Science, Engineering and Technology *Volume 1, Issue 1, Pages 1-14*
www.setjournal.com *https://doi.org/10.54327/set2021/v1.i1.3*

Wireless communication technologies for the Internet of Things

Alem Čolaković, Adisa Hasković Džubur, Bakir Karahodža

University of Sarajevo, Faculty of Traffic and Communications, Zmaja od Bosne 8, Sarajevo 71000, Bosnia and Herzegovina

Abstract

Internet of Things (IoT) is the inter-networking paradigm based on many processes such as identifying, sensing, networking and computation. An IoT technology stack provides seamless connectivity between various physical and virtual objects. The increasing number of IoT applications leads to the issue of transmitting, storing, and processing a large amount of data. Therefore, it is necessary to enable a system capable to handle the growing traffic requirements with the required level of QoS (Quality of Service). IoT devices become more complex due to the various components such as sensors and network interfaces. The IoT environment is often demanding for mobile power source, QoS, mobility, reliability, security, and other requirements. Therefore, new IoT technologies are required to overcome some of these issues. In recent years' new wireless communication technologies are being developed to support the development of new IoT applications. This paper provides an overview of some of the most widely used wireless communication technologies used for IoT applications.

Keywords: *Internet of Things, wireless technologies, WSN, W-Fi, LR-WPAN, LR-WAN*

1 Introduction

There are many applications of the Internet of Things (IoT). IoT is most abundant in manufacturing, transport, logistics, healthcare, retail, agriculture, process automation, etc. The development of IoT applications requires various technologies to enable device identification, object detection, measurements, networking, data transfer, data analysis, and other processes. Some IoT applications require connectivity between physical and virtual objects anytime and anywhere. The capabilities of various IoT technologies have improved dramatically over the past few years allowing development of new applications. However, the fragmentation of standards and technologies creates complex problems and challenges in providing a complete connection of everything [1]–[6]. Besides, the increased number of IoT applications causes several problems related to the increase in traffic requirements [7], [8]. It is necessary to enable the deployment of IP (*Internet Protocol*) architecture to provide the connectivity of different devices via the Internet [6], [9], [10]. IoT devices often have limited hardware capabilities which cause several challenges such as device identification and addressing, interoperability, mobility, scalability, system management, energy efficiency, security, QoS (Quality of Service) assurance, etc. Also, future development should focus on the green technologies [11].

In this paper, the focus is set on wireless communication technologies widely used for IoT applications. There is a number of new wireless communication technologies adapted for IoT applications such as different WSNs (*Wireless Sensor Networks*), WLAN (*Wireless Local Area Networks*), LR-WPAN (*Low-Rate Wireless Personal Area Networks*), and LP-WAN (*Low Power Wide Area Networks*). Some of these technologies are based on the IP protocol architecture while others have a different architecture. This paper aims to present technologies and their characteristics used for IoT applications. The paper is structured as follows. After an introductory discussion, Section 2 introduces the concept of IoT architecture. Section 3 presents the wireless communication technologies most commonly used in the IoT environment. Section 4 provides an overview of both mobile communication systems and their applications in the IoT environment. Section 5 contains concluding remarks and some guidelines for future research.

2 IoT (Internet of Things)

IoT involves the application of many technologies to connect different physical and virtual objects. The IoT architecture should enable multi-integration of various systems and technologies.

Published: 30 April 2021
Corresponding author: Alem Čolaković *(alem.colakovic@gmail.com)*

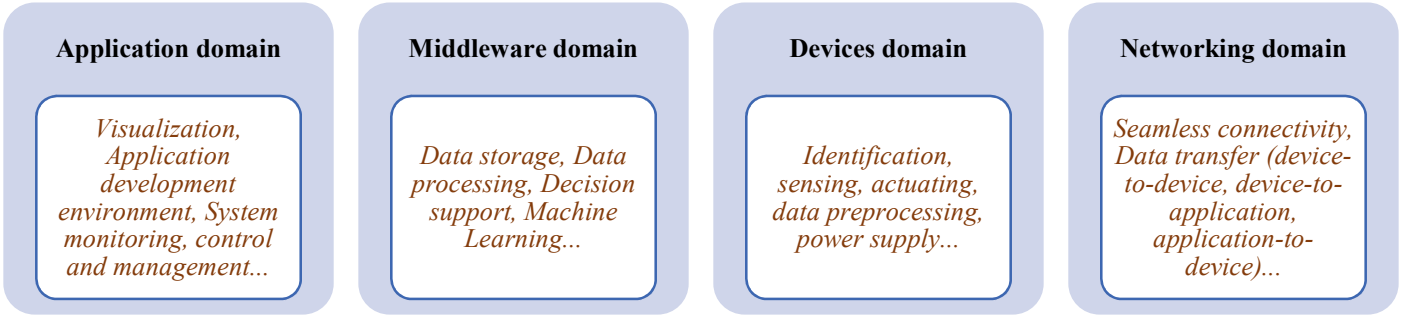

Figure 1. IoT functional domains

An IoT system can consist of physical objects (e.g. sensors, actuators, etc.) and virtual objects (e.g. cloud services, IoT protocols, communication layers, etc.). These objects need to be interoperable through the corresponding system architecture [12]. IoT technologies should provide seamless connectivity between these objects. Also, IoT applications include many different functions such as object identification, event detection, measurements, data processing, etc. These functions can be grouped according to a conceptual architecture formed on the basis of different tasks performed in the IoT system. [1]. Figure 1 shows functional blocks composed of four main domains (layers).

There are some overlaps in the functionality of domains. We do not include a deep analysis of all domains. Instead, we present some of the most used wireless communication technologies used to provide seamless connectivity between IoT components as well as perform data transfer.

3 An overview of wireless communication technologies towards Internet of Things (IoT)

Network technologies should enable seamless connectivity between different IoT devices and other infrastructure (e.g. cloud systems). Due to a huge increase in data traffic, it is becoming a challenging issue to meet the growing demands of IoT applications. There are many challenges to deploy different network technologies. The key challenges include interoperability, object identification, addressing, routing and mobility management, access control, energy efficiency, QoS performance, scalability, reliability, security, resource control and management, auto configuration, etc. Some new network technologies, mechanisms, and protocols have been developed to overcome these challenges. Also, there are some improvements in existing solutions to adapt to IoT applications. Figure 2 present the most common wireless technologies used for IoT.

Examples of some technologies that support the development of IoT applications are: EPCglobal based on RFID (*Radio-frequency identification*) and EPC (*Electronic Product Code*) based IoT architecture [13], [14], WSN (*Wireless Sensor Network*) architecture [15], [16], *peer-to-peer* [17], and autonomous architecture [18]. Existing communication protocols can be used for data exchange. However, in many cases, these protocols are not effective for new IoT traffic models. Therefore, new protocols have been developed on almost all layers of the network architecture.

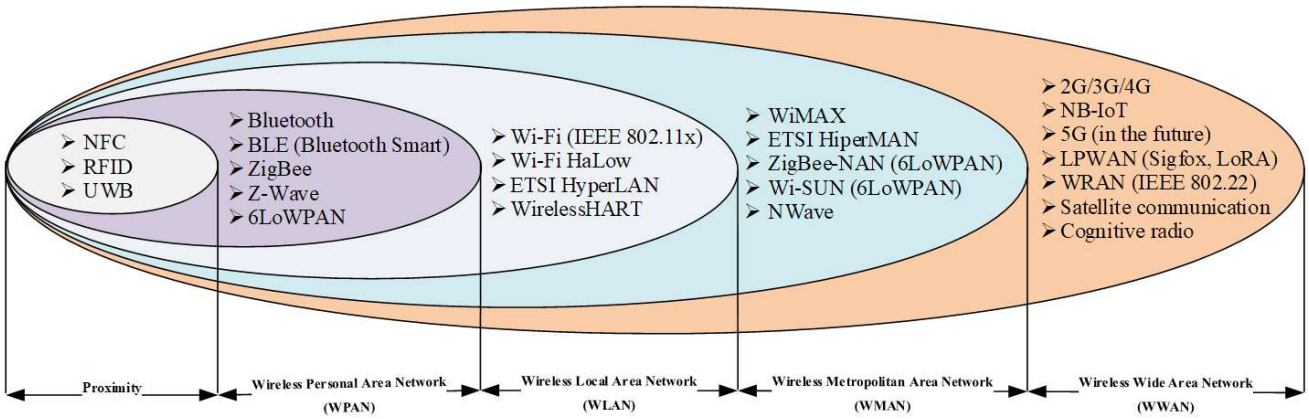

Figure 2. Wireless communication technologies suitable for Internet of Things [1]

3.1 IoT communication protocols

The development of new protocols and communicational architectures for future applications of IoT concepts will have one of the key roles in the following years. The protocols used in traditional internet services are most commonly not appropriate for IoT because additional requests are applied, such as energy efficiency. As a consequence, a set of application layer protocols such as CoAP (*Constrained Application Protocol*), MQTT (*Message Queue Telemetry Transport*), MQTT-SN (*MQTT for Sensor Networks*), AMQP (*Advanced Message Queuing Protocol*), DDS (*Data Distribution Service*) REST, and WebSocket have been developed (Table 1). There are also other projects aimed to develop protocols for current and future purposes, such as: Mihini / M3DA, Laba (*Lightweight Local Automation Protocol*), LWM2M, etc. According to the protocols used, IoT objects can be classified into two groups: those that support and those do not support the TCP/IP protocol architecture. For example, IoT applications that use CoAP, MQTT, MQTT-SN, AMQP, REST, and some other application protocols support TCP/IP, likewise, there are apps using non-TCP/IP based protocols, and consequently the problem of interoperability occurs.

For adjustment of IoT to the surroundings, different protocols have been developed for service discovery such as: DNS-SD (*DNS Based Service Discovery*), SSDP (*Simple Service Discovery Protocol*), SLP (*Service Location Protocol*), mDNS (*multicast DNS*), APIPA (*Automatic Private IP adrese*), Physical Web, HyperCat, UPnP (*Universal Plug and Play*). These protocols are used to enable efficient communication establishment. They can be classified by their function in the following way: discovery protocols (DNS-SD, SLP), naming (mDNS) and addressing (APIPA).

On the transport layer, along with the *TCP (Transmission Control Protocol)* [19] and UDP (*User Datagram Protocol*) [20], other protocols can be used such as QUIC (*Quick UDP Internet Connections, pronounced quick*) [21] and NanoIP (*Nano Internet Protocol*) [22]. QUIC has been created by the Google company to support multiplexed connections between two endpoints through UDP for providing protection of analog TLS/SSL, delay reduction and congestion avoiding. NanoIP is a concept based on the two transport techniques: nanoUDP for simple unreliable transmission and nanoTCP which provides mechanisms of retransmission and flow control. This protocol provides an alternative to networking, mechanism control and sensor network automatization. TLS is a cryptographic protocol that enables secure communication. Using the TLS protocol, the IoT device and the destination point negotiate to specify which version (TLS 1.0, 1.2, 1.3) and the cipher suites they will use. Further, the authentification is applied by exchange of public and private keys. TLS has to be used over a reliable transport channel (usually TCP), whereas some IoT applications prefer the usage of UDP transport protocol. Accordingly, a TLS variant compatible with the UDP datagrams is needed. For that purpose, the DTLS protocol has been developed, which was based on TLS providing equal security guarantees [23]. This communication protocol ensures security in a way that it strives to stop network eavesdropping, unauthorized message handling or forgery. The above security protocols use different mechanisms and standards such as X.509 which is used to manage digital certificates and public-key encryption in TLS. The application protocols are based on different transport protocols, and therefore use different security mechanisms on this layer. For example, CoAP uses ATLS, while compromised version of DTLS is used for *Lightweight Secure CoAP* adjusted for IoT environments. XMPP and AMQP use TLS and SALS (*Simple Authentication and Security Layer*). MQTT is mostly based on TLS/SSL solutions [5], but there are other solutions such as OASIS MQTT which uses a somewhat different security approach.

On the network layer, both versions of IP protocol are used (IPv4 i IPv6) where IPv6 takes on an increasingly important role. IPv6 protocol is one of the key protocols for IoT [24], simply because IPv4 cant't provide enough addresses needed for the growing number of connected objects.

Table 1. Application layer protocols for IoT

Application protocol	Standard	RESTful support	Trasnport protocol	Security	QoS support
CoAP [36]	IETF RFC 7252	Yes	UDP	DTLS	Yes
MQTT [37]	OASIS Standard	No	TCP	TLS/SSL	Yes
MQTT-SN	IBM Zurich Research website	No	TCP	TLS/SSL	Yes
XMPP [38], [39]	IETF RFC 6120, 6121	No	TCP	TLS/SSL	No
AMQP [40]	ISO and IEC	No	TCP	TLS/SSL	Yes
DDS [41]	OMG (*Object Management Group*)	No	UDP	DTLS	Yes
HTTP	IETF RFC (2068, 2616, 7230), W3C	Yes	TCP	SSL	No
WebSocket [42]	IETF Internet Draft	Yes	TCP	TLS/SSL	No

IPv6 is a protocol for network layer that provides end-to-end encryption. In terms of the routing process, the new routing protocols have been developed. IETF workgroup ROLL has developed an RPL protocol for routing IoT traffic in IPv6 networks [25]. This protocol has been developed especially for LLN networks which include WSN and IoT environments. Besides RPL, there are also additional routing protocols such as AODV, LOAD, DYMO-Low, HI-Low, et al. These protocols are most commonly used in 6LoWPAN networks.

In order to enable a simple end-to-end connection and satisfy traffic requirements, an adaptation of existing networki technologies is needed. There are efforts to adjust the data link layer within existing reference models (TCP / IP) to adapt to new IoT traffic models. 6LoWPAN [26]–[28] has been developed as a convergence layer for the IPv6 packet data layer over IEEE 802.15.4 networks. It integrates IPv6 infrastructure and WSN using header compression, fragmentation, limited package size, multi-hop transfer and different address length [29]. Routing tasks perform protocols in the upper layers of the protocol architecture (e.g. RPL). Additionally, it should be noted that not all network technologies used for IoT are based on the TCP/IP stack protocol, i.e., some of these technologies have a special protocol architecture.

New application layer protocols and certain improvements in the network access layer have found the widest application in the IoT environment. In development of IoT solutions, the following technologies are mostly applied: WSNs (*Wireless Sensor Networks*), RFID, NFC, WLAN (*Wireless Local Area Networks*), LR-WPAN (*Low-Rate Wireless Personal Area Networks*), LP-WAN (*Low Power Wide Area Networks*) and mobile communication systems.

3.2 WSN

WSN (*Wireless Sensor Networks*) represent a distributed system made up of sensor nodes that are mutually connected by some of the wireless communication technology. Along with the previously explained sensor functionalities, besude the possibility of communication (data transfer), in come cases the sensor nodes – SN must also have features for storage and processing smaller quantities of collected data. Consequently, the hardware of the sensor node usually includes four key components: (1) power and energy managenet, (2) detection and/or measurement sensor, (3) microcontroller and (4) transceiver. The power module enables the power needed for certain functions. The measurement sensor is in charge of detection and measuring values such as temperature, humidity, light intensity, vibrations, etc. With the data collected, a transformation of signals into electrical signals which are later transferred with a transceiver to microcontrollers is performed. The microcontroller does data processing with the goal of making a decision on further steps (e.g., discard data or forward them on another infrastructure). Most commonly, the communication technologies used for WSN are E 802.15.4 and ZigBee, but there are also other technologies used in different scenarios (Table 2).

The sensor nodes are mainly arranged at small distances (usually up to 10m). The collected information is transferred through mutual communication between SN and one or more access/sink devices. These access devices can represent the destination of all data, and in the case of digital sensors applications, they enable bidirectional communication with SN. Bidirectional communication is made of data reception from SN and giving instructions or transmission of management and other data to other direction (towards SN).

An IoT network requires gateways as a bridge between specific radio protocols and the Internet. These gateways have to forward packets to the Internet. For example, the collected data can be forwarded by LAN, WLAN or internet network (Figure 3). The WSN edge node, which includes IP support, can act as a gateway between the WSN and the IP network. Also, certain nodes can be used for local processing and data storage, as well as support for connection of special user interface (e.g. LCD).

Table 2. An overview of WSNs towards IoT

Standard	Throughput (kbps)	Frequency range (MHz)	Defined (standardized) layer
IEEE 802.15.4	20, 40, 250	868, 915, 2400	PHY, MAC
ZigBee	250	868, 915, 2400	NET, APP
BLE	1000	2400	PHY, MAC, NET, TRA, APP
Bluetooth	1000-3000	2400	PHY, MAC, NET, TRA, APP
Z-Wave	40	868, 915	PHY, MAC, NET, APP
MiWi	250	2400	PHY (802.15.4), NET
WirelessHART	250	2400	PHY (802.15.4), MAC, NET, TRA, APP
ISA 100.11a	250	2400	PHY (802.15.4), MAC, NET, TRA, APP
ANT/ANT+	1000	2400	PHY, MAC, NET, APP

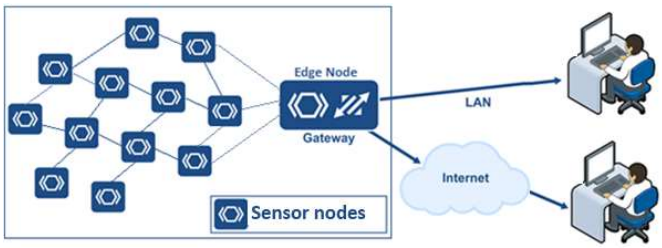

Figure 3. WSN connected to local infrastructure and internet

Every node has to be aware of the identity and location of its nearby node in order to enable data transfer. If the network is well planned, the topology is set up according to priorities. However, in ad-hoc mode of organizing WSN, the topology is determined in real-time and periodically renewed depending on the exclusion of the node from the network (e.g. due to a change of location they are no longer in range) or new nodes are added. This implies that in these networks the knowledge about change of arrangement of nodes is not needed.

Sensors within the WSN system have certain restrictions related to operating speed, storage, communication range, energy source, etc. A key challenge within the WSN systems is how to provide source of energy. Efficient charging and energy consumption have to be provided with the goal of enabling long-term working time. There are also issues related to changes in topology, device discovery, energy efficient routing, etc. One of the important development issues is assurance of secure operation in various environments. However, regardless of the maintenance complexity and other occurring issues, WSN systems have to keep an affordable price. All these challenges have to be overcome so WSN could be able to sustain the growing needs for development of systems for monitoring, tracking and control of different events and objects. In addition to the sensor development technology, a special attention is paid to the development of appropriate communication technologies which neeed to provide the possibility of overcoming some of the above-listed challenges.

3.3 RFID i NFC

Alongside sensor networks, some of the key technologies in the beginning developments of IoT solutions are RFID (*Radio Frequency Identification*) and NFC (*Near Field Communication*) [30]–[33]. RFID is a short-span communication technology that uses the electromagnetic field for automatic identification and monitoring of tags attached to objects. RFID standrads include ISO RFID standards (including ISO 18000, 29167, 20248, JTC 1/SC 31) and EPCglobal standards which are used for specification and standardization of RFID systems and elements. RFID is not allowed to "bother" other systems such as radio of emergency services or TV signals.

The integration of sensor technology and RFID enables a lot of new possibilities into the IoT paradigm such as detection, various measurements and the possibilities of connection into passive systems. RIFD technology benefits are extended with possibilities of tracking and data availability through the Internet. In many cases, RFID identification is also used by applying EPCglobal, which has a similar function as a barcode. However, this technology can be used for running various activities, while barcodes don't have this capability [34].

RFID tags (active or passive) have a unique identificatory, where the most used is EPC. Active tags have a battery connected to the object and transfer signals continuously, while passive tags broadcast signals only when activated. Therefore, passive tags do not have their own energy source, and they rather completely rely on the reader for their working power. They are powered by the reader, which sends electromagnetic waves which induce electric power into the tag antenna. These tags are the smallest and cheapest and as such are mostly used. Active tags have batteries, used to start the electric circuit of the microchip and for broadcasting the signal to the reader. This technology uses more frequency bands (Global: 6 MHz, ISM: 13.5 MHz, 433 MHz, 902-928 MHz, 2.4 GHz, ISM EU: 863-870 MHz, UWB: 5-27 GHz) which causes different channel widths, depending on the range used. The maximum capacity of data transfer is 500 Kbps with the typical distance of 0.1-5 m [33].

Another technology that is increasingly integrated integrated into smartphones is NFC with similar identification possibilities. The NFC is based on ISO/IEC 18092, 14443, and JIS X6319-4 standards and it was created based on RFID to enable short-range communication. The basic idea of NFC is usage simplicity and a safe performance mode. NFC communication is very secure. Due to its limited range, it would be very difficult to perform any kind of attack without the users noticing.

NFC technology uses an unlicensed frequency range of 13.56 MHz whereby it allows different data transfer speeds to maximum of 848 kbps between devices with the typical range of around 10 cm [33]. Every NFC tag has a unique identificator - UID (*Unique Identification*). When internet connection is available, there is a possibility of data transfer using different network services which expands the benefit of this technology. There is a large number of research where a comparison between RFID and NFC technologies from different aspects is made, eg. [30]–[33], [35].

Table 3. An overview of Wi-Fi standards

Standard	Year	Frequency (GHz)	Bandwidth (MHz)	Throughput (Mbps)	Modulation	Range (~)	
						Indoor	Outdoor
802.11-1997	Jun. 1997.	2.4	22	1, 2	DSSS, FHSS	20 m	100 m
802.11b	Sep. 1999.	2.4	22	1, 2, 5.5, 11	DSSS	35 m	140 m
802.11a	Sep. 1999.	5	5/10/20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35 m	120 m
802.11j	Nov. 2004.	4.9/5.0				?	?
802.11p	Jul. 2010.	5.9				?	1,000 m
802.11y	Nov. 2008.	3.7				?	5,000 m
802.11g	Jun. 2003.	2.4				38 m	140 m
802.11n	Oct. 2009.	2.4/5	20	Up to 288.8	MIMO-OFDM	70 m	250 m
			40	Up to 600			
802.11ac	Dec. 2013.	5	20	Up to 346.8	MIMO-OFDM	35 m	?
			40	Up to 800			
			80	Up to 1733.2			
			160	Up to 3466.8			
802.11ad	Dec. 2012.	60	2,160	Up to 6,757 (6.7 Gbit/s)	OFDM	3.3 m	?
802.11af	Feb. 2014.	0.054–0.79	6–8	Up to 568.9	MIMO-OFDM	?	?
802.11ah	Dec. 2016.	0.7/0.8/0.9	1–16	Up to 8.67		?	?

3.4 Wi-Fi

IEEE (*Institute of Electrical and Electronics Engineers*) defined the series of specifications 802.11 for local wireless networks – WLAN (*Wireless Local Area Network*) which are mostly known by the term Wi-Fi. These networks were created to use frequency bands. There is a huge number of improvements to the original standard which were implemented over time (Table 3) [4], [6], [36]–[40].

Wi-Fi (*Wireless Fidelity*) is intended to use in medium and short data transfer lengths (up to a few hundred meters), but the exact lengths can't be defined because they depend on multitude factors: variances in standards, distance between devices, atmospheric conditions, optic visibility obetween antennas, quality of hardware, etc. For some Wi-Fi technology versions, measurements were made which give approximate values, while for other versions this characteristic has a high level of stochasticity. As a result, in the above-listed table for some versions of Wi-Fi, the symbol "?" is given. The main challenge in the implementation of IoT system that includes Wi-Fi technology is the big energy consumption compared to Bluetooth and ZigBee [6].

During the time, different versions of IEEE 802.11 standard have been developed with the goal of constant improvements and elimination of certain restrictions. Compared to the first versions, there are improvements for overcoming problems such as energy efficiency, mobility, QoS, etc. For example, IEEE 802.11ah (*Low-Power Wi-Fi*) [38] supports a wide spectre of IoT applications while being energy efficient, supporting QoS, following scalability (a big number of devices), as well as solutions with low expenses [36], [37].

3.5 LR-WPAN

The LR WPANs (*Low-Rate Wireless Personal Area Networks*) are networks optimized for use in systems with low data rates and low power consumption. The networks

composed of highly limited nodes (limited processing power and memory) that are interconnected by low power radio links are commonly referred to as Low power and lossless networks (LLNs). They are characterized by low data transfer speed, low bandwidth and low cost. Some examples of networks with such specifications are: ZigBee, BLE, Bluetooth 5, ISA 100.11a, WirelessHART, MiWi, SNAP, Thread, 6LoWPAN, Z-Wave (Table 4) [33], [41].

IEEE 802.15.4 (*Low-Rate Wireless Personal Area Networks - LR-WPANs*) [42] has been developed as a sublayer for MAC (*Medium Access Control*) and PHY (*Physical Layer*). Its primary purpose is to allow reliable communication in the IoT environment. The following features are provided: low power requirements, lower data transfer speed, low prices, high bandwidth, security, encryption, authentication and support for a large number of nodes [5]. This standard is the basis for several other specifications such as ZigBee, ISA100.11a, MiWi, and WirelessHART.

6LoWPAN (*IPv6 Low Power Personal Area Network*) is one of the most important technologies in the IoT domain. It enables the achievement of end-to-end communication via IP. The IETF recommendations are focused on header compression and with two main defined functions. 6LoWPAN consists of specific equipment to conform to the 802.15.4 standard and its characteristics of low power and low cost. 6LoWPAN is characterized by a small packet size. Considering the maximum frame of the physical layer is 127 bytes, the resulting maximum frame size in the media access control layer is 102 octets. The data rates are limited to 250 kbps, 40 kbps, and 20 kbps for each of the currently defined physical layers (2.4GHz, 915MHz i 868MHz). One of the key features is the sleeping mode of the device. In such mode, the device reduces power consumption, without the ability to exchange data. In 6LoWPAN networks, each node has its own IPv6 address, allowing it to connect directly to the Internet using open standards. The 6LoWPAN system is used for a variety of applications, but the most important application domain is wireless sensor networks. Since the IPv4 protocol has become increasingly congested due to the rapid growth in the number of devices, 6LoWPAN technology offers a solution to low-power networks using IPv6 as the basic IP format. The IPv6 protocol distinguishes this technology from others by providing a set of benefits for LoWPAN. Such benefits include: the existing infrastructure is used, good interoperability and easier development of the application layer due to well known IP technologies, easier connection to other networks based on IP architecture, and large number of addresses with straightforward automatic configuration of network parameters. The last one is very important for 6LoWPAN networks where many devices must be supported.

Table 4. An overview of LR-WPAN technologies

Technology	Standard	Frequency	Range	Throughput	No. devices
IEEE 802.15.4	IEEE	868 / 915 MHz, 2,4 GHz	100 m	20/40/250 kbps	50
ZigBee	ZigBee AllianceIEEE802.15.4	IEEE 802.15.4 (868 / 915 MHz, 2,4 GHz)	100 m	250 kbps	2^{16}
BLE	IEEE 802.15.1 Bluetooth SIG	2,4 GHz	100 m	1 Mbps	2^{31}
Bluetooth 5	IEEE 802.15.1 Bluetooth SIG	2,4 GHz	200 m	2 Mbps	-
ISA 100.11a	International Society of Automation (ISA)	IEEE 802.15.4 (2,4 GHz)	300 m	250 kbps	-
WirelessHART	HART Communications Foundation (HCF)	IEEE 802.15.4 (2,4 GHz)	10-600 m	250 kbps	-
UWB	IEEE 802.15.3a	3.1 – 10.6 GHz (USA)	4-20 m	110 Mbps-1.6 Gbps	128
Z-Wave	Z-Wave Alliance ITU-T G.9959	868 / 915 MHz (ISM)	30 m	9.6/40/100 kbps	232
6LoWPAN	IETF RFC6282	Adapted for use with other networks	N/A	20/40/250 kbps	N/A

**N/A - not applicable*

In addition to these benefits, there are challenges to using IP communication in LoWPANs that should be considered, though. The limited packet size requires compression of IPv6 headers and upper layers whenever possible. Since the simplified network protocols are required to detect services, including control and maintenance of the services provided by devices, the new protocols must be developed.

IEEE 802.15.4-2006 (*ZigBee*), specification defines the protocol architecture layers above the physical layer and the MAC sublayer. The most popular specification based on the IEEE 802.15.4 standard is ZigBee technology that operates in the 2.4 GHz frequency range with 250 kbps with a maximum number of nodes of 1024. ZigBee is a wireless technology (standard) used in many sensor networks. Due to the use of only one communication channel is unreliable [6], though. It can be used with 6LoWPAN and traditional internet protocols that provide additional features. The problem is that it does not support QoS, which is an interesting area of research with a focus on the application of IP multicasting solutions, queue management and traffic analysis techniques [43]. The topologies supported by ZigBee are the following: (a) star topology where the network is controlled by one device - ZigBee coordinator initializes and manages devices in the network, while end devices mutually communicate via ZigBee coordinator, (b) tree topology where ZigBee coordinator runs the network and selects the key parameters, while ZigBee router transmits data and control messages through the network using a hierarchical routing strategy, and (c) mesh topology that allows full communication of entities of the same level..

Z-Wave is based on the ITU G.9959 standard and represents a short-range RF communication technology primarily intended for home automation and data exchange between products such as controllers and sensors. It enables reliable communication of small packets with transfer speeds of 100 kbps. The interference of other wireless technologies in the range of 2.4 GHz with low power is avoided. This technology does not need a node coordinator and is highly customizable allowing control of up to 232 devices that also have additional slave nodes. Some communication devices have a range of up to 30 meters inside a building, and in open space allows range of up to 100 meters. The Z-Wave has several limitations compared to ZigBee including higher latency, though.

One of the most widely used short-range technologies is *IEEE 802.15.1 (Bluetooth)* that uses the ISM band. As a representative of low power and low-cost technology, it is suitable for data transfer between devices at short range for up to 10 meters. There are several versions that have been improved over time (Table 5). Bluetooth SIG (*Special Interest Group*) proposed BLE (*Bluetooth Low-Energy*) in the Bluetooth 4.0 specification, and later improved in the Bluetooth 5 specification [44] in order to allow data collection and aggregation from data-generating devices (sensors). The BLE is intended for short-range communication and is suitable for the control and monitoring applications. It is also known as the "Bluetooth Smart" protocol for short-range communication with low power consumption. Previous studies [45]–[49] have presented the BLE functionalities with the conclusion that this technology is a good option for specific IoT solutions with certain limitations mostly related to bandwidth and range. IETF 6LoWPAN WG has developed a specification that allows transmission of IPv6 packets over BLE [50], thus improving IoT capabilities. The Bluetooth 5 is focused on improvement of several functionalities: speed, range, security, energy efficiency, location-based functionality, and interoperability with other technologies. It increases the outdoors range for up to 200m and indoors for up to 40m, allowing the entire home wireless connectivity. The theoretical bandwidth of Bluetooth 5 is doubled from 1 Mbps to 2 Mbps, without increasing power consumption compared to BLE, resulting in extended battery life. Some specific IoT communication protocols have also been added to the BTIoT-5 (*Bluetooth IoT*) architecture.

WirelessHART is based on the HART communication protocol specifically designed for WSNs and actuators. The basic types of network devices include the following: (a) field devices that perform sensor or activation functions, (b) routers that must be able to route packets, (c) access points that connect a wireless network to a gateway, (d) a simple or redundant gateways that function as a bridge to applications, and (e) security managers usually exist as built into device or as separate devices.

ISA100.11a was developed by the International Society for Automation (ISA) and is designed to support a different set of needs of wireless industrial plants, including the process automation. ISA100.11a defines protocol stack, system management, and security functions for use over low-speed wireless networks and small power consumption (currently IEEE 802.15.4). It does not specify the automation process of the application layer protocol or interface for the existing protocol, but specifies tools for building the interface.

Table 5. Basic characteristics of Bluetooth technology

Characteristics	Bluetooth Classic	Bluetooth 4.x	Bluetooth 5
Certification	Bluetooth SIG		
Frequency (MHz)	2400-2483.5		
Media access control technique	FHSS (*Frequency-hopping spread spectrum*)		
Range (m)	Up to 100 m		Up to 200 m
Throughput (Mbps)	1-3 Mbps	1 Mbps	2 Mbps
Latency (ms)	<100 ms	<6 ms	<3 ms
Topology			
Number of active devices	7	Theoretically there is no limit	
Message size (bytes)	Up to 358	31	255

3.6 LP-WAN

LPWAN (*Low Power Wide Area Networks*) technologies are primarily developed for IoT applications that require high network coverage, low power consumption due to battery life, low device cost, etc. [51]. They aim to enable the transmission of data over long distances with the application of low power. They are suitable for communication within a distance of up to several kilometers in urban areas and a few tens of kilometers in rural areas. The long range of the wireless signal is achieved by reducing the possible data rate, using appropriate modulation techniques, etc. Many of the proposed LPWAN technologies are in the early stages of development, while some are already in widespread use. Table 6 present the most known LPWAN technologies including LoRaTM, LoRaWAN™ [52], Sigfox [53], NB-IoT (*Narrow-Band IoT*) [54], RPMA (*Random Phase Multiple Access*) [55], Wi-Fi HaLow [56] and LTE-M [57] [33], [41], [61]–[63], [52]–[56], [58]–[60]. The 5th generation mobile networks can also be included in this group. In many cases, these technologies are based on unlicensed spectrum, which has its advantages in terms of costs, but it also brings some challenges such as spectrum congestion.

LoRa is used to create a long-range communication link based on CSS (*Chirp Spread Spectrum*) modulation. By applying this modulation, the same low consumption characteristics as FSK (*Frequency-shift keying*) modulation are maintained, but a significantly longer communication range is achieved. The main advantage of the LoRa technology is the long range. Its name is derived from the English words "*Long Range*". *LoRaWAN*™ defines both the network layer protocol and the system architecture while the LoRa technology that defines only the physical layer that allows communication over long distances. At its core, it is an LPWAN technology specifically developed for battery-powered wireless devices with need to transmit data at low speeds over long distances in rural and urban areas. The speed of data transmission usually warries between 0.3 kbps and 50 kbps. It does not enable communication between devices, but only two-way communication between devices and servers. The battery life of these devices is predicted to be more than 10 years due to low power consumption.

SigFox is one of the most widely used LPWAN technologies. It was named after the French global manufacturer of IoT network equipment intended exclusively for long ranges. SigFox is a narrowband technology that uses BPSK (*Binary phase-shift keying*) modulation. Each access point supports up to a million devices with the ability to cover large rural and urban areas. It allows connection of remote devices using UNB (*Ultra-Narrow Band*) technology and short messages. A packet size is limited to 150 messages with 12 bytes per day, while packets in the downlink are limited to four messages with 8 bytes per day. This is sufficient for many IoT applications. Sigfox devices are characterised with a low manufacturing cost.

NB-IoT (Narrowband IoT) technology is designed to achieve excellent coexistence with legacy GSM, GPRS and LTE technologies. It is a narrowband LPWAN technology standardized by 3GPP for networks with minimum power consumption in order to use in applications that require exchange of small amounts of data. There are two versions presented: CAT-NB1 (Rel 13) and CAT-NB2 (Rel 14). Both versions are characterized by low data transfer rate in uplink and downlink along with high reliability. NB–IoT was developed to enable connection of many devices via mobile telecommunications bands. The key advantages of NB-IoT compared to other similar technologies are area coverage and long battery life. Another advantage is the possibility to operate on the existing LTE and GSM infrastructure allowing mobile service operators to quickly add a mobile intelligent internet connection to the services they provide. Since NB-IoT operates in the licensed spectrum as LTE, it also enables secure and reliable transmission. It can be used to connect many devices distributed over large geographical areas with minimal power consumption and without the need for frequent battery replacement. NB–IoT technology is designed to achieve excellent coexistence with legacy GSM, GPRS and LTE technologies.

Table 6. An overview of LPWAN technologies

Technology	Standard	Frequency	Bandwidth	Throughput	Range
LoRaWAN	LoRa-Alliance	ISM (EU: 868 MHz, USA: 433/915 MHz, AS: 433 MHz)	250 kHz i 125 kHz	50 kbps	5 km (urban) 40 km (rural)
Sigfox	Sigfox in cooeration with ETSI	ISM (EU: 868 MHz, USA: 433/915 MHz, AS: 433 MHz)	100 Hz, 600 Hz in North America	100 bps (UL) 600 bps (DL)	10 km (urban) 40 km (rural)
NB-IoT	3GPP	Licenced 2G/3G/4G frequency range (prefered LTE spectrum)	180 kHz ili 200 kHz	250 kbps	1 km (urban) 20 km (rural)
RPMA	Ingenu	Non-licenced ISM spectrum (2.4 GHz)	1 MHz	80 kbps	15 km
Wi-Fi Hallow	IEEE 802.11 ah	Sub-1GHz (700-900 MHz)	1-16 MHz	40 Mbps	1 km
LTE-M	3GPP	Licenced spectrum (700-900 MHz)	1.4-20 MHz	1 Mbps	5-11 km

**UL – Uplink, DL – Downlink, EU (Eurpme), USA (United States of America), AS (Asia)*

LTE-M ili *LTE-MTC LPWA* is a technology standardized by 3GPP in Rel. 13 specification suitable for application in IoT systems due to support for simple devices with a large coverage area, lower power consumption and utilization of LTE infrastructure. With a requirement to enable battery life of up to 10 years, the PSM (*Power Saving Mode*) mechanism has been implemented. During the operation in PSM mode, the LTE-M device is not unavailable, which leads to extremely low battery consumption, even lower than competing LPWAN technologies like Sigfox or LoRaWAN. Additionally, it supports relatively fast data transfer, mobility and roaming, and operation in a licensed frequency spectrum, where interference is not as much present as in the unlicensed spectrum.

RPMA (*Random Phase Multiple Access*) is a random-access technology developed by Ingenu. It offers data transmission in the 2.4 GHz spectrum and uses DSSS (Direct Sequence Spread Spectrum) transmission technology, a method of spectral propagation which was used by the military for the purpose of secure data transmission. The spectrum used is Due to the use of this spectrum, it is prone to interference from other technologies that use the same spectrum. Usually consumes higher power than other LPWAN options. The RPM protocol for IoT is intended exclusively for communications between devices over long distances, with the range dependent on optical visibility. It provides offerbetter two-way communication compared to other LPWAN technologies, such as SigFox.

WiFi HaLow was developed by the Wi-Fi Alliance which proposed a new 802.11ah standard with the aim of enabling devices to connect with a larger range compared to Wi-Fi and with lower power consumption. It enables data transfer at higher speeds compared to other mentioned technologies with a range of up to one kilometer. Some of the advantages of this technology is the fact that it takes advantage of the huge base of already installed Wi-Fi devices, which is the key reason why it is expected to grow and become popular within the IoT. Another key advantage of this technology is the interoperability with existing and future devices that support Wi-Fi. Consequently, an IoT device or a sensor with support for WiFi HaLow technology (integrated HaLow module) is able to connect to a Wi-Fi access point, which leads to further forwarding data via the Internet.

4 Mobile communication technologies

Many IoT applications rely on data transmission over mobile systems, such as 2G (GSM, D-AMPS, PDC), 2.5G (GPRS), 2.75G (EDGE), 3G (UMTS / WCDMA, HSPA, HSUPA, EVDO) and 4G (LTE, LTE-A). The development of certain applications is also conditioned by the development of 5G technologies. IoT connectivity in the context of cellular networks is known as M2M (*Machine-to-Machine*) or MTC (*Machine-type Communication*) within 3GPP. The 3G and 4G technologies such as 3GPP LTE enable wide area coverage, support for QoS, mobility and roaming, scalability, high level of security, ease of management, as well as sensor connectivity through a standardized API

[6]. LTE-A (*Long Term Evolution - Advanced*) and mobile WiMAX Release 2 (*Wireless MAN - Advanced* or *IEEE 802.16m*) provide higher speeds and scalability as well as low costs. These technologies meet most IoT requirements with some open issues and challenges such as QoS and network congestion due to the large number of nodes/devices [64].

To meet the growing demands of the IoT market, which includes the need to overcome the problem of technology fragmentation and the corresponding challenge of ensuring interoperability, the 3GPP has made related improvements through Release-13 and Release-14. The same purpose has eMTC (*enhanced Machine-Type Communication*), NB-IoT, and EC-GSM-IoT. The eMTC brings technology enhancements to LTE in order to adjust MTC, such as PSM (*Power Save Mode*) to improve energy efficiency. Release-14 also proposes new features for eMTC, for example: (a) support for positioning (location services and multicast), (b) protocol optimization and (c) higher data rates [59]. Other Release-14 enhancements are related to NB-IoT: (a) support for multicast, (b) reduction of latency, (c) reduction of power consumption, and (d) improvement of the mobility and reliability necessary for service continuity, etc.

Table 7. Evolution of mobile communication technologies (1G to 5G)

Generation	Access technology and switching	Requency	Bandwidth	Throughput
1G	AMPS (*Advanced Mobile Phone Service*) FDMA (*Frequency Devision Multiple Access*) komutacija kanala	800 MHz	30 KHz	2.4 kbps
2G	GSM (*Global System for Mobile Communications*) TDMA (*Time Devision Multiple Access*) channel comutation	850/900/ 1800/1900 MHz	200 KHz	10 kbps
	CDMA (*Code Devision Multiple Access*) channel comutation		1.25 MHz	10 kbps
2.5G	GPRS (*General Packet Radio Service*) channel/packet comutation		200 KHz	50 kbps
2.75G	EDGE (*Enhanced Data rates for GSM Evolution*) channel/packet comutation		200 KHz	200 kbps
3G	UMTS (*Universal Mobile Telecommunications System*) / WCDMA (*Wideband Code-division multiple access)*, channel/packet comutation	850/900/1800/ 1900/2100 MHz	5 MMHz	384 kbps
	CDMA (*Code-division multiple access) 2000* channel/packet comutation		1.25 MHz	384 kbps
3.5G	HSPA (*High Speed Packet Access*): HSUPA (uplink) / HSDPA (downlink) packet comutation		5 MHz	5-30 Mbps
	EVDO (*Evolution-Data Optimized*) packet comutation		1.25 MHz	5-30 Mbps
3.75G	LTE (*Long Term Evolution*) OFDMA *Orthogonal frequency-division multiple access)* / SC-FDMA (*Single carrier frequency-division multiple access),* packet comutation	1.8/2.6 GHz	1.4-20 MHz	100-200 Mbps
	WIMAX (*Worldwide Interoperability for Microwave Access*) – Fixed WIMAX SOFDMA (*Scalable Orthogonal Frequency Division Multiple Access*), packet comutation	3.5/5.8 GHz	3.5 i 7 MHz za 3 .5 GHz / 100 MHz za 5.8 GHz	100-200 Mbps
4G	LTE-A (LTE Advanced) OFDMA *Orthogonal frequency-division multiple access)* / SC-FDMA (*Single carrier frequency-division multiple access)*, packet comutation	1.8/2.6 GHz	1.4-20 MHz	DL: 3 Gbps UL: 1.5 Gbps
	WIMAX (*Worldwide Interoperability for Microwave Access*) – Mobile WIMAX SOFDMA (*Scalable Orthogonal Frequency Division Multiple Access*), packet comutation	2.3/2.5/3.5 GHz	3.5/5/7/8.5/10 MHz	100-200 Mbps
5G	BDMA (*Beam Division Multiple Access*) FBMC (*Frequency Division* Multiple Access *for Filter Bank Multicarrier*), packet comutation	1.8/2.6 and 30-300 (*) GHz	60 GHz	10-50 Gbps (*)

UL – uplink, DL – Downlink, (*) – expected values

EC-GSM-IoT proposes EGPRS improvement that enables the application of GSM / EDGE technologies for IoT systems combined with PSM. The improvements include: (a) rank extensions (signal coverage), (b) support for a large number of devices (at least 50,000 per cell), (c) security enhancements, and more. An overview of eMTC, NB-IoT and EC-GSM-IoT is given in the 3GPP IoT Report [58].

The development of 3GPP (*3rd Project Generation Partnership*) technologies has made it possible to overcome some of the key IoT challenges. However, some other open issues remain, such as providing QoS in conditions of network congestion due to the large number of devices [64]. The continuous improvements have contributed to improving the performance of these technologies, though. Table 7 presents an overview of some of the basic characteristics of the 1G-5G system.

The global perspective of 5G (*5th Generation Mobile Networks or 5th Generation Wireless Systems*) considers the capabilities listed in ITU-R M.2083-0 and connects them in the following use cases: mobile broadband networks, extensive device-to-device communications, and sensitive (critical) communications which should enable utilization of potential of the IoT paradigm. 3GPP Release 15 and Release 16 are focused on a set of new 5G standards as well as LTE-Advanced Pro specifications. Their aim is to include performance analysis according to the requirements of mMTC (*massive Machine Type Communications*), specifications for eMBB (enhanced Mobile Broadband), URLLC (*Ultra-Reliable and Low Latency Communications*), etc. The detailed overview of 5G cellular architecture and technologies such as spectrum sharing with cognitive radio, interference management, cloud computing, SDN, etc. is given in [4].

There are authors [65] that claims about strong relationship and overlap between the development of 5G and IoT systems. The main goal of 5G systems is support to the required bandwidth and speeds for a large number of devices with lower power consumption and cost reduction. The work on 5G design aims to support a large number of devices to enable global IoT deployment with lower power consumption and lower costs. 3GPP has worked to support M2M applications, but there are still a number of challenges such as issues related to energy efficiency and battery life, cost and spectrum costs, coverage, user identification, security enhancement, QoS support, complexity, IoT diversity application (traffic models), etc.

Enabling D2D (*Device-to-Device*) communications (data exchange without the inclusion of BS - base station or with partial BS assistance) is one of the milestones in the cellular system [66]. Also, the design of 5G networks is related to other open issues [67] related to areas such as mobile cloud computing systems, context-aware services, interference avoidance, QoS management, etc.

5 Conclusion

There are many devices connected to the Internet using different wireless technologies. IoT needs to enable seamless connectivity of any device, anytime, anywhere and by anyone. One of the challenges is the high network load due to the constant increase in traffic requirements. Therefore, there is an issue of achieving the required QoS performance, energy efficiency, and optimizing the usage of available system resources. New technologies and improvements should overcome some of these issues. One of the components of an IoT system are wireless communication technologies. Some wireless technologies have been developed due to new traffic models and the growing demands for bandwidth, QoS performance, energy efficiency, mobility, security, etc. There are also new network protocols developed witin all layers of the TCP / IP model, as well as some non TCP/IP protocols. Usually, existing protocols are not adopted for IoT applications. For example, the application of traditional protocols can cause high power consumption on battery-powered devices. Therefore, new architectures have been developed and some existing protocols are improved. This paper presents some of the most widely used wireless technologies for IoT applications. We summarized the current state-of-the-art IoT wireless communication technologies in order to provide a comprehensive list of their characteristics as well as some open issues. However, all the improvements led to new challenges. For example, great diversity in network technologies causes interoperability issues. Also, a significant issue includes the need for new traffic models, improvement of existing and development of new mechanisms to ensure QoS performance, etc. Along with above presented open issues, in IoT networks, security is much more critical and compulsory than in traditional networks. All these issues need to be considered in the future development of wireless technologies for the IoT.

References

[1] A. Čolaković and M. Hadžialić, “Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues,” *Computer Networks*, vol. 144, pp. 17–39, 2018.

[2] M. H. Miraz and M. Ali, “A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet of Nano Things (IoNT),” in *Internet Technologies and Applications (ITA)*, 2015, pp. 219–224.

[3] D. Singh, G. Tripathi, and A. J. Jara, “A Survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services,” in *IEEE World Forum on Internet of Things 2014*, 2014, pp. 287–291.

[4] A. Gupta and R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,” *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[6] M. R. Palattella *et al.*, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[7] E. Soltanmohammadi, K. Ghavami, and M. Naraghi-Pour, "A Survey of Traffic Issues in Machine-to-Machine Communications Over LTE," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 865–884, 2016.

[8] G. Aloi, G. Caliciuri, G. Fortino, and R. Gravina, "Enabling IoT interoperability through opportunistic smarthpone based mobile gateways," *Journal of Network and Computer Applications*, vol. 81, pp. 74–84, 2016.

[9] B. Soret, K. I. Pedersen, N. T. K. Jorgensen, and V. Fernández-López, "Interference coordination for dense wireless networks," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 102–109, 2015.

[10] J. G. Andrews, "Seven ways that HetNets are a cellular paradigm shift," *IEEE Communications Magazine*, vol. 51, no. 3, pp. 136–144, 2013.

[11] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, "Green Internet of Things for Smart World," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.

[12] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University -- Computer and Information Sciences*, 2016.

[13] H. Hada and J. Mitsugi, "EPC based internet of things architecture," in *IEEE International Conference on RFID-Technologies and Applications*, 2011, pp. 527–532.

[14] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *International Conference on Advances in Energy Engineering*, 2010, pp. 69–72.

[15] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, and M. Zorzi, "Architecture and protocols for the Internet of Things: A case study," in *8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2010, pp. 678–683.

[16] S. Hong *et al.*, "SNAIL: an IP-based wireless sensor network approach to the internet of things," *IEEE Wireless Communications*, vol. 17, pp. 34–42, 2010.

[17] F. Andreini, F. Crisciani, C. Cicconetti, and R. Mambrini, "Context-aware location in the Internet of Things," in *2010 IEEE Globecom Workshops*, 2010, pp. 300–304.

[18] G. Pujolle, "An Autonomic-oriented Architecture for the Internet of Things," in *Modern Computing, 2006. IEEE JVA '06*, 2006.

[19] IETF, "Transmission Control Protocol," *IETF RFC 793*, pp. 1–85, 1981.

[20] IETF, "User Datagram Protocol," *IETF RFC 768*, pp. 1–3, Aug. 1980.

[21] I. (R. Hamilton, J. Iyengar, I. Swett, and A. Wilk), "QUIC: A UDP-Based Secure and Reliable Transport for draft-tsvwg-quic-protocol-02," *Internet-Draft*, pp. 1–37, 2016.

[22] I. (Z. Shelby, M. Huttunen, M. Saarnivala, J. Riihijärvi, O. Raivio, and P. Mähönen), "nanoIP," *Internet-Draft*, pp. 1–10, 2005.

[23] I. (E. Rescorla and N. Modadugu), "Datagram Transport Layer Security," *IETF RFC 4347*, pp. 1–25, Apr. 2006.

[24] A. J. Jara, L. Ladid, and A. Skarmeta, "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 4, no. 3, pp. 97–118, 2013.

[25] IETF, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *IETF RFC 6550*.

[26] I. (N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," *IETF RFC 4919*, pp. 1–12, Aug. 2007.

[27] I. (J. Hui and P. Thubert), "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," *IETF RFC 6282*, pp. 1–24, 2011.

[28] I. (B. Campbell and H. Tschofenig), "An IETF URN Sub-Namespace for OAuth," *IETF RFC 6755*, vol. 6755, pp. 1–5, 2012.

[29] M. R. Palattella *et al.*, "Standardized Protocol Stack for the Internet of (Important) Things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2012.

[30] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

[31] L. Chunli and L. Donghui, "Application and development of RFID technique," in *2nd International Conference on Consumer Electronics*, 2012, pp. 900–903.

[32] Y. Choi, Y. Choi, D. Kim, and J. Park, "Scheme to guarantee IP continuity for NFC-based IoT networking," in *19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 695–698.

[33] L. Oliveira, J. J. P. C. Rodrigues, S. A. Kozlov, R. A. L. Rabêlo, and V. H. C. de Albuquerque, "AC Layer Protocols for Internet of Things: A Survey," *Future Internet*, vol. 11, no. 1, pp. 1–42, 2019.

[34] U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T.

Kamal, "Review on Internet of Things (IoT)," *nternational Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, 2015.

[35] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[36] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11AH: the WiFi approach for M2M communications," *IEEE Wireless Communications*, vol. 21, pp. 144–152, 2014.

[37] E. Khorov, A. Krotov, and A. Lyakhov, "Modelling machine type communication in IEEE 802.11ah networks," in *IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1149–1154.

[38] I. Std, "WG802.11 - Wireless LAN Working Group," *802.11ah-2016*, 2016.

[39] A. M. S. Abdelgader and W. Lenan, "The Physical Layer of the IEEE 802.11p WAVE Communication Standard: The Specifications and Challenges," in *WCECS 2014*, 2014, pp. 22–24.

[40] W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz," *Journal of ICT Standardization*, vol. 1, no. 1, pp. 83–108, 2013.

[41] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.

[42] IEEE, "802.15.4 IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Standard - WG 802.15*, 2020.

[43] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. Mohammadi, "Toward better horizontal integration among IoT services," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 72–79, 2015.

[44] B. S. I. G. (SIG), "At the core of everything Bluetooth." 2019.

[45] S. Raza, P. Misra, Z. He, and T. Voigt, "Bluetooth smart: An enabling technology for the Internet of Things," in *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 155–162.

[46] J. DeCuir, "Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies," *IEEE Consumer Electronics Magazine*, vol. 3, no. 1, pp. 12–18, 2014.

[47] R. Frank, W. Bronzi, G. Castignani, and T. Engel, "Bluetooth Low Energy: An alternative technology for VANET applications," in *11th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, 2014, pp. 104–107.

[48] E. Mackensen, M. Lai, and T. M. Wendt, "Bluetooth Low Energy (BLE) based wireless sensors," in *Sensors*, 2012, pp. 1–4.

[49] M. O. Al Kalaa, W. Balid, N. Bitar, and H. H. Refai, "Evaluating Bluetooth Low Energy in realistic wireless environments," in *IEEE Wireless Communications and Networking Conference*, 2016, pp. 1–6.

[50] I. (J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez), "IPv6 over bluetooth(r) low energy," *IETF Draft*, pp. 1–21, Aug. 2015.

[51] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *Communications Surveys & Tutorials*, vol. 144, p. 1, 2017.

[52] L. Alliance, "What is the LoRaWAN® Specification?" 2021.

[53] Sigfox, "Sigfox Technology." 2021.

[54] 3GPP, "Standardization of NB-IOT," 2016.

[55] I. Inc, "Random Phase Multiple Access technology." 2021.

[56] W.-F. Alliance®, "Wi-Fi HaLow." 2021.

[57] GSMA-White-Paper, "3GPP Low Power Wide Area Technologies."

[58] 3GPP, "Progress on 3GPP IoT," 2016.

[59] 3GPP, "Release 14," 2017.

[60] K. Mekki, E. Bajic, and F. M. F. Chaxel, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, pp. 1–7, 2018.

[61] D. Ismail, M. Rahman, and A. Saifullah, "Low-power wide-area networks: opportunities, challenges, and directions," in *Workshops ICDCN*, 2018, pp. 1–6.

[62] M. Chen, Y. Miao, X. Jian, X. Wang, and I. Humar, "Cognitive-LPWAN: Towards Intelligent Wireless Services in Hybrid Low Power Wide Area Networks," *IEEE Transactions on Green Communications and Networking*, pp. 1–9, 2018.

[63] R. Sanchez-Iborra and M.-D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors*, vol. 16, no. 5, pp. 1–14, 2016.

[64] M. Hasan, E. Hossain, and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," *Communications Magazine*, vol. 51, pp. 86–93, 2013.

[65] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The tactile internet: vision, recent progress, and open challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 138–145, 2016.

[66] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *Communications Magazine*, vol. 52, pp. 86–92, 2014.

[67] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, "5G Backhaul Challenges and Emerging Research Directions: A Survey," *Access*, vol. 4, pp. 1743–1766, 2016.