based variant that allows remote people to communicate with the access point via UNB (Ultra Narrow Band). Sigfox has designed it to meet the IoT network requirements. It's a perfect solution for boosting the performance and efficiency of applications that will be developed as wide area networks, such as smart agriculture and smart cities, thanks to its long battery life, low device cost, low connection fee, high network capacity, and long-range (Vejlgaard et al., 2017).

The Sigfox network consists of two layers, the network equipment layer and the system support layer. Between these two layers, a standard network including GSM, Wi-Fi, or Ethernet is deployed. End devices located in the network devices layer transmit sensor data to Sigfox stations. Stations transmit data to Sigfox cloud servers using the internet. This part is called the system support layer. Users receive the processed and interpreted data after this stage.

Sigfox uses 868 MHz ISM band, and the spectrum is split into 400 channels of 100 Hz. Its frequency efficiency enables low energy consumption while offering more range. It is built on the Sigfox star topology, and a mobile operator should carry the generated traffic. Each node device has a 12-pole payload capacity and can send 140 messages per day at a data rate up to 100 bps. The Sigfox network's access points are theoretically designed to serve up to one million end devices across a range of 30-50 kilometers in rural areas and 3-10 kilometers in urban areas.

As shown in Figure 4 (g), Sigfox consists of a physical layer, MAC layer, frame layer and application layer. The physical layer determines the modulation of Sigfox transmissions. Here it adds or removes headings in this layer. It uses BPSK modulation for uplink and GFSK modulation for downlink. Based on the location where the system is deployed, the bit rate is either 100 or 600 bits per second. In Europe, power transmission reaches a maximum of 14 dBm, while in North and South America, it reaches 22 dBm. This layer also controls operating frequencies. The MAC layer adds the required fields to identify the device that will receive data and other standard parameters such as error detection codes. It prepares the packages according to the protocol's transfer and reception forms. The frame layer receives data from the application layer. It systematically transfers it to the lower layer while also adding a sequence number, as seen in the TCP/IP protocol set's transport and network layers. The application layer supports different applications in Sigfox technology. This layer defines several interfaces or protocols to facilitate transfer between WAN and servers, such as SNMP (Simple Network Management Protocol), HTTP, MQTT, and IPv6.

3.9. Comparison of the Protocols

In Table 1, the protocols are summarized according to frequency, distance and data transfer rates within the scope of the current study. The protocol should be chosen based on the type of application, the distance between objects, and the transmission power.

Table 1. Comparison of protocols

Protocol	Frequency	Distance	Data Transfer Speed
Bluetooth	2.4 GHz	50-150 m	1 Mbps
ZigBee	2.4 GHz	10-100 m	250 kbps
Z-Wave	900 MHz	30 m	9.6 / 40/100 kbps
6LoWPAN	2.4 GHz	10-100 m	250 kbps
NFC	13.56 MHz	10 cm	100-420 kbps
Sigfox	900 MHz	30-50 km in the countryside, 3-10 km city center	10-1000 bps
LoRaWAN	Unstable	2-5 km, 15 km	0,3-50 kbps

4. Conclusions

In this article, which deals with the common problems of grasping the protocols of IoT applications, the usage areas of IoT applications are principally examined per the current data. Looking at the sectoral distribution of applications developed in 2020, industrial production, transportation, energy, retail, smart cities, healthcare, supply chain, agriculture and livestock, and smart buildings were amongst the prominent applications.

In the literature, there are various architectural methods for IoT applications. A common standard similar to TCP/IP or OSI has not been adopted yet. This is because different applications are applied in different subject areas where different protocols and technologies are used. It can be said that establishment of a standard is not possible soon. In other words, as the number of M2M applications increases, a standard is needed to make data transfer between devices used in different applications more seamless. Current architectures in the literature are explored in this article. The most utilized architecture has been identified to be four-layer architecture. Nevertheless, adoption of a five-layer architecture is expected to increase, especially as core phases of IoT applications such as smart business operations, data analytics, and big data analytics become more common.

The article discusses technology and processes involved in architectural layers. There are many technologies and protocols to choose from, depending on the number of devices connected to the network, the data transfer rate, the energy, and the range. This selection should be made according to application type. Wide area networks like Sigfox and LoRaWAN should be chosen because smart farming operations require, for example, dissemination over large areas. Smart home systems can use Z-Wave or ZigBee protocols created specifically for this purpose. The Bluetooth LE technology, on the other hand, is widely employed in consumer electronics.

The IoT protocols and technologies examined through the article have been mapped to the layers of OSI and TCP/IP protocol and standards, which are globally acknowledged and presented in Figure 4 . Based on this information, protocol structures that inherit relatively similar usage areas and tasks are also designed similarly. Generally, the perception layer of IoT protocols is based on IEEE 802.15.4 protocol. At the same time, network and business layers are similar to the network and transport layers observed in TCP/IP protocol. Besides, almost every application layer seen in these protocols is customized in line with the usage areas of protocols.

References

Adelantado, F., et al. (2017), Understanding the limits of LoRaWAN. IEEE Communications magazine. 55(9): p. 34-40 DOI: http://doi.org/doi:10.1109/MCOM.2017.1600613

Bris, A.C., Chan Heng, Lanvin, Bruno (2019), Smart City Index 2019, The IMD World Competitiveness Center. Available: https://www.imd.org/research-knowledge/reports/imd-smart-city-index-2019/

Chen, F., et al. (2010), Simulation study of IEEE 802.15. 4 LR-WPAN for industrial applications. Wireless Communications and Mobile Computing,. 10(5): p. 609-621 DOI: http://doi.org/doi:10.1002/wcm.736

Coskun, V., K. Ok, and B. Ozdenizci, (2011) Near field communication (NFC): From theory to practice. 2012: John Wiley & Sons. 256.

Ercan, T. & Kutay, M. (2016). Endüstride Nesnelerin Interneti (IoT) Uygulamaları . Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi , 16 (3) , 599-607 . Retrieved from https://dergipark.org.tr/tr/pub/akufemubid/issue/43551/532437

Erdal, E. & Ergüzen, A. (2020). Nesnelerin İnterneti (IoT) . International Journal of Engineering Research and Development , Elektrik Mühendisliği ve Bilgisayar Bilimleri Özel Sayısı , 24-34 . DOI: 10.29137/umagd.827676

Farahani, S., ZigBee Wireless Networks and Transceivers. Newnes. 360 DOI: http://doi.org/doi:10.1016/B978-0-7506-8393-7.X0001-5

Forbes, Microsoft Soars: How Azure, AI And IoT Are Driving Cloud Hypergrowth At $20-Billion Scale, in Forbes. 2018. Available: https://www.forbes.com/sites/bobevans1/2018/05/03/microsoft-soars-10-factors-driving-satya-nadellas-20-billion-cloud-juggernaut/#234d406a2037

I-CIO, John Deere: How information-enabled farming will feed the world in I-CIO. 2018. Available: https://www.i-cio.com/innovation/internet-of-things/item/john-deere-how-information-enabled-farming-will-feed-the-world

Kim, D. and M.G. Solomon (2016), Fundamentals of information systems security 3rd Edition 2016: Jones & Bartlett Learning. 548.

Mulligan, G. (2007) The 6LoWPAN architecture. in Proceedings of the 4th workshop on Embedded networked sensors. Cork, Ireland: Association for Computing Machinery DOI: http://doi.org/doi:10.1145/1278972.1278992.

Miller, B.A., C. Bisdikian, and T. Foreword (2000) By-Siep, Bluetooth revealed : Prentice Hall.

Paetz, C., Z-Wave Essentials. 2018: CreateSpace Independent Publishing Platform. 310.

Scully, P. (2020), Top 10 IoT applications in 2020, in IoT Analytics: Market Insights for the Internet of Things. Available : https://iot-analytics.com/top-10-iot-applications-in-2020/

Shelby, Z. and C. Bormann (2011), 6LoWPAN: The wireless embedded Internet. Vol. 43.: John Wiley & Sons. 244.

Sethi P., Smruti R. Sarangi, (2017) "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017,. https://doi.org/10.1155/2017/9324035

TU Automotive, Volvo Claims 1M Connected Car Milestone, in TU Automotive. (2019). Available https://www.tu-auto.com/volvo-claims-1m-connected-car-milestone/

Vejlgaard, B., et al. (2017) Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. in 2017 IEEE 85th vehicular technology conference (VTC Spring). IEEE. DOI: http://doi.org/doi:10.1109/VTCSpring.2017.8108666

Yalçınkaya, F, et al. (2020). IoT based Smart Home Testbed using MQTT Communication Protocol . International Journal of Engineering Research and Development , 12 (1) , 317-324 . DOI: 10.29137/umagd.654056

World Medical Innovation Forum, Calibrating Innovation Opportunity and Urgency. (2020). Available: https://www.youtube.com/watch?v=VXyvxIMQi0c

Wu, M., et al.(2010) Research on the architecture of Internet of Things. in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE. DOI: http://doi.org/doi:10.1109/ICACTE.2010.5579493