A Review on Internet of Things: Communication Protocols, Wireless Technologies, and Applications

Meenu Garg, Gurjinder Kaur, Gurmehr Singh, Gursharan Sandhu, Sheifali Gupta, Soumya Ranjan Nayak, and Muhammad Fazal Ijaz

Abstract Internet of things (IoT) is a cloud-based "extensive global network" that connects numerous devices. Various devices are connected to the Internet for acquiring and storing the data. With the growth of technology, wireless networks, and affordable computer chips, everything can be integrated into the IoT. Wireless IoT can utilize a variety of different wireless communication technologies and protocols to connect various smart devices. Recent advancements in communication protocols and data processing permit the description of a new sort of restricted communication in terms of how objects communicate with one another on the Internet of things. This review paper presents a novel classification for the various traditional IoT network protocols and highlights different wireless IoT technologies along with their applications. In addition, comparative analysis of different features of IoT communication protocols is also presented.

M. Garg · G. Kaur · G. Singh · G. Sandhu · S. Gupta
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: meenu.garg@chitkara.edu.in

G. Kaur
e-mail: gurjinder.kaur@chitkara.edu.in

G. Singh
e-mail: gurmehr172118.ece@chitkara.edu.in

G. Sandhu
e-mail: gursharan172119.ece@chitkara.edu.in

S. Gupta
e-mail: sheifali.gupta@chitkara.edu.in

S. R. Nayak (✉)
Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India
e-mail: nayak.soumya17@gmail.com

M. F. Ijaz
Department of Intelligent Mechatronics Engineering, Sejong University, Seoul 05006, South Korea
e-mail: fazal@sejong.ac.kr

S. Dhar et al. (eds.), *Advances in Communication, Devices and Networking*, Lecture Notes in Electrical Engineering 902, https://doi.org/10.1007/978-981-19-2004-2_23

Keywords Internet of things · IoT protocols · IoT wireless technologies · IoT applications

1 Introduction

The Internet of things (or IoT) is a combination of traditional fields such as embedded systems, control systems, and automation that permits the automatic transmission of data across a network without human interaction. Sensors and actuators embedded in physical things communicate via wired and wireless networks, which usually use the same Internet protocol (IP) that connects the Internet. After Kevin Ashton presented a completely new technology called "radio frequency identification" (or RFID) at Procter and Gamble, the term "Internet of things" (or IoT) was coined. The Internet of things (IoT) is based on the concept of ubiquitous communication [1]. IoT devices enable everyday things to communicate with humans and provide continuous support. The Internet and other devices can be accessed via wireless technologies such as Wi-Fi, Bluetooth, ZigBee, and RFID. The collected data will be processed, kept, and examined by the user. It has seen the IoT's potential in the commercial and industrial development of prospering areas. However, data security is a major concern and a tremendous challenge [2]. The Internet has opened several channels for hackers, resulting in data vulnerabilities. However, IoT is committed to delivering the most effective solutions for dealing with this information and its security concerns. In addition, creating a secure method to communicate between social networks and privacy concerns is a big difficulty in IoT. There are numerous wireless technologies available today that operate in the roughly 2.4 GHz ISM band. Wireless devices are exploding in popularity. Thus, at a broad range of applications, the replacement of wires with wireless technology is also underway. For example, Bluetooth is being used to replace cable connections between desktop computers and external devices, while ZigBee is being used to monitor systems that require low energy consumption.

2 Literature Review

The Internet of things (or IoT), being an alarming technology and with the widespread anomalous research interest, presents qualitative work that copes with different factors of standardization in IoT. A lot of work has been done constantly to focus on abundant factors of standardization associated with IoT. Numerous Internet of things applications are already accessible, owing to the fact that a large number of individuals worldwide working in a related industry. Akyildiz et al. [3] made an exclusive IoT prototype, for the development of a bus transportation system in Singapore. With the help of this model, the customer can easily identify and estimate the available bus options for any particular destination, and it also gives an idea about the arrival timing and crowd on the bus. Sharma et al. [4] proposed a unique IoT-based model, using virtual components for the replacement of the advertising system in large shopping centers and in many more organizations. A humidity controller is also a part of this model, which maintains the humidity inside the shopping malls and organizations without any human effort. Elkhodr et al. [5] highlighted the exceptional characteristics of wireless technologies and the problems with their integration into the IoT. Specifically, it concentrates on Bluetooth low energy, ZigBee, LoRa, and a number of distinct versions of Wi-Fi. Chen et al. [6] examined the efficiency of various IoT protocols in healthcare settings, including CoAP, DDS, MQTT, and UDP. The efficiency of the various protocols is evaluated using a network emulator. This emulator enabled the author to simulate a system with a high latency and a low bandwidth. The scientists compared the performance of the protocols and concluded that DDS's higher bandwidth consumption, high dependability, and data latency make it the optimal choice for healthcare applications. Al-Sarawi et al. [7] examined the issue of selecting the most appropriate technology for a certain application. Thus, a comparison of the general communication protocols used in IoT using diverse criteria has been conducted. Topology, cryptography, power consumption, standards, frequency ranges, data rate, features, security, and range are some of the criteria. According to the author by comparing the protocols, they can determine which one is feasible for a particular function. Alavi et al. [8] stated issues rose due to urbanization in the metropolis. The authors concluded that IoT-enabled technology is essential for smart city expansion to solve certain issues such as waste collection and traffic management.

This paper aims to provide an extensive review to explain all the predominant protocols and also provide newly arising standards protocols as shown in Fig. 1 The presented work exclusively gives an extensive overview of all the various IoT communications protocols, technologies, and their applications. The rest of the paper is structured as follows: The existing IoT protocols are summarized in Sect. 3, followed by IoT wireless technologies in Sects. 4 and 5 present the conclusion of the present work.

3 IoT Protocols

All IoT devices communicate using specific regulating protocols. These protocols are a set of rules that govern how data is transmitted to and from the Internet. They ensure that data from a device or sensor is read and interpreted by one device or sensor and not by another [9]. There are numerous procedures, all of which are briefly addressed in the paper below.

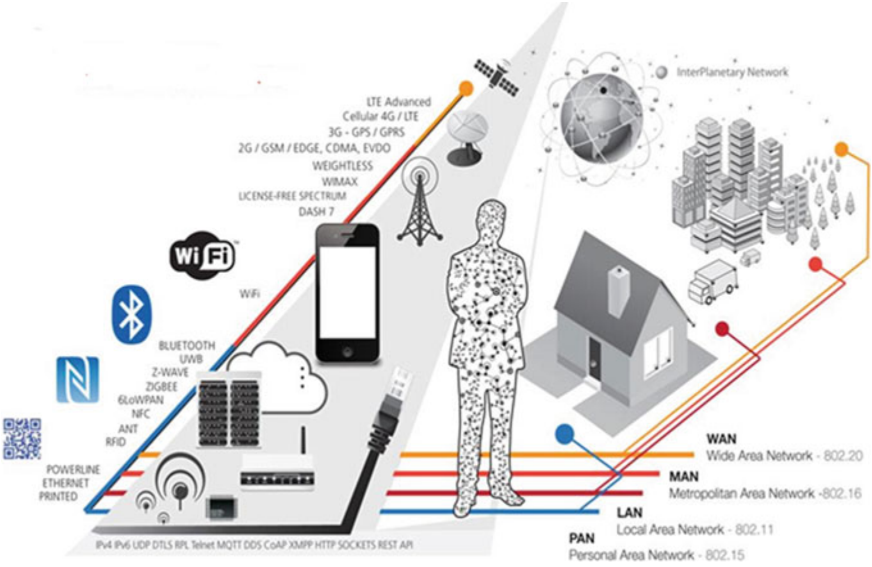

LTE Advanced
Cellular 4G / LTE
3G - GPS / GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
WiFi
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
InterPlanetary Network
WAN
Wide Area Network - 802.20
MAN
Metropolitan Area Network -802.16
LAN
Local Area Network - 802.11
PAN
Personal Area Network - 802.15

Fig. 1 IoT communication protocols and technologies

3.1 The Internet Protocol Version Four (IPv4)

The Internet protocol, or IP, is a unique numerical identifier assigned to each device connected to a larger computer network. It is used for a wide variety of functions and is further classified into two types: IPv4 and IPv6. IPv4 is the fourth generation of the Internet protocol, which was released in 1981 and is widely used in data communication [10]. It is a connectionless protocol that is implemented in packet switching layer networks. Typically, this 32-bit addressing mechanism is denoted by dot-decimal notations. 32-bit addressing is typically used in IPv4 in five classes, namely A, B, C, D, and E. The classes A to C use distinct bit lengths to define the network host. Pre-allocations of classes D and E have been made for military and future use, respectively. IPv4 can be configured with a wide variety of devices, either manually or automatically, depending on the network type.

3.2 Internet Protocol Version Six (IPv6)

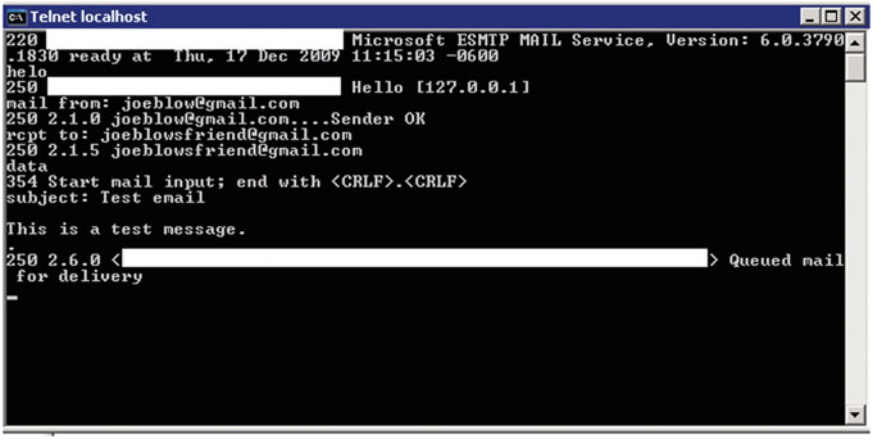
IPv6 is the most recent version of the Internet protocol; it is essentially an upgrade to IPv4. It was created in 1998 by the Internet engineering task force (IETF) to address the long-predicted issue of IPv4 address exhaustion. IPv6 addresses are 128 bits in length and include both source and destination addresses [11]. Addresses are divided into eight groups by colons or hexadecimal characters. Along with increased address space, IPv6 supports hierarchical address assignment methods, which reduces the expansion of routing tables. IPv4 and IPv6 are both compatible and have no linkages.

3.3 User Datagram Protocol (UDP)

Designed by David P. Reed in 1980, UDP is known as one of the most essential members of the IP suite. It is an unreliable and simple connectionless protocol and offers a minimal transport facility to the applications that do not use the level of service of TCP [12]. The only service it gives is checksums for received data incorruptibility and multiplexing by port numbers to address different functions at the starting place and target of the datagram. UDP is mainly useful for concurrent services like gaming and voice/video communication. As great functioning is required in these services, UDP permits the packets to be dropped rather than handling the ones which are delayed. Also, quite a lot of bandwidth is saved as no error checking is done by UDP, thus making it very efficient in terms of both latency and bandwidth.

3.4 Teletype Network

Telnet is an application protocol that enables users to communicate in a bidirectional, eight-bit format. It was developed in 1969 and included a command-line interface (CLI) for communicating with remote hosts, as illustrated in Fig. 2. Telnet is an acronym for teletype network, and the verb "to telnet" may also be used [13]. The Telnet application allows users to run commands on the server, allowing users to



```
220 [redacted] Microsoft ESMTP MAIL Service, Version: 6.0.3790
.1830 ready at  Thu, 17 Dec 2009 11:15:03 -0600
helo
250 [redacted] Hello [127.0.0.1]
mail from: joeblow@gmail.com
250 2.1.0 joeblow@gmail.com....Sender OK
rcpt to: joeblowsfriend@gmail.com
250 2.1.5 joeblowsfriend@gmail.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: Test email

This is a test message.
.
250 2.6.0 <[redacted]> Queued mail
 for delivery
_
```

Fig. 2 Telnet CLI

operate it and communicate with other servers on the network. Telnet is frequently used to provide remote access to multi-user dungeon (MUD) games and secure internal connections, as well as to test web and mail servers.

3.5 Datagram Transport Layer Security (DTLS)

DTLS is used to secure datagram-based communications. DTLS provides communication security for datagram protocols and is based on TLS with a few modifications to address issues caused by packet rearrangement or loss. DTLS does not guarantee message delivery in any particular order, or even that messages will be delivered at all. As the DTLS protocol uses UDP, it thus deals with packet reordering, datagram loss and data being pretty larger in size than that of a network packet [14]. It is used for web browsing, mail, instant messaging, and voice over IP (VoIP).

3.6 Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is a routing protocol designed for wireless networks with minimal power consumption and a strong probability of packet loss. It is a demanding protocol based on distance vectors that operate on IEEE 802.15.4 and were designed for multi-hop and many-to-one communication as well as one-to-one messaging. This protocol can quickly construct network routes, disseminate routing knowledge, and efficiently adapt the topology.

3.7 Message Queuing Telemetry Transport (MQTT)

MQTT is a featherlight publish/subscribe messaging protocol developed for devices and networks that are strained due to excessive latency, low bandwidth, or instability. It was invented by Dr. Andy Stanford-Clark and Arlen Nipper in 1999. The MQTT design principles were developed in such a way that they minimize network bandwidth and device resource needs while ensuring soundness and some level of delivery assurance. Thus, MQTT is primarily designed for connections with a remote site that require a “minimal code footprint” or that have a limited network capacity.

3.8 Data Distribution Service (DDS)

DDS is a data communications model for machine-to-machine (M2M) communication. The DDS integrates system components, resulting in low-latency data transfer, high accuracy and an extendable architecture required for crucial IoT applications that require real-time data interchange. It completely removes the requirement for network programming that manages communications which automates their interaction.

3.9 Constrained Application Protocol (CoAP)

CoAP is a protocol for the service layer that is used with managed nodes and networks. These nodes are equipped with 8-bit microcontrollers and a tiny amount of read-only memory (ROM) and Random Access Memory (RAM). It implements a request/response mechanism for application interaction and includes built-in services and resources. The protocol is primarily targeted at hardware that cannot run HTTP, such as 8-bit microcontrollers, or TLS, as well as low-power sensors [15].

3.10 Extensible Messaging and Presence Protocol (XMPP)

The extensible messaging and presence protocol (XMPP) is a free and open set of technologies for real-time communication. This enables real-time communication and powers a wide variety of applications, including instant messaging. It collectively means:

- **X (Extensible)**: This indicates that it can be customized or expanded to meet specific requirements.
- **M (Messaging)**: This protocol is optimized for real-time messaging and features a very competent push mechanism in comparison with other protocols
- **P (Presence)**: It indicates if you are online, offline, or occupied in another way.
- **P (Protocol)**: A protocol is a collection of standards that enable systems to communicate with one another.
- This protocol is used to communicate with VoIP systems, publish–subscribe systems, file transfer systems, and gaming systems, among others.

3.11 Sockets

These are forms of communication that enable the flow of data both locally and across networks. Sockets are classified into four types:

- **Stream Sockets**: If you send three things “A, B, C” through a stream socket, they will arrive in the exact same order as they were sent. These sockets make use of TCP for data delivery. If delivery is not completed, the sender is notified of the failure.
- **Datagram Sockets**: These are connectionless sockets because they do not require an open network to function and instead use UDP.
- **Raw Sockets**: They enable the use of socket abstractions in basic communication protocols. They are useless to the general public and have been supplied solely to persons interested in inventing new protocols or acquiring access to multiple complex protocol facilities. They enable the user to edit a packet’s headers using the sequenced packet protocol (SPP) or the Internet datagram protocol (IDP), as well as to receive the headers on incoming packets.

3.12 Representational State Transfer (REST)

REST, as defined by Roy Fielding in 2000, is a collection of rules and regulations that specify how Web standards (e.g., HTTP and URIs) should be utilized. It is mostly famous for its simplicity and the concept upon which it is built-in order to accomplish its goals. RESTful Web services are services that adhere to the REST architectural style and enable Internet-based interoperability between computer systems. They allow the system to interact with textual representations of Web resources [9].

RESTful systems strive for stability, rapid performance, and extensibility through the reuse of components that may be controlled and updated separately from the rest of the system through the use of a stateless protocol and standard operations. To aid comprehension, Fig. 3 summarizes the REST-based messaging system.

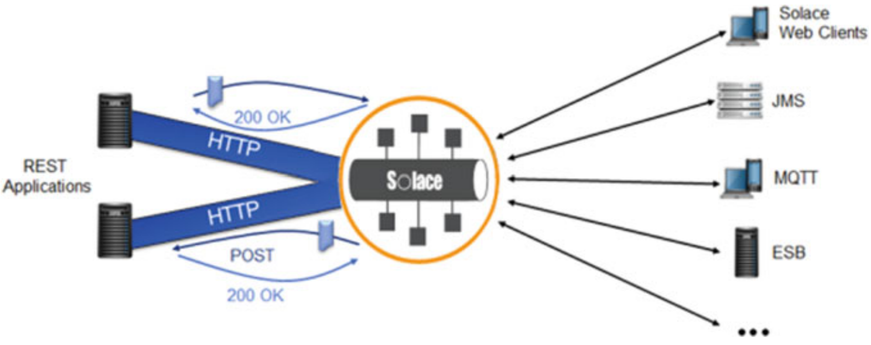


Fig. 3 REST messaging protocol

3.13 Application Programming Interface (API)

An API is a computing interface which influences interactions between numerous software mediators. It is basically a group of routines, protocols, and means for creating software applications. It defines the types of calls or requests that can be made, how we form them, the data formats that can be used, the conventions that must be followed, and so on. It also provides extension techniques so that users can extend current performances in numerous ways and to varying degrees [16].

The names of the OSI model layers, their data units, the TCP/IP model, function, and TCP/1P protocols for the particular layers are mentioned in Table 1

Table 1 Layers of model

OSI model layers	Data units	TCP/IP model	Function	TCP/IP protocols
Application layer	Data	Application	Produced the data, which has to be transferred over the network	CoAP, MQTT, XMPP
Presentation layer	Data	Application	Data extraction and manipulation as needed	FTP
Session layer	Data	Application	Established connections between two processes	API
Transport layer	Segments	Transport	Provide the acknowledgment after the complete data transmission, and re-transmit the data if an error occurs	DTLS, DDS, sockets
Network layer	Packets	Internet	Transfer data from one host to another across multiple networks	IPv4, IPv6, UDP, RPL, 6L0WPAN
Data link layer	Frames	Network access	Ensure that data is transmitted from one node to another without errors	Teletype network
Physical layer	Bits	Network access	Transmit bits from one node to another	Z-Wave, UWB, PLC

4 IoT Wireless Technologies and Applications

4.1 Wi-Fi

Wireless fidelity (Wi-Fi) belongs to the family of wireless networks, and it is based upon IEEE 802.11 standard, which are mostly used for LAN networking of devices and Internet access. Wi-Fi is a type of WLAN network. The only drawback of it is that it consumes a lot of power for some of the IoT applications. Its range is up to 50 m. Wi-Fi usually works at 2.4 and 5 GHz of frequencies.

4.2 Bluetooth

Bluetooth is commonly used for short-range wireless technology. It is mostly used for pairing and connecting smart watches or bands with our mobile phones. The latest Bluetooth technology used as an IoT protocol is Bluetooth low energy (BLE). BLE provides common Bluetooth range along with lesser power consumption. Bluetooth is based upon IEEE 802.15.1 standard but is now managed by Bluetooth special interest group (BSIG).

4.3 Ultra-Wide Band

Ultra-wide band, which is IEEE 802.15.3 standard, is used for wireless transmission of data. It has a very large bandwidth, and therefore, it is used for communications that require a very high bandwidth. UWG spreads information upto a large bandwidth of greater than 500 MHz. It has many disadvantages like higher achievable data rates and high immunity to interference because of its lower spectral power density.

4.4 ZigBee

It operates at a frequency of 2.5 GHz; it is mostly used by the industries. It is based upon IEEE 802.15.4 standard and is a low-cost device which consumes very less power. It is mainly focused on battery-powered devices in wireless and IoT applications. Its physical range is up to 10–20 m. The biggest advantage of ZigBee is that it also supports low data rates with the help of mesh networking protocol to avoid hubs in order to create a self-healing architecture.

4.5 Z-wave

It is mostly used for home automation, and it has a long range of up to 100 m. It uses low energy radio waves to enable communication between different devices, and its frequency range varies from 800 to 900 MHz; due to this specific frequency range Z-Wave becomes immunized to noise signals and interference which becomes its advantage over other wireless networks, and it also uses encryption techniques to transfer data between different appliances which makes it a secure wireless networking protocol.

4.6 6LoWPAN

It is an acronym for IPv6 low-power wireless personal area network. It is based on the IEEE 802.15.4 standard and is primarily focused on enabling IoT devices to communicate via IPv6 packets even when their power supply and processing power are constrained. It operates at a 2.4 GHz frequency. It is supported by a wide variety of networking technologies, including low-power radio frequency, Bluetooth smart, PLCs, and low-power Wi-Fi.

4.7 Adaptive Network Topology (ANT)

It is a protocol which is used for ultra-low-power wireless applications to send data between wireless devices in a robust and flexible way. Due to a large number of nodes present, this protocol can operate in a large number of network topologies ranging from peer to peer/star topology to practical mesh topology in personal area networks. ANT is a perfect protocol that can be used for LAN applications in homes and industrial automation applications.

The advantages of ANT protocol in networks are:

- The networks become operational even at very low power.
- The network becomes highly optimized and compact.
- The network becomes more flexible and scalable.

ANT devices can operate at any frequency range from 2400 to 2524 MHz, and operational frequency range of 2457 MHz is reserved for ANT+ devices.

4.8 Radio Frequency Identification (RFID)

In this technology, radio waves are used to capture and store information from an RFID [16] tag even if the tag is not present in the direct line of sight or it is present far away from the sensor. A sensor basically senses all the information from the RFID tag and sends the data collected to the interpreter which further sends the data to a computer. The latest standard of operation of RFID is EPC global class 1 gen—2 protocols. There are two kinds of RFID tags:

- Active tags: These tags are connected to some external power source to turn on their circuitry.
- Passive tags: These tags are very simple and cheap, and these are not connected to any external power source instead it uses reader signals to turn on its circuitry and advanced modulation techniques like QAM and PSK are also not possible in case of passive RFID tags.

4.9 Near-Field Communication (NFC)

NFC consists of protocols used to enable communication between devices placed very close to each other upto the distance of 2 m; these are also used as electronic documents and can be used to facilitate cashless payments using mobile phones or NFC cards.

NFC tags can operate at a frequency range of 13.56 MHz. Three modes of operation of an NFC device are:

- NFC emulation cards: It enables us to use our credit cards and our smart phones for cashless payments.
- NFC readers/writers: It can be used to obtain and store information from an NFC tag or any smart poster.
- NFC peer to peer: This allows two NFC devices to share and transmit data to each other by providing a low-speed connection between both the devices.

4.10 Powerline Ethernet Communication

It is used to provide Internet access in the house using the electrical wiring installed in the house to transfer AC current signals. It does not require any extra wiring to allow the transfer of data signals. Power Ethernet communication basically adds a modulating carrier signal to the existing electrical wiring system to facilitate the flow of data signals over the wiring systems. The limitations of powerline communication are the propagation problem because the power distribution system was developed for transmission of power at frequency range from 50 to 60 Hz. A comparison between the technology, frequency, data range, power usage, and cost is shown in Table 2.

Table 2 Comparative analysis of different technologies

Technology	Frequency	Data rate	Range (feet)	Power usage	Cost
Wi-Fi	Sub GHz, 2.4 GHz, and 5 GHz	0.1–54 Mbps	<300	Medium	Low
Bluetooth/BLE	2.4 GHz	1–3 Mbps	300	Low	Low
Ultra-wide band	1.3 GHz	675 Mbps	>1	Low	Low
ZigBee	2.5 GHz	250 kbps	300	Low	Medium
Z-wave	Sub GHz 800–900 MHz	100 kbps	100	Low	Medium
6LoWPAN	2.4 GHz	250 kbps	380	Low	Low
ANT	2457 MHz	60 kbps	>100	Low	Low
RIFD	2.45–5.8 GHz	640 kbps	6–90	Low	Very low
NFC	13.56 MHz	424 kbps	>1	Medium	Very low
Powerline Ethernet communication	50–60 Hz	400 Mbps	984	Low	Low

5 Conclusion

In this work, an exhaustive review of the IoT Protocols has been presented. Numerous similar protocols have been developed by organizations such as the Internet Engineering Task Force, the IEEE, and the ITU, and many more are being developed for future advancements. The primary objective of this study is to educate developers and service providers about the various IoT communication protocols and IoT wireless technologies. Different protocols along with their history, their basic mechanisms, and their applications have been discussed briefly for a better understanding.

References

1. Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, Leung KK (2013) A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wirel Commun 20(6):91–98
2. Granjal J, Monteiro E, Silva JS (2015) Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutor 17(3):1294–1312
3. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422
4. Sharma V, Tiwari R (2016) A review paper on "IOT" & it's smart applications. Int J Sci Eng Technol Res (IJSETR) 5(2):472–476
5. Elkhodr M, Shahrestani S, Cheung H (2016) Emerging wireless technologies in the internet of things: a comparative study. arXiv preprint arXiv:1611.00861
6. Chen Y, Kunz T (2016) Performance evaluation of IoT protocols under a constrained wireless access network. In: 2016 international conference on selected topics in mobile & wireless networking (MoWNeT). IEEE, pp 1–7

7. Al-Sarawi S, Anbar M, Alieyan K, Alzubaidi M (2017) Internet of things (IoT) communication protocols. In: 2017 8th international conference on information technology (ICIT). IEEE, pp 685–690
8. Alavi AH, Jiao P, Buttlar WG, Lajnef N (2018) Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement 129:589–606
9. Karagiannis V, Chatzimisios P, Vazquez-Gallego F, Alonso-Zarate J (2015) A survey on application layer protocols for the internet of things. Trans IoT Cloud Comput 3(1):11–17
10. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376
11. Partridge C, Pink S (1993) A faster UDP (user datagram protocol). IEEE/ACM Trans Network 1(4):429–440
12. Postel J (1983) Telnet protocol specification. In: RFC 854, ISI
13. Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G (2012) A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In: 37th annual IEEE conference on local computer networks-workshops. IEEE, pp 956–963
14. Vasseur J, Agarwal N, Hui J, Shelby Z, Bertrand P, Chauvenet C (2011) RPL: the IP routing protocol designed for low power and lossy networks. Internet Protocol Smart Objects (IPSO) Alliance 36
15. Hunkeler U, Truong HL, Stanford-Clark A (2008) MQTT-S—a publish/subscribe protocol for wireless sensor networks. In: 2008 3rd international conference on communication systems software and middleware and workshops (COMSWARE'08). IEEE, pp 791–798
16. Yashiro T, Kobayashi S, Koshizuka N, Sakamura K (2013) An internet of things (IoT) architecture for embedded appliances. In: 2013 IEEE region 10 humanitarian technology conference. IEEE, pp 314–319