Internet of Things (IoT) Communication Protocols : Review

Shadi Al-Sarawi[1], Mohammed Anbar[2] , Kamal Alieyan[3] , Mahmood Alzubaidi[4]
[1-4]National Advanced IPv6 Centre (NAV6)
Universiti Sains Malaysia, 11800 Gelugor, Penang, Malaysia
Emails :(Shadi, Anbar, Kamal_alian, Mahmood)@nav6.usm.my

***Abstract*-- Internet of Things (IoT) consists of smart devices that communicate with each other. It enables these devices to collect and exchange data. Besides, IoT has now a wide range of life applications such as industry, transportation, logistics, healthcare, smart environment, as well as personal, social gaming robot, and city information. Smart devices can have wired or wireless connection. As far as the wireless IoT is the main concern, many different wireless communication technologies and protocols can be used to connect the smart device such as Internet Protocol Version 6 (IPv6), over Low power Wireless Personal Area Networks (6LoWPAN), ZigBee, Bluetooth Low Energy (BLE), Z-Wave and Near Field Communication (NFC). They are short range standard network protocols, while SigFox and Cellular are Low Power Wide Area Network (LPWAN).standard protocols.**

This paper will be an attempt to review different communication protocols in IoT. In addition, it will compare between commonly IoT communication protocols, with an emphasis on the main features and behaviors of various metrics of power consumption security spreading data rate, and other features. This comparison aims at presenting guidelines for the researchers to be able to select the right protocol for different applications.

Keywords: 6LoWPAN, AES, ASK, BLE, BPSK, BT, CCK, COFDM, DBPSK, DSSS, ESP, FHSS, ICT, IoT, IPv6, MAC, NFC, RC4, WPAN, WSNs, OFDM, O-QPSK, TDMS and UNB.

I. INTRODUCTION

IoT Information Communication Technology (ICT) is expected to be a revolution in transferring the information from human-to-human, human-to-things and things-to-things. Smart devices can connect, transfer information and make decisions on behalf of people. This new technology is called 'connectivity for anything'. It can connect anywhere, anytime and anything.

The IoT environment consists of an enormous number of smart devices, but with many constraints. Processing capability storage volume, short in power life and radio range are among of these constraints. Therefore, the IoT implementation requires a communication protocols that can efficiently manage these conditions [1] [2] [3] [9].

This paper will also review and compare between IoT communication protocol which is realized as a clear insight for the readers of different IoT communication protocol vision, their pros and cons, and their power speed and range consumption.

The rest of the paper will be organized as following; Section II will describe the IoT communication protocols available from previous literature. In section III the Table 1 illustrates the different communication technologies for IoT applications and their properties. Finally, the conclusion of the study is in hand of the final Section.

II. IOT COMMUNICATION PROTOCOLS

This section will give a thorough description for each communication protocol. Commonly, the communication protocols for IoT can be categorized into: (1) LPWAN and (2) short range network, as shown in Figure 1

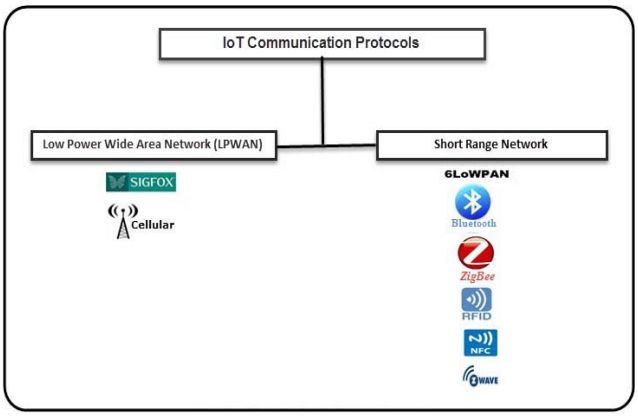

Figure 1 : IoT communication protocols

978-1-5090-6332-1/17/$31.00 ©2017 IEEE

II.I Low Power Wide Area Network (LPWAN)

II.I.A SigFox

SigFox is a low power technology for wireless communication of a diverse range of low energy objects such as sensors and M2M applications. It allows the transportation of small amounts of data ranging up to 50 kilometers. SigFox uses Ultra Narrow Band (UNB) technology. This technology is only designed to handle low data transfer speeds of 10 to 1, 000 bits per second, and can run on a small battery. NFC technology is used in smart meters, patient monitors, agriculture, security devices, street lighting and environmental sensors. SigFox support start network topology [5] [7].

II.I.B Cellular

Cellular technology is a great fit for applications that need high throughput data and have a power source of IoT application that requires operation over longer distances. It can take the advantage of GSM/3G/4G cellular communication capabilities it can provide reliable high speed connectivity to the internet .However, it needs high power consumption. Therefore, it's not suitable for M2M or local network communication. Cellular communication protocol is also used for many applications especially for applications that involve mobile devices. Cellular topology depends on various based technology [5] [24] [21].

II.II Short Range Network

II.II.A 6LoWPAN

6loWPAN is the first and most commonly used standard in IoT communication protocols, since it is an IP-based standard internetworking protocol. It can be connected directly with another IP network without intermediate entities like translation gateways or proxies. This standard has been created by the Internet Engineering Task Force (IETF), a standard Internet Protocol (IP) communication over low power wireless IEEE802.15.4 networks utilizing IPv6. It supports 2^{128} IP addresses, so the numbers of addresses are more than sufficient. This aims at supporting different length of addresses. It is also low cost, low bandwidth power consumption. 6loWPAN supports different types of topologies like mesh and star topology. 6loWPAN proposes an adaptation layer in between the MAC layer and the network layer (IPv6) in order to handle interoperability between IEEE 802.15.4 and IPv6. The most competitive alternative to 6LoWPAN is ZigBee as it is seen in Figure 2. Both of them use the same IEEE 802.15.4 protocol at the physical layer [6] [22][35].

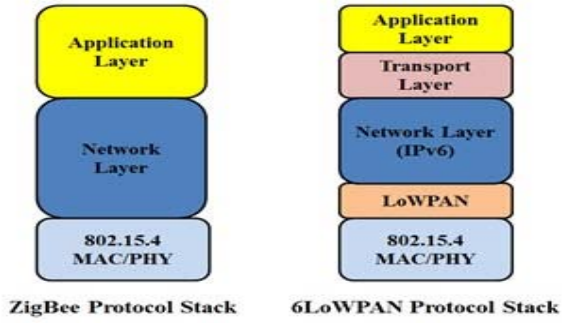

Figure 2: 6LowPAN and ZigBee protocol stack [35]

II.II.B ZigBee

ZigBee protocol has been created by ZigBee Alliance based on low-power wireless IEEE802.15.4 networks standard. ZigBee is created to be a standard to suite high level low cost communication protocols creating personal area networks from small size, low power digital radios that transmit data over longer distances. at the same time, it will be used in applications that require a low data rate, longer battery life, and secure networking devices. Moreover, ZigBee can support different types of topologies like mesh, star and tree network topology [5] [6].

II.II.C BLE

BLE is also known as Bluetooth smart which is a significant protocol for IoT application. It's designed and enhanced for short-range, low bandwidth, and low latency for IoT applications. The advantages of BLE classic Bluetooth include lower power consumption, lower setup time, and supporting star network topology with unlimited number of nodes[5] [6].

II.II.D RFID

RFID has a variety of standards including (ISO, IEC, ASTM International, the DASH7 Alliance and EPC-global. .RFID systems consisting of a reading device called reader, and a small radio frequency transponder called RF tag. This tag is electronically programmed with unique information that has a distance reading characteristic. There are two technologies of RFID tag systems: the first is called active reader tag system and the other is called passive reader tag system. Active tags are battery- powered, more expensive, and use higher frequencies, while the passive tag one uses lower frequencies and does not have an internal power source. Because RFID information is static and must be programmed into the tag, it cannot be used directly for the measurement or diagnostic data .Some of IoT applications using RFID include smart shopping, health care, national security and agriculture. RFID can support P2P network topology [4] [7] [8].

II.II.E NFC

NFC is a very short range wireless communication technology that enables the data transmission among devices by touching them together or bringing them together no more than a few inches. NFC uses similar technology principles in RFID. However, it is not only used for identification but also

for more elaborate two-way communication. NFC has a tag that can contain small amount of data. This tag can be read only (similar to RFID tags for identification purposes) or can be rewritable and be altered later by the device .There are three main operating modes for NFC: card emulation mode (passive mode), reader/writer mode (active mode) and peer-to-peer mode). NFC technology is extensively used in mobile phones, industrial applications and contactless payment systems. Similarly, NFC makes it easier to connect, commission, and control IoT devices in different environments like home, factory and the work. NFC supports P2P network topology [4] [6] [7] [23].

II.II.F Z-Wave

Z-Wave Is a low power MAC protocol developed by Zensys that uses wireless home automation to connect 30-50 nodes and has been used for IoT communication, especially for smart home and small commercial domains. This technology is designed for small data packets at relatively low speeds up to 100 kbps and 30 meter point to point communication. Therefore, it is suitable for small messages in IoT applications, like light control, energy control, healthcare control. Z-Wave depends on two types of devices (controlling and slave). Slave nodes properties are low cost devices unable to initiate messages. It can only reply and execute commands sent by controlling devices that initiate messages within the network. Z-Wave support mesh network topology [6] [7] [23].

Figure 3: IoT IP coverage [34]

III. COMMARIZION BETWEEN COMMUNICATION PROTOCOLS IN IOT

This section aims to provide a guideline for research to select the right communication protocol by providing a comparison between the above mentioned communication protocols. Different criteria are used to benchmark the differences between the communication protocols. Such criteria include standard, network, topology, power, range, cryptography, spreading, modulation type, coexistence mechanism, security and power consumption as shown in IoT IP coverage in Figure 3 and Table 1.

In terms of security, all the nine communication protocols have the encryption and authentication mechanisms. 6LoWPAN, ZigBee, BLE, NFC, Z-Wave use the Advanced Encryption Standard (AES) block cipher with counter mode, while Cellular and RFID use RC4. However, several serious weaknesses were identified. AES is extremely secure while RC4 is not. RC4 is very fast compared to AES.

In terms of power consumption, 6LoWPAN, ZigBee, BLE, Z-Wave and NFC are designed for portable devices and limited battery power. Thus, it offers low power consumption. On the other hand, Cellular high power consumption is in the list.

In term of data rate, 6LoWPAN, ZigBee, BLE, NFC, SigFox and Z-Wave have data rate < = 1 Mbps. However, RFID has the highest data rate of 4 Mbps

In term of range, SigFox and Cellular are range longer than the coverage of several KM. However, 6LoWPAN, ZigBee, BLE, NFC, Z-Wave, and RFID are range shorter that cover less than KM. Table 1 shows a comparison between the communication protocols in IoT.

According to the comparison of communication protocol in IoT, 6LoWPAN will be the future protocol because it is IP-based WSN. It allows a vast number of smart devices to be deployed over the internet easily by using the huge address space of IPv6 for data and information gathering through features and behaviors of various metrics, including low bandwidth, different topologies, and star or mesh, power consumption, low cost, scalable networks.

.

Characteristics	6LoWPAN	ZigBee	BlueTooth LE	RFID	NFC	SigFox	Cellular	Z-Wave
Standard	IEEE 802.15.4 [18]	IEEE802.15.4 [18]	IEEE 802.15.1 [18]	RFID [18]	ISO/IEC 14443 A&B,JIS X-6319-4 [30]	SigFox [20]	3GPP and GSMA, GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G) [7]	Z-Wave [18]
Frequency Bands	868Mhz(EU) 915Mhz(USA) 2.4Ghz(Global) [12]	2.4 GHz [19]	2.4 Ghz [15]	125 kHz, 13.56 MHz, 902-928 MHz [31]	125Khz 13.56Mhz 860Mhz [15]	868MHz (EU) 902MHz(USA) [20]	Common Cellular bands [31]	868 MHz - 908 MHz [12]
Network	WPAN [23]	WPAN [23]	WPAN [23]	Proximity [10]	P2P Network [23]	LPWAN [10]	WNAN [20]	WPAN [23]
Topology	Star Mesh Network [16]	Star ,Mesh Cluster Network [19]	Star –Bus Network [16]	P2P Network [04]	P2P Network [14]	Start Network [20]	NA [05]	Mesh Network [19]
Power	(1-2 years lifetime on batteries) Low power consumption [14]	30 mA Low power [26]	30 mA Low Power [26]	Ultra-low power [05]	50 mA low power Very Low [30]	10 mW - 100 mW [20]	High power consumption [05]	2.5 mA Low power consumption [14]
Data Rate	250 kbps [15]	250 kbps [16]	1Mbps [15]	4 Mbps [18]	106 212 or 424 kbps [15]	100 bps(UL), 600 bps(DL) [20]	NA [05]	40kbps [17]

Range	Short Range 10-100 m [12]	Short Range 10-100 m [12]	Short Range ~15-30 m [15]	Short Range Up to 200 m [18]	Short Range 0-10cm 0-1m 10cm-1m [15]	Long Range 10km(URBAN) 50km (RURAL) [20]	Several km [31]	30m (indoors) 100(outdoors) [12]
Security	AES [13]	AES [13]	E0 Stream AES-128 [13]	RC4 [32]	RSA AES [25]	Partially addressed [29]	RC4 [27]	AES-128 [13]
Spreading	DSSS [17]	DSSS [17]	FHSS [17]	DSSS [33]	GSMA [23]	DSSS [11]	DSSS [27]	No [17]
Modulation Type	BPSK O-QPSK [12]	BPSK/BPSK O-QPSK [12]	TDMA [17]	FSK PSK [32]	ASK [23]	UNB DBPSK (UL), GFSK(DL) [20]	BPSK OFDM [27]	BFSK [28]
Features	Commonly Used Internal Access [31]	Mesh Network [31]	Low power version available [31]	Low Cost [31]	Security [31]	Long Battery life (up to 20 years) Low Cost [10]	Longer Range [31]	Simple Protocol [31]
Common Applications	Monitor and Control via internet [31]	Home industry monitoring and controlling [31]	Wireless headsets, Audio Applications [31]	Tracking, Inventory, Access [31]	Payment, Access [31]	Street Lighting Energy meters [24]	M2M [31]	Home Monitoring and Control [31]

Table 1: IoT communication protocols

IV. CONCLUSION

As there are many wireless technologies in the IoT network, each one has certain specifications and benefits. However, it is quite hard to conclude which one is perfect. Therefore, the question that someone needs to answer is "which technology is the best one for my application. From this point of view, the current study reviews and compares between the common communication protocols in IoT. Different criteria used to compare between the communication protocols. Such criteria include network, topology, power, range, cryptography, spreading, modulation type, coexistence with mechanism and power consumption. In Future work, this work will be extended to review IoT applications and IoT security mechanisms to dynamically detect the attacks in IoT, even new IoT attacks and raise an alarm in case of any anomaly.

REFERENCES

[1] Tan, L. & Wang, N. 2010. Future internet: The internet of things. Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on: V5–376.
[2] Strategy, I. & Unit, P. 2005. ITU Internet Reports 2005: The internet of things. Geneva: International Telecommunication Union (ITU).
[3] Li, X., Xuan, Z. & Wen, L. 2011. Research on the architecture of trusted security system based on the internet of things. Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on: 1172–1175.
[4]Porkodi, R. & Bhuvaneswari, V. 2014. The Internet of Things (IoT) applications and communication enabling technology standards: An overview. Intelligent Computing Applications (ICICA), 2014 International Conference on: 324–329.
[5]Samie, F., Bauer, L. & Henkel, J. 2016. IoT technologies for embedded computing: A survey. Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2016 International Conference on: 1–10.
[6] Salman, T. 2015. Internet of Things Protocols and Standards.
[7] Affairs, M. of E. n.d. 2015.Internet of Things in the Netherlands Applications trends and potential impact on radio spectrum.Startix
[8]Paavola, M. 2007. Wireless technologies in process automation-review and an application example. Control Engineering Laboratory, University of Oulu.
[9] Le, A., Loo, J., Lasebae, A., Aiash, M. & Luo, Y. 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. International Journal of Communication Systems, 25(9): 1189–1212.
[10] Martha Zemede, K. T. 2015. Explosion of the Internet of Things:What does it mean for wireless devices?. Keysight Technologies
[11] Goursaud, C. & Gorce, J.-M. 2015. Dedicated networks for IoT: PHY/MAC state of the art and challenges. EAI endorsed transactions on Internet of Things.
[12] Gomez, C. & Paradells, J. 2010. Wireless home automation networks: A survey of architectures and technologies. IEEE Communications Magazine, 48(6).
[13] Rathnayaka, A. D., Potdar, V. M. & Kuruppu, S. J. 2011. Evaluation of wireless home automation technologies. Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on: 76–81.
[14] Aragues, A., Mart'\inez, I., Del Valle, P., Muñoz, P., Escayola, J. & Trigo, J. D. 2012. Trends in entertainment, home automation and e-health: Toward cross-domain integration. IEEE Communications Magazine, 50(6).
[15] López, P., Fernández, D., Jara, A. J. & Skarmeta, A. F. 2013. Survey of internet of things technologies for clinical environments. Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on: 1349–1354.
[16] Tabish, R., Mnaouer, A. B., Touati, F. & Ghaleb, A. M. 2013. A comparative analysis of BLE and 6LoWPAN for U-HealthCare applications. GCC Conference and Exhibition (GCC), 2013 7th IEEE: 286–291.
[17] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys \& Tutorials, 17(4): 2347–2376.
[18] Kuzlu, M., Pipattanasomporn, M. & Rahman, S. 2015. Review of communication technologies for smart homes/building applications. Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE: 1–6.
[19] Samuel, S. S. I. 2016. A review of connectivity challenges in IoT-smart home. Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on: 1–4.
[20] Raza, U., Kulkarni, P. & Sooriyabandara, M. 2017. Low Power Wide Area Networks: An Overview. IEEE Communications Surveys \& Tutorials.
[21] Frantz, T. L. & Carley, K. M. 2005. A formal characterization of cellular networks.
[22] Hossen, M., Kabir, A., Khan, R. H., Azfar, A. & others. 2010. Interconnection between 802.15. 4 devices and IPv6: implications and existing approaches. arXiv preprint arXiv:1002.1146.
[23] Azamuddin Bin Ab Rahman, R. J. 2015. Comparison of Internet of Things (IoT) Data Link Protocols.
[24] Alliance, L. 2015. A technical overview of LoRa and LoRaWAN. White Paper, November.
[25] Shreya Shah, T. M. n.d. Security of NFC Data. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6,(ISSN: 2277 128X).
[26] Hughes, J., Yan, J. & Soga, K. 2015. Development of wireless sensor network using bluetooth low energy (BLE) for construction noise monitoring. International Journal on Smart Sensing and Intelligent Systems, 8(2): 1379–1405.
[27] Ahmad, A. 2005. Wireless and mobile data networks. John Wiley \& Sons. [28] Gomez, C., Oller, J. & Paradells, J. 2012. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors, 12(9): 11734–11753.
[29] Sanchez-Iborra, R. & Cano, M.-D. 2016. State of the art in LP-Wan solutions for industrial IoT services. Sensors, 16(5): 708.
[30] Cerruela Garc'\ia, G., Luque Ruiz, I. & Gómez-Nieto, M. Á. 2016. State of the Art, Trends and Future of Bluetooth Low Energy, Near Field Communication and Visible Light Communication in the Development of Smart Cities. Sensors, 16(11): 1968.
[31] Frenzel, L. 2012. The Fundamentals of Short-Range Wireless Technology. ELECTRONIC DESIGN, Oct, 11.
[32] Alarcon-Aquino, V., Dominguez-Jimenez, M. & Ohms, C. 2008. Desing and Implementation of a Security Layer for RFID Systems. Journal of applied research and technology, 6(2): 69–82.
[33] Amin, M., Reaz, M., Jalil, J. & Rahman, L. 2012. Digital modulator and demodulator IC for RFID tag employing DSSS and Barker code. Journal of applied research and technology, 10(6): 819–825.
[34] Friess, P. 2013. Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.
[35] Lu, C.-W., Li, S.-C. & Wu, Q. 2011. Interconnecting ZigBee and 6LoWPAN wireless sensor networks for smart grid applications. Sensing Technology (ICST), 2011 Fifth International Conference on: 267–272.