2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)

Overview of Communication Protocols in Internet of Things: Architecture, Development and Future Trends

Yonghong Cheng*
China National Institute of Standardization
Beijing, China
chengyh@cnis.gov.cn

Huajun Zhang
School of Software & Microelectronics
Peking University
Beijing, China
thevastworld@pku.edu.cn

Yi Huang
Institute of Scientific and Technical Information of China
Beijing, China
huangyi@istic.ac.cn

***Abstract*—The Internet of Things (IoT) transmits data between devices and users with the help of communication protocols. IoT communication protocols can be classified into 3 architecture kinds from different aspects: OSI model hierarchy, IEEE 802 protocol standard or network types. Designed for diverse situation and with growing technique, the protocols show different features in technology roadmap, communication distance, and signal frequency spectrum rang. The future trends of the IoT communication protocols might locate in their optimization, integration and information security.**

Keywords—Internet of Things, communication protocol, 5G, Wi-Fi, low-power wide area network

I. Introduction

In recent years, the Internet of Things (IoT) has developed rapidly throughout the world.

In regard to what is IoT, the international communities have no universally admitted definition yet. However, many countries and scholars have proposed its definition of concept and functions. According to the definition in Report on the work of the government of China in 2010, the Internet of Things is a network which may connect any item to the Internet with agreed protocols and information sensing devices [1]. In a narrow sense, IoT extends and expands the Internet. In a broad sense, it fuses information and physical space to materialize the intelligent identification, interaction and management of items such as locating, tracking or monitoring [2]. The framework of IoT communication network could be divided into three layers: sensors layer, network layer, and application layer [3]. The sensors layer (also called perception layer) connect various sensors into a networks to collect data [4]. The network layer uses the wireless or wired network such as Internet and mobile Internet infrastructure to upload data [5]. The application layer uses cloud devices to process and analyze data for controlling IoT devices [6]. Therefore, to transmit information between terminal devices of different types and performances, The IoT should process, present and transmit data in a seamless, efficient, standardized, and easily interpretable format [7]. Keysight Technologies' research report (2015) showed that and IoT communication protocols are designed for and applied in specific scenarios to obtain better performance [8]. The protocols in different layers cooperate with each other, and naturally constitute a system with hierarchical architecture.

In order to provide a comprehensive overview of IoT communication protocols, this paper introduces the current IoT communication protocols by presenting their architecture and developing process. We classified and reviewed these protocols by OSI model hierarchy, by IEEE 802 protocol standard and by network types. Then we analyzed various IoT communication protocols from their technology roadmap, communication distance, and signal frequency spectrum rang. Finally, we summarize and suggest some future trends of IoT communication protocols' development.

II. IoT Communication Protocols' Architecture

From different angles and aspects, IoT communication protocols can be divided into the following architectures.

A. Divided by OSI Model Hierarchy

Based on the Open Systems Interconnection (OSI) model, IoT communication protocols can be divided into application layer, network layer and physical layer [9].

The protocols in the application layer, including CoAP, ISA100.11a, MQTT, SOAP, Web Socket, etc., describe data's logical structures and features, and provide host-to-host communication services for applications [10]. The network layer includes SMS/USSD protocol suite, TCP/UDP protocol suite and wireless sensing protocols [11]. The physical layer and data link layer protocol architecture consist of three types of protocols: short-range communication protocols, long-range cellular communication protocols and long-range non-cellular communication protocols,.

IoT communication protocols' architecture based on the OSI model is supports modular engineering and multivendor interoperability [12]. However, it has fuzzy areas in the layer division, and the boundary is not clear enough. Some protocols such as Bluetooth may be applied in more than one layers, and their ratios varies in different layers, thus it is controversial to classify which layer it should be.

B. Divided by IEEE 802 Protocol Standard

The IEEE 802 protocol standard suite has also become the basis of many IoT communication protocols [8].

The IoT communication protocols based on IEEE 802.11 include Wi-Fi, Wi-Fi HaLow and V2X. Compared to 2.4GHz and 5GHz Wi-Fi, Wi-Fi HaLow, which works in the 900MHz band, has lower power consumption is and farther distance [13]. V2X was developed for intelligent transportation systems, especially for wireless communication of vehicles [14]. The

978-1-5386-7325-6/18/$31.00 ©2018 IEEE
DOI 10.1109/WI.2018.00-25

protocols based on IEEE 802.15 include Bluetooth, UWB, ZigBee, Thread, Wireless HART, ISA100.11a, etc. [15].

This architecture directly reveals the technical norms of IoT communication protocols. However, it is not comprehensive enough as it only correspond to the lowest two layers of the OSI network reference model.

C. Divided by Communication Network Types

American Federal Communications Commission divided IoT communication protocols into four network types: personal area network (PAN), local area network (LAN), wide area network (WAN), and mobile network [16]. This architecture own a clear classification of the protocols. However, this division is not precise enough. It is wireless local area network (WLAN) and wireless wide area network (WWAN) that people actually use on a large scale in IoT, instead of wired communication networks such as LAN and WAN.

III. Comparison and Analysis of IoT Communication Protocols' Development

In this section we will compare features and developments of major IoT communication protocols.

A. Technology Roadmap

After investigating various IoT communication protocols, we can use timeline and network types as dimensions to summarize and compare their developing process.

TABLE I. TECHNOLOGY ROADMAP OF MAJOR IOT COMMUNICATION PROTOCOLS

Timeline	Communication Networks Types			
	PAN	***WLAN***	***WWAN***	***LPWAN***
1989			2G	
1993	IrDA			
1996		Wi-Fi		
1998	Bluetooth			
1999		V2X		
2000			3G	
2003	ZigBee			
2004	NFC RFID			
2005	6LoWPAN suite			Telensa
2007	Wireless HART			
2011	DASH7			
2012	Wi-SUN		4G	
2013				Sigfox
2014	ISA100.11a Thread			
2015				LoRa
2016		Wi-Fi HaLow		NB-IoT
2017				LTE-M
2018			5G	

[a] The timeline in this table refers to the time when protocols standards was established.

Above all, we can find the following features of IoT communication protocols' development from the timeline.

The oldest IoT communication protocol is RFID with a research starting time began from 1973, while the youngest is 5G, whose international standardization is expected to be completed in 2018. Secondly, the recent IoT communication protocols have faster research and development period. For example, it takes nearly 30 years for the RFID protocol to be established as an international standard, and 15 years for the 3G protocol. Nevertheless, the exponential growth of technology and industry productivity along with the refinement of communication infrastructures such as base stations have accelerated the research and development cycle of IoT communication protocols. Bluetooth takes 5 years from the beginning of research to its standard establishment; ZigBee takes 4 years, and 6LoWPAN takes just one year. Moreover, in recent 5 years new IoT communication protocols have come out in a high frequency, which illustrates that the protocols are in the rising period of technological hype cycle [17].

In the second place, looking closely at the network types, we can find these following trends.

Current main development of IoT communication protocols in the past five years has focused on low-power wide-area IoT (LPWAN) communication networks. Main LPWAN protocols consist of protocols working on unlicensed spectrum such as LoRa and SigFox; and protocols working on licensed spectrum with 3GPP's technical support, such as NB-IoT and LTE-M. Besides, nearly all these LPWAN protocols finished a whole research and development cycle form establishing standards to applying in the massive production of commercial hardware equipment in this five-year period.

IoT communication protocols within PAN and WLAN has thrived as they have been paid fair attention and been applied into industry from the beginning and early stage of IoT development history. However, the development momentum in this two field has slowed down comparing to their glorious years. On the one hand, it shows the slowing-down trend of innovation in this two field. On the other hand, it indicates that the existing IoT communication protocols within these two networks have already been developed to a mature technique status and own a stable industrial and commercial application. 5G within the field of WWAN has received widespread attention around the world. Its predecessor, 4G has a broad application scope and covers a large number of users, thus, it is naturally expected to perform a promoting role in the development of IoT.

B. Communication Distance

Taking into account of network type, IoT communication protocols can be classified as follows according to the communication distances of 10cm, 5km and 100km.

TABLE II. COMMUNICATION DISTANCE OF MAJOR IOT COMMUNICATION PROTOCOLS

Distance	Communication Networks Types			
	PAN	***WLAN***	***WWAN***	***LPWAN***
<10 cm	NFC			

Distance	Communication Networks Types			
	PAN	*WLAN*	*WWAN*	*LPWAN*
10cm~5 km	Bluetooth ISA100.11a MiWi RFID Thread Wireless HART Wi-SUN ZigBee Z-Wave	V2X Wi-Fi Wi-Fi HaLow	2G 3G 4G 5G	
5km~ 100km				LoRa LTE-M NB-IoT Sigfox Telensa

The increase of communication distance can improve the mobility of devices, thereby expand their application scope. As the user requirement to IoT terminals' convenience is getting higher, the recent IoT communication protocols show tendency in chasing frontier technology to ensure signal stability in a longer communication distance.

C. *Communication Signal Frequency Spectrum Range*

To ensure that different services use spectrum resources in a reliable way without interference with each other while to make rational use of spectrum resources [18], the International Telecommunications Union Radio communication Committee (ITU-R) has rules for spectrum allocation. Therefore, the signal frequency bands of IoT communication protocols are generally different as listed below.

TABLE III. COMMUNICATION SIGNAL FREQUENCY SPECTRUM RANGE OF MAJOR IOT COMMUNICATION PROTOCOLS

Spectrum	Communication Networks Types			
	PAN	*WLAN*	*WWAN*	*LPWAN*
125 KHz	RFID			
133 KHz	RFID			
13.56 MHz	NFC RFID			
433 MHz	DASH7 RFID			LoRa
470 MHz				LoRa
779 MHz	ZigBee	Wi-Fi HaLow		
862 MHz ~ 928 MHz	RFID			
868 MHz	DASH7 ZigBee Z-Wave	Wi-Fi HaLow		LoRa Sigfox Telensa
915 MHz	DASH7 ZigBee Z-Wave	Wi-Fi HaLow		LoRa Sigfox Telensa
920 MHz	Wi-SUN ZigBee Z-Wave	Wi-Fi HaLow		
2.4 GHz	Bluetooth IrDA ISA100.11a RFID Thread Wireless HART ZigBee	Wi-Fi		
5.8 GHz	RFID	Wi-Fi		
5.9 GHz		V2X		
Other			2G 3G 4G 5G	LTE-M

b. Other: these IoT communication protocols have a common ground as they are all based on 3GPP technology. Their signal frequency spectrum range vary according to country and specific protocol technology details.

WWAN communication protocols suite and LTE-M have a common spectrum as they are all based on 3GPP technology. They work in licensed signal spectrum ranges which vary according to country and specific protocol details. However, except the cellular network protocols and LTE-M, most of the protocols work in license-free signal bands, such as the common called Industrial, Scientific, and Medical (ISM) signal frequency bands, including 13.56 MHz, 433 MHz, and 2.4 GHz. WLAN often uses the U-NII signal band with a frequency spectrum range around 5.8 GHz. Besides, lightly licensed signal bands are also popular, including signal frequency bands of 868 MHz, 915 MHz and 920 MHz.

IV. CONCLUSION AND FUTURE PROSPECTS OF IOT COMMUNICATION PROTOCOLS

Designed for diverse situation and with growing technique, IoT communication protocols show different features in technology roadmap, communication distance, and signal frequency spectrum rang. Each of these protocols has their advantages, drawbacks and specific applicable scope, thus numerous protocols work in close coordination with a hierarchical system in actual industrial scenarios. At present, the protocols can be classified into different architecture from 3 main aspects: OSI model, IEEE 802 protocol standard and network types. However, the current ecosystem of these protocols still has room for improvement. This paper considers that the protocols should be ameliorated mainly in their optimization, integration and information security.

A. *Optimization and Integration*

IoT has been developed for many years, but it still relies on data transmission protocols originally designed for the Internet and mobile Internet, such as 3G, 4G or other WWAN protocols. Admittedly, several Internet protocols are not fully applicable to IoT, thus they may reduce the efficiency and performance of IoT communications when merely grafted into this field. For example, HTTP is too complex to be execute by devices with limited processing power of IoT devices, while Wi-Fi protocol consumes much energy [19]. However, the existing technology of IoT communication protocols needs time to improve. Some researches pointed out that Wi-Fi, Bluetooth, and WWAN are the main force of IoT communication protocols [19]. At present, the low-power-consuming version of Wi-Fi is already on the way of application. The prospect of 5G is generally viewed with optimism, but when applied to the IoT, optimization should be adapted in energy consumption or other aspect.

In addition, due to the motive of commercial competition or technical limitation, some IoT communication protocols cannot easily switch or connect to each other. In order to realize the versatility of the connection of objects in the IoT, it is an inevitable trend to formulate relevant standards in the future to promote the integration and intercommunication of various IoT communication protocols. At the same time, it is necessary to further develop sensor networks and promote the development of technologies such as chip design, sensors, and radio frequency identification [20].

B. Information Security

Information security is one of the most concerned issue so far in IoT communication. The number of perception terminals in the IoT is huge and diverse, and they can perceive, capture and measure the ID, position, displacement, surrounding environment, current activity state and other data of people or objects at anytime and anywhere. Therefore, the privacy and information security issues involved in IoT communication are more complex than those in other means of communication.

Strict technical specifications for communication security of IoT should be formulated to verify the data security and safety precautions of the actual IoT communication system and prevent companies from stealing private information of users. At the technical level, further improvement of access control, authentication and identity management mechanisms should be paid more attention to better identify and match up the authenticate users and IoT devices.

At present, homomorphic encryption, anonymization and routing protocol are three main methods to protect privacy adopted by the major IoT communication protocols. However, due to the complexity of data sources and data structures, there are much difficulty to well process and protect those data. It is still indispensable to optimize technologies to better ensure information security. Moreover, some research proposed that the introduction of semantic annotation and ontology into privacy protection technology is the future. Draw support from mantic annotation and ontology processing technology, the IoT communication protocols could hide or destroy the information of a specific semantic attribute, and thus realizes information hiding to ensure the security of the communication [21].

ACKNOWLEDGMENT

This work was supported by the National Key Research and Development Program of China (No. 2017YFF0209504). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Wen Jiabao. Report on the Work of the Government - March 5, 2010 at the Third Session of the Eleventh National People's Congress [J].Today, Xinjiang, 2010, 56 (6): 6-20.

[2] Sun Qibo , Liu Jie , Li Shan. IoT: Summarize on Concepts , Architecture and Key Technology Problem. [J].Journal of Beijing University of Posts and Telecommunications, 2010, 33 (3): 1-9.

[3] Alkhatib A A A, Baicher G S. Wireless Sensor Network Architecture[J]. International Proceedings of Computer Science & Information Tech, 2012.

[4] Zhu Q, Wang R, Chen Q, et al. IOT Gateway: BridgingWireless Sensor Networks into Internet of Things[C]. International Conference on Embedded and Ubiquitous Computing. IEEE, 2011:347-352.

[5] Bello O, Zeadally S, Badra M. Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT) [M]. Elsevier Science Publishers B. V. 2017.

[6] Qiao Q. Research on Key Technology of IoT Application Layer[J]. Telecommunications Science, 2011.

[7] Gubbi J, Buyya R, Marusic S, et al. Internet of Things (IoT): A vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7):1645-1660.

[8] Keysight Technologies. The IoT: Enabling Technologies and Solutions for Design and Test - Application Note [DB/OL], 2015. http://digsys.upc.es/ed//ISESC/terms/1516Q1/EX/EX1/IoT_Keysight_5992-1175EN.pdf

[9] Fu Guoqiang, Zhang Xianjin. Protocol analysis of IoT applicable to WoT architecture, [J]. Telecommunication Network Technology, 2014 (3): 4-9.

[10] Braden R. Requirements for Internet Hosts - Communication Layers[M]. RFC Editor, 1989.

[11] Rayes A, Salam S. The Internet in IoT—OSI, TCP/IP, IPv4, IPv6 and Internet Routing[M]// Internet of Things From Hype to Reality. Springer International Publishing, 2017.

[12] Qutabuddin M, Hazmi A, Badihi B, et al. Performance analysis of IoT-enabling IEEE 802.11ah technology and its RAW mechanism with non-cross slot boundary holding schemes[C]// World of Wireless, Mobile and Multimedia Networks. IEEE, 2015:1-6.

[13] Zhang D, Zhang B, Zhou Z, et al. Distributed Cache Enabled V2X Networks: Proposals, Research Trends and Challenging Issues[J]. 2018.

[14] Lee J S, Su Y W, Shen C C. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi[C]// Industrial Electronics Society, 2007. IECON 2007. Conference of the IEEE. IEEE, 2008:46-51.

[15] Freedman M J. A peer-to-peer anonymizing network layer[J]. Lecture Notes in Computer Science, 2002, 2429:121-129.

[16] Federal Communications Commission Technological Advisory Council, IoT Working Group Position Statements [DB/OL]. https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92314/TAC-Internet-of-Things-Position-Statements.pdf

[17] Lente H V, Spitters C, Peine A. Comparing technological hype cycles: Towards a theory[J]. Technological Forecasting & Social Change, 2013, 80(8):1615-1628.

[18] Cao L, Zheng H. Distributed spectrum allocation via local bargaining[C]// Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005. 2005 Second IEEE Communications Society Conference on. IEEE, 2005:475-486.

[19] Salman T, Jain R. Networking Protocols and Standards for IoT [M]. John Wiley & Sons, Inc. 2017.

[20] Liu Qiang, Cui Li, Chen Haiming. Key Technologies and Applications of Internet of Things [J]. Computer Science, 2010, 37 (6): 1-4.

[21] Qian Ping, Wu Meng. Survey on privacy preservation in IoT [J]. computer application research, 2013, 30 (1): 13-20.