A Study on IoT Technologies, Standards and Protocols

Karthik Kumar Vaigandla[1] , Radha Krishna Karne[2] , Allanki Sanyasi Rao[3]

[1,2,3]Dept. of Electronics and Communication Engineering, Balaji Institute of Technology and Science,

Abstract

During the past couple of decades, the Internet of Things (IoT) has grown tremendously. The IoT is increasingly used in industries including medicine, engineering, safety, and transportation. In order to define this vision, various challenges need to be overcome, including issues surrounding interoperability, data confidentiality and security, and development of energy efficient management systems. A network and data are the basis for IoT protocols. Wireless technologies include Bluetooth, ZigBee, and Long Range Wide Area Networks (LoRa WAN). There is a rapid development of new standards, technologies, and platforms for the IoT ecosystem. IoT is rapidly growing; this paper represents an overview of IoT Network protocols and several Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and International Telecommunication Union (ITU) standards.

Keywords: Internet of Things (IoT), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), IoT Network protocols, Long Term Evolution Advanced (LTE-A), Long Range Wide Area Network (LoRaWAN), ZigBee.

1. Introduction

Internet of things (IoT) refers to recent development in the interconnectivity of devices. Internet usage has become the norm in more aspects of our everyday lives in recent years. Our modern world is filled with objects that can gather, process, and send data to other objects, servers, and applications. We cover a variety of sectors and use cases, such as engineering, medicine, and safety [1]. With the creation of smart objects communication, the vision of a global networking platform has already progressed greatly. As a result of the IoT technology, people and things are practically connected and information systems are formed by means of wireless sensor networks and nodes [2]. Social media and the internet will be able to interact freely and effectively with each other. It enables new services and applications to be developed [6].

IoT consists of two key elements: "internet" and "things". Communication allows things to coordinate their actions and reach decisions together it allows them to hear, see, think, compute, and act. The technology gives things making authoritative decisions that benefit various applications using intelligence and consensus. From the standpoint of passive observers, they transform objects or sensors into active members of a computing system, communicating, working collaboratively and making critical decisions. As a result, they present challenges that require specialized communication standards [3].

A number of existing technologies contribute to the Internet of Things paradigm, including Bluetooth, ZigBee, Wi-Fi, and Long Term Evolution Advanced (LTE-A). It will likely be very challenging to create an acceptable and successful, these technologies form the basis of an IoT system. Providing interoperability and advanced functionality to IoT is critical, identifiers for sensors are also required by this system [7]. The IoT systems must be energy-efficient and have efficient data management systems for being environmentally sustainable [8]. According to the type of network technology used, these challenges must all be addressed. IoT technology has been studied in many ways [9-13].

Devices connected to the Internet of Things generally have low memory, inadequate batteries, limited processing capabilities, and a weak radio. Working groups have begun adapting existing protocols to new updations for IoT because the TCP/IP stack is incompatible with this environment [4]. Due to the many interconnected nodes, an addressing scheme like IPv6 is important. There are a lot of working groups already defining ways to support IPv6 in constrained environments, such as LoWPAN, IEEE and ZigBee. Denial of Service attacks are on the rise, so privacy and security are also demands [4].

2. Internet of Things (IoT)

IoT consists of two key elements: "internet" and "things". Communication allows things to coordinate their actions and reach decisions together it allows them to hear, see, think, compute, and act. The technology gives things making authoritative decisions that benefit various applications using intelligence and consensus. From the standpoint of passive observers, they transform objects or sensors into active members of a computing system, communicating, working collaboratively and making critical decisions. As a result, they present challenges that require specialized communication standards [3].

In addition to connected devices, the IoT consists of a large number of components, which enables the transfer of data without requiring human or computer interaction. There are three categories of things in the IoT: Sensors that collect data and send it to a server, a computer that receives information and then acts on it, and Things that perform both functions. The Internet of Things makes it possible to sense and control objects remotely across existing network infrastructure, allowing them to be integrated with computer-based systems at a lower point of integration, and reducing human intervention while improving efficiency, accuracy and economic benefit [5].

Figure 1 outlines the various types of connections that the Internet of Things has, including those between devices, gateways, and data systems. When devices are in direct contact, information can be exchanged between them instantaneously without a middleman. Sensors and gateway nodes communicate via the device-to-gateway connection. Data is transmitted from a gateway to an appropriate data system through a gateway-to-data system connection. In addition to the connection system, there is also another system for transferring information among the data centers or cloud servers [1].

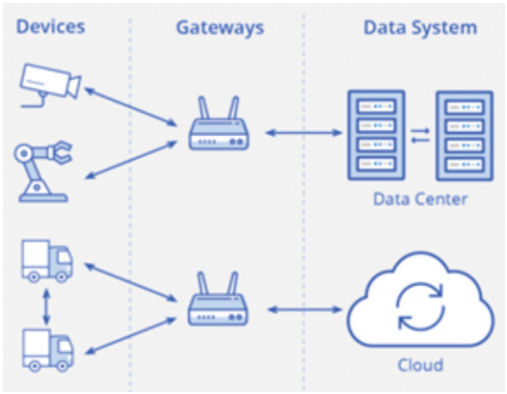

Fig. 1. Basic architecture of IoT

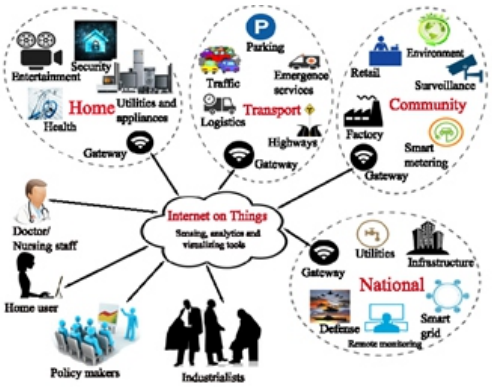

Fig. 2. IoT applications

The figure 2 illustrates the main applications of IoT. Nearly every aspect of life is affected by the IoT. The IoT can be utilized to fabricate smart cities, smart homes, and smart objects with greater security. Some of the applications are wearables, health monitoring, traffic monitoring, fleet management, agriculture, Hospitality, water supply, maintenance management, industrial automation, smart grid and energy saving.

Figure 3 illustrates the seven layers of the IoT ecosystem. Each layer includes market, acquisition, interconnectivity, integration, analysis, applications, and services. These layers must also be augmented with security and administration applications.

3. Technologies and protocols for the Internet of Things

In order to support the IoT, a variety of exciting technologies are available. IoT technologies and protocols are presented here in the best way. The figure 4, summarizes the compiled IoT technologies on the basis of architecture in order to describe each aspect of a technology and the qualifications.

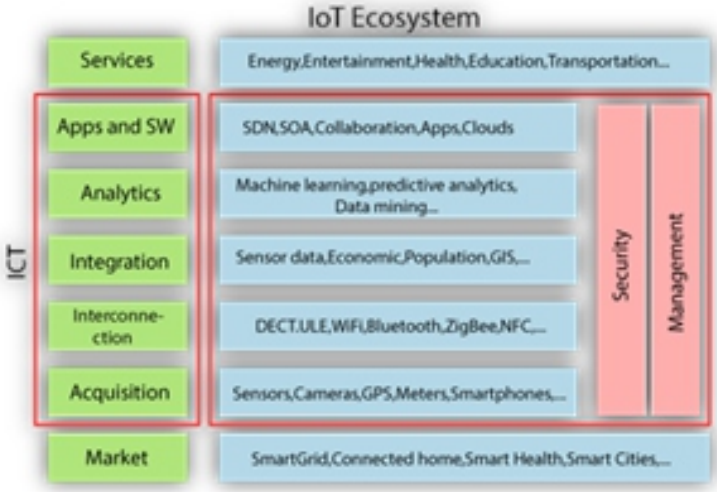

Fig. 3. IoT Ecosystem

3.1Bluetooth and Bluetooth Low Energy (BLE)

Bluetooth is a widely used protocol for short-range communications. IoT data is transferred wirelessly via this protocol. Compared to other wireless protocols, the Bluetooth protocol is safe, inexpensive, short-range, and requires little power. The Bluetooth low energy (BLE) protocol offers low-energy versions of Bluetooth. It helps to reduce energy consumption and increases the connectivity of IoT devices [1]. The Bluetooth Low Energy specification provides a lightweight Bluetooth feature suitable for low-energy devices [5]. In comparison to its competitors, BLE has many advantages; it does not support open firmware or hardware standards [2]. Table 1 compares Bluetooth classic and Bluetooth Low Energy.

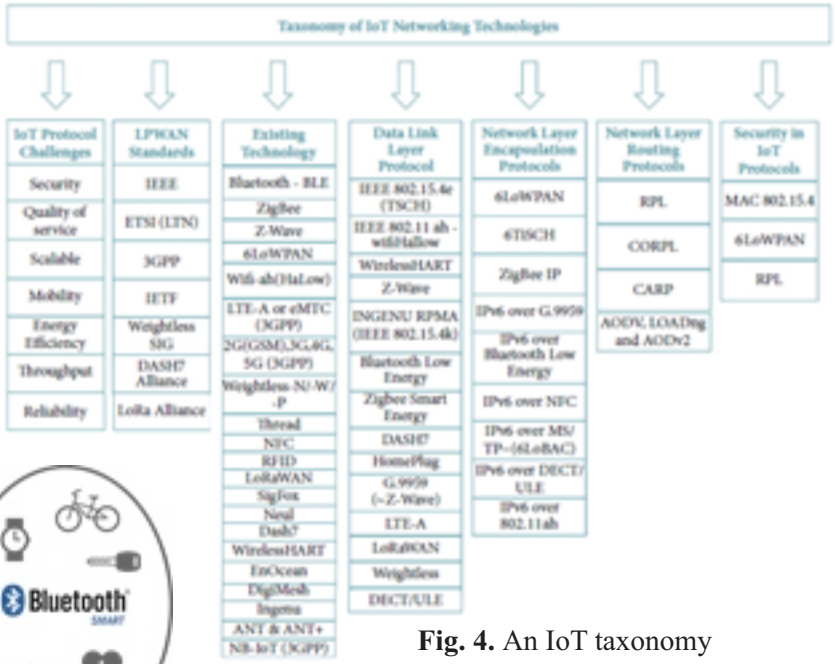

Fig. 4. An IoT taxonomy

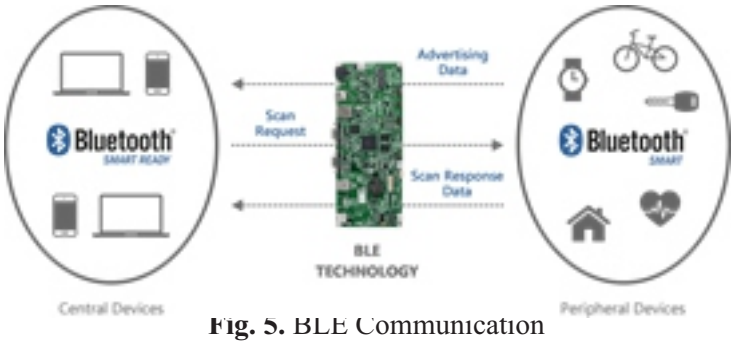

Fig. 5. BLE Communication

Table 1. Classic Bluetooth vs Bluetooth Low Energy

Specifications	Classic Bluetooth	Bluetooth Low Energy
Network/Topology	Scatternet	Star Bus
Power consumption	Low	Very Low
Speed	700 Kbps	1 Mbps
Range	<30 m	50 meters
RF Frequency band	2400 MHz	2400 MHz
Frequency Channels	79 channels from 2.400 GHz to 2.4835 GHz with 1 MHz spacing	40 channels from 2402MHz to 2480 MHz
Modulation	GFSK (modulation index 0.35), π/4 DQPSK, 8DPSK	GFSK (modulation index 0.5)
Latency in data transfer between two devices	Approx. 100 ms	Approx. 3 ms
Spreading	FHSS (1MHz channel)	FHSS (2MHz channel)
Link layer	TDMA	TDMA
message size(bytes)	358 (Max)	8 to 47
Error detection/correction	8 bit CRC(header), 16 bit CRC, 2/3 FEC(payload), ACKs	24 bit CRC, ACKs
Security	64b/128b, user defined application layer	128 bits AES, user defined application layer
Application throughput	0.7 to 2.1 Mbps	less than 0.3 Mbps
Nodes/Active Slaves	7	Unlimited

3.2 ZigBee

Smart objects can communicate with one another through the ZigBee protocol. Short-distance data transfer is supported by ZigBee. Automation of the home is the main use case for ZigBee. Industrial settings are primarily utilizing ZigBee. The latest version of ZigBee is v3.0, which integrates several ZigBee standards into one. The IEEE 802.15.4-2003 standard defines a set of ZigBee protocol specifications for remote control of small, low-power radios. [22].

Fig. 6. Application areas of ZigBee

3.3 ZigBee IP

An IPv6-based full-mesh wireless network based on ZigBee IP is the first open standard. The device allows for easy control of thousands of devices to provide seamless Internet connectivity without sacrificing power or cost. A ZigBee internet protocol was designed to support the ZigBee Smart Energy Internet Protocol system. A ZigBee IP stack is illustrated in Figure 7, which is based on IEEE 802.15.4, the low layer standard. Using the IPv6 addressing and routing protocol, all nodes of the network can be addressed individually in Zigbee IP. IEEE and IETF standards are referenced and used by ZigBee IP, however it defines the options that are to be used.

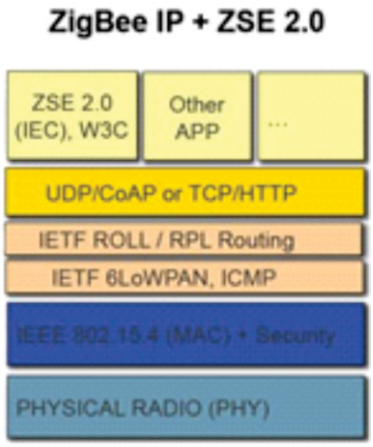

Fig. 7. ZigBee IP protocol stack

3.4 ZigBee IP

An IPv6-based full-mesh wireless network based on ZigBee IP is the first open standard. The device allows for easy control of thousands of devices to provide seamless Internet connectivity without sacrificing power or cost. A ZigBee internet protocol was designed to support the ZigBee Smart Energy Internet Protocol system. A ZigBee IP stack is illustrated in Figure 7, which is based on IEEE 802.15.4, the low layer standard. Using the IPv6 addressing and routing protocol, all nodes of the network can be addressed individually in Zigbee IP. IEEE and IETF standards are referenced and used by ZigBee IP, however it defines the options that are to be used.

3.25Long Range Wide Area Network (LoRaWAN)

LoRaWAN is a wireless technology that is designed for IoT applications with features such as low power consumption, low cost, mobility, security, and bidirectional communication. Under the noise level, this protocol can detect low-strength signal over long distances. This protocol has been optimized for scalable networks with millions of wireless devices and is powered by low power consumption. To meet the future needs of IoT, it supports redundant operation, low cost, low power, and energy harvesting technologies that enable ease of use and mobility [3]. It is a protocol built for supporting large-scale public networks with a single operator by utilizing the Media Access Control (MAC) protocol. Utilizing coded messages, instead of narrowband transmission, it distributes data over a variety of radio channels and transmission rates. Depending on the requirements of each application, LoRaWAN devices have varying specifications.

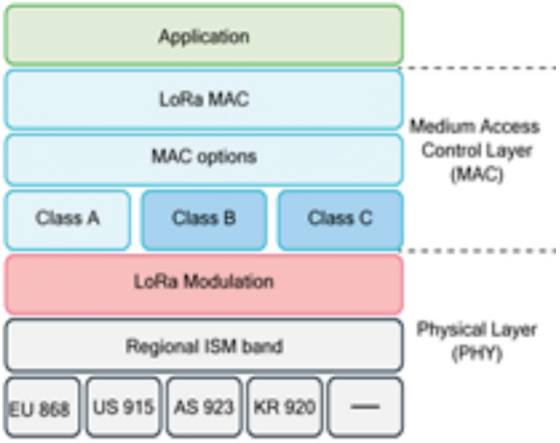

Fig. 8. LoRaWAN Protocol

3.5 6 LoWPAN

6LoWPAN protocols represent one of the most significant IoT schemes. Small IoT devices as well as sensors can communicate securely and safely with 6LoWPAN wireless modules. IEEE 802.15.4 was originally conceived as the base for 6LoWPAN, which defines the operation of low power wireless networks at 2.4 GHz, the technology has been adapted and extended to work with a variety of other wireless technologies [2]. A working group of the IETF developed LowPAN for interconnected networks and embedded devices by IEEE 802.15.4 in RFC4944. 6LoWPAN then developed encapsulation and compression to enable wireless IPv6 data transmissions. The first two bits in a 6LoWPAN packet determine its type. The remaining structure depends on type and the next 6 bits. Four types of headers are used by 6LoWPAN frames based on 2 bits: a no 6LoWPAN header (00), a dispatch header (01), a mesh header (10), and a fragmentation header (11) [3].

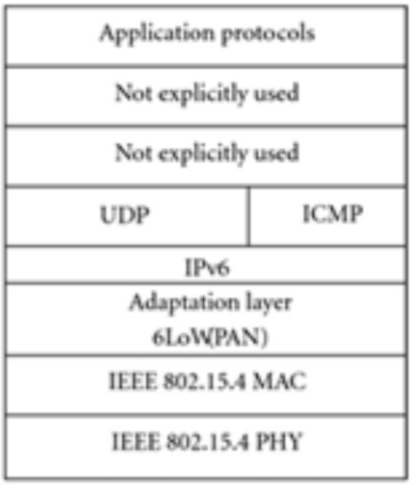

Fig. 9. LoRaWAN Protocol

3.6 LTE Advanced (LTE-A)

The Long Term Evolution (LTE) network standard was developed in 2008, and it represents new 4G network technology. LTE-A (advanced) improves upon LTE's architecture. This includes increasing spectral efficiency, network capacity, power efficiency, and reducing operator costs [2]. LTE-A was introduced in 2009 and has since released many variations to accommodate new technologies. The technology uses orthogonal frequency division multiple access (OFDMA), which divides the frequency into multiple subcarriers. There are three main components within LTE-A: a core network (CN), a radio access network (RAN), and mobile nodes.

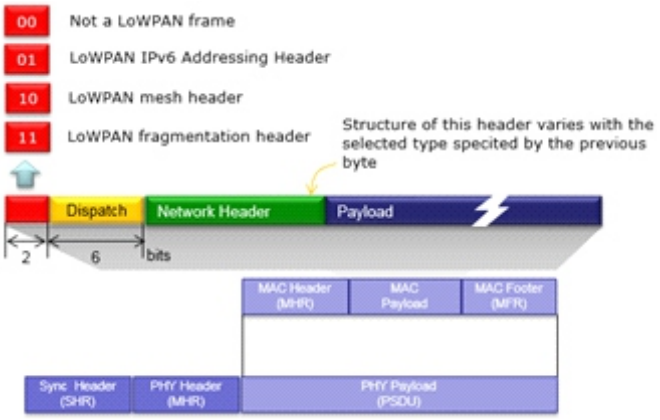

Fig. 10. Frame structure in LoRaWAN

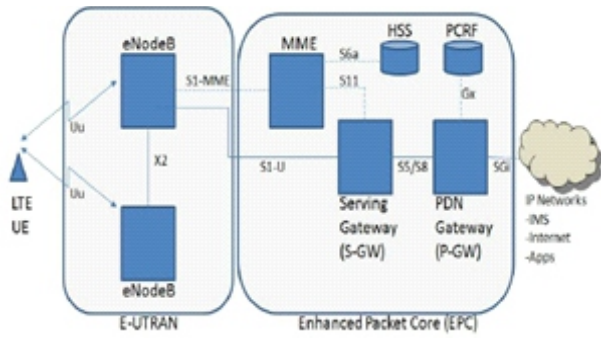

Fig. 11. Architecture of LTE-A

3.7Z-Wave

Low energy radio waves are used in wireless Z-Wave protocol. The system is primarily used for controlling home appliances via wireless devices such as a lighting system, security system, thermostat, garage door opener, etc. Using mesh technology, Z-Wave can connect devices up to 30 meters away. For reliable transmission, CSMA/CA is used along with small ACK messages [16]. Compared to other alternatives, Z-Wave uses a simpler protocol, which makes development easier. The data rate is 9.6/40/100 kbit/s, and the frequency is 900MHz.

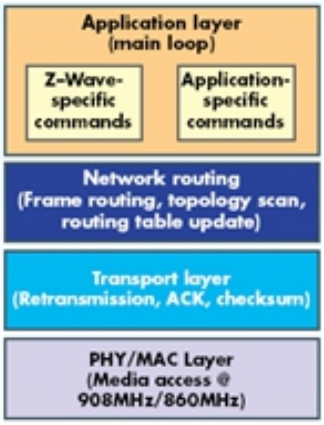

Fig. 12. Z-Wave Protocol

3.9RPL, RPL Enhancements and CORPL

A new protocol called Distance Vector Routing Protocol for Low Power and Lossy Networks (RPL) was published by the IETF in 2012 [14]. With RPL, one has only one path from any leaf node to any root node, a Destination Oriented Directed Acyclic Graph (DODAG). Each node initially broadcasts itself as the root through the DODAG information object (DIO). When a node communicates with its parents, the parent sends an advertisement (DAO) to the root, and the root decides where to route it [17]. To improve the performance of the basic RPL protocol, various enchantments have been suggested. Enhancing the reliability of the RPL protocol is the goal of Enhanced-RPL. For applications in IoT using dynamic logic, dynamic RPL is used [15]. The CORPL protocol relies on DODAG topology generation and is designed for cognitive networks. To forward packets, CORPL selects multiple forwarders opportunistically. The neighbors will use DIO messages to update each other's forwarding lists instead of their parents. Forwarder set is dynamically constructed by each node according to the updated information [18].

3.10 CARP and E-CARP

A non-standard distributed routing protocol used in Underwater Wireless Sensor Networks (UWSNs) is Channel Aware Routing Protocol (CARP). This technology features low energy consumption and provides packet delivery in reasonable time. When selecting the forwarding route, the measure of the quality of the historical links is taken into account. To select the routing nodes, history is gathered from adjacent sensors. CARP has the disadvantage that data collected in the past cannot be reused. Enhanced-CARP allows previously received sensory data to be saved by the sink node. Sensor nodes respond to E-CARP packets with new data when new data is required. Communication overhead is dramatically reduced with E-CARP [19].

3.11Message Queue Telemetry Transport

Messaging Queue Telemetry Transport (MQTT), which originally emerged in 2003, is a messaging protocol that connects embedded devices with applications and middleware [21]. Considering its low resource requirements, it is usually built over TCP. This entity can be broken down into three components, subscribers, publishers, and brokers. Publishers send data through subscribers, who forward it to the Broker. A broker can also provide security by authorizing both entities. In health care, monitoring, machine-to-machine messaging, or Facebook notifications, it is commonly used because of its low resource usage [20]. A message header includes one to four bytes, depending on the length of the message. Initially two bits are fixed, Message Type is set to one of the following: CONNECT(1), CONNACK(2), PUBLISH(3), SUBCRIBE(8) or others. "DUP" is the next field. Messages received earlier may be considered duplicates, if it is set. The PUBLISH message headers contain three levels of "QoS". Messages that are marked as "Retain" will be kept by the broker for the purpose of sending them out as their first message.

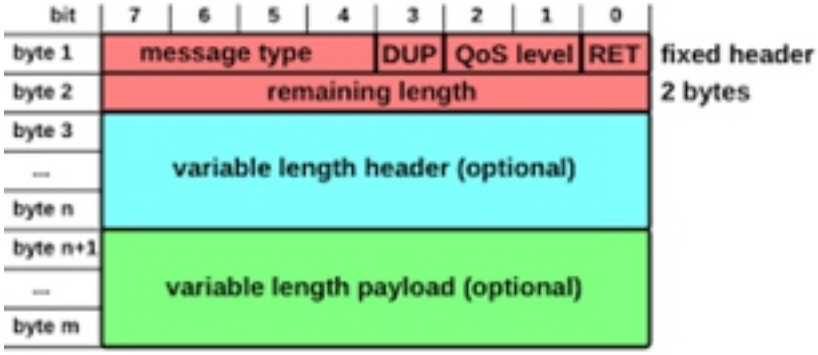

Fig. 13. MQTT Message format

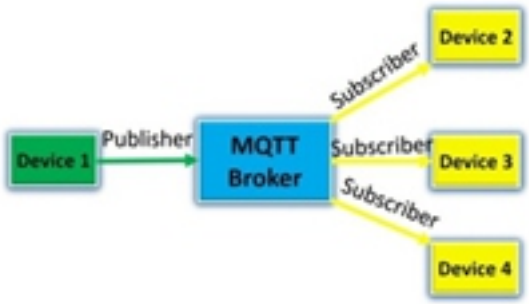

Fig. 14. MQTT architecture

3.11Constrained Application Protocol (CoAP)

Constrained Application Protocol is an IETF standard from the CoRE (Constrained Resource Environments) group. CoAP uses a client-server interaction model similar to HTTP. Interactions between machines usually involve CoAP implementations that function both as servers and as clients. Using CoAP, simple, constrained devices can access the IoT through low bandwidth, low availability networks even within constrained environments. A standard interface widely used in modern web applications is representational state transfer (REST). A lightweight mechanism is used to ensure reliability, since it is built over UDP rather than TCP [20]. Messages are exchanged over UDP using the CoAP protocol, which is based on compact messages. There is a short binary header (4 bytes) followed by compact binary options and a payload. Next comes a variable-length Token string, which can range from 0 to 8 bytes in length. CoAP Options are followed by a sequence of zero or more Type-Length-Value (TLV) values, optionally followed by the payload.

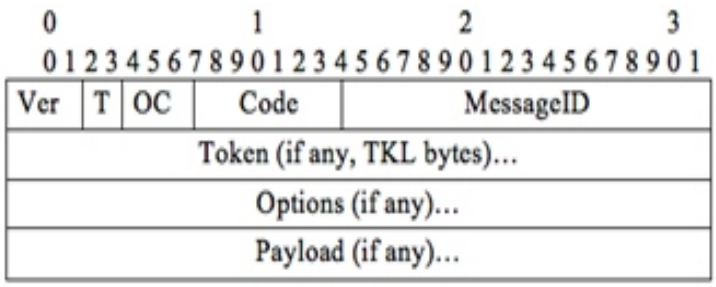

Fig. 15. CoAP message format

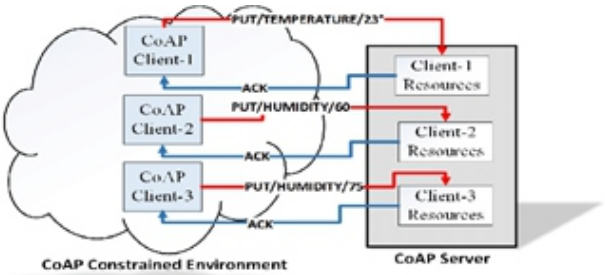

Fig. 16. CoAP architecture between constrained nodes & server

Table 2. Comparisons of IoT Standards

Parameter	AMQP	CoAP	DDS	MQTT
Transport	TCP/IP	UDP/IP	UDI/IP, TCP/IP	TCP/IP
Paradigm	Point To Point Message Exchange	Request / Reply	Publish / subscribe/ Request / Reply	Publish / subscribe/
Scope	D2D, D2C, C2C	D2D	D2D, D2C, C2C	D2D
Discovery	No	Yes	Yes	No
Content awareness	None	None	Content based routing	None
Data centricity	Encoding	Encoding	Encoding declaration	Undefined
Security	TLS	DTLS	TLS, DTLS, DDS	TLS
Data prioritization	None	None	Transport priorities	None

4. Conclusion

Modern human life has become integrated with Internet of Things. By automating, connecting devices and applications and making information faster and more available, it looks to improve life quality. It discusses some standard technologies designed specifically for embedded devices and environments with tight constraints. In this paper, Several applications protocols were presented and compared. This paper is intended to get developers and service providers thinking about different protocols for the Internet of Things and how to pick between them. The majority of the finalized standards were presented at each level and several drafts were highlighted. As each of the discussed IoT protocols has different applications under different circumstances, it is impossible to give a priority to one over another in terms of Internet of things technologies. By advancing and upgrading the technical base, we can set a solid networking base for the Internet of Things of the future. By using our research as a motivation, scholars and professionals can identifying gaps in network architectures, developing more efficient protocols, and addressing important deficiencies.

References

Pallavi Gupta and Usha Tiwari(2020) " Review on Internet of Things Network Protocols", Journal Of Critical Reviews, VOL 7, ISSUE 3, pp.790-794.

Anna Triantafyllou ,Panagiotis Sarigiannidis and Thomas D. Lagkas (2018) "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends", Wireless Communications and Mobile Computing, https://doi.org/10.1155/2018/5349894

Tara Salman and Raj Jain(2017) "A Survey of Protocols and Standards for Internet of Things", Advanced Computing and Communications, Vol. 1, No. 1.

Iulia Florea, Razvan Rughinis, Laura Ruse and Dan Dragomir (2017)"Survey of Standardized Protocols for the Internet of Things", International Conference on Control Systems and Computer Science, DOI 10.1109/CSCS.2017.33.

P.Vamshi Krishna Rao(2018)"Multiple Motion Control System Of Robotic Car Based On IoT To Produce Cloud Service", International Journal of Management, Technology And Engineering, Volume 8, Issue IX, pp. 190-1905.

D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac(2012) "Internet of things: vision, applications and research challenges," AdHoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis(2017) "ASTo: a tool for security analysis of IoT systems," in Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications, pp.395–400.

R. Khan, S. U. Khan, and R. Zaheer(2012) "Future internet: the internetof things architecture, possible applications and key challenges,"in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT' 12), pp. 257–260.

H. S. Dhillon,H.Huang and H. Viswanathan(2017) "Wide-area wireless communication challenges for the internet of things," IEEE Communications Magazine, vol. 55, no. 2, pp. 168–174.

V. Gazis(2017)"A survey of standards for machine-to-machine and the internet of things," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482–511

A. Al-Fuqaha,M. Guizani, M. Mohammadi,M. Aledhari, and M. Ayyash(2015) "Internet of things: a survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no.4, pp. 2347–2376.

Z. G. Sheng, S. S. Yang, Y. F. Yu,A. V. Vasilakos, J. A. McCann, and K. K. Leung(2013) "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," IEEE Wireless Communications Magazine, vol. 20, no. 6, pp. 91–98.

L. Mainetti, L. Patrono, and A. Vilei, (2011) "Evolution of wireless sensor networks towards the Internet of Things: a survey," in Proceedings of the 19th International Conference on Software,

Telecommunications and Computer Networks (SoftCOM '11), pp. 16–21.

H.-S. Kim, J. Ko, D. E. Culler, and J. Paek(2017) "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): a survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2502–2525.

M. Zhao, A. Kumar, P. H. JooChong, andR. Lu(2017) "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities," Peer-to-Peer Networking

and Applications, vol. 10, no. 5, pp. 1232–1256.

Z-Wave (2017) "Z-wave protocol overview," April 2006, https://wiki.ase.tut.fi/courseWiki/images/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf.

T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander(2017) "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, March 2012, http://www.ietf.org/rfc/rfc6550.txt.

Aijaz and A. Aghvami(2015) "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," in IEEE Internet of Things Journal, vol. 2, no. 2, 2015, pp. 103-112.

S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini (2015) "Carp: A channel-aware routing protocol for underwater acoustic wireless networks", in Ad Hoc Networks,V34, pp.92-104

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash(2015) "Internet of things: A survey on enabling technologies, protocols, and applications.", IEEE Communications Surveys & Tutorials, vol. 17(4), pp. 2347-2376,.

D. Locke(2010) "Mq telemetry transport (mqtt) v3. 1 protocol specification", IBM developer Works Technical Library.

V. Karthik Kumar and M. Vennela (2017) " Design Tracking System for At-home Medical Equipment during Natural Disasters", International Journal of Research, Vol 04, pp. 1042-1045.

V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate(2015) "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17.