International Journal of Innovation in Computer Science and Information Technology
Vol.1, NO.2 , P:71 - 78
Received: 04 Des 2018
Accepted: : 02 Mar 2019

Communication Protocols in the Internet of Things (IoT): Comparing 7 Protocols

Farid sheykhnourani, Department of Computer Novin Institute of Higher Education, Ardabil, Iran
Farid_sh_nourani@yahoo.com
Yasser Narimani, Department of Computer Novin Institute of Higher Education, Ardabil, Iran
Yasser.narimani@qiau.ac.ir
Farid Soleymani, Department of Computer Novin Institute of Higher Education, Ardabil, Iran
Farid.soleymani@yahoo.com

Summary

The rapid growth of information and communication technology has led to the appearance of new phenomena in this area every day. One of these phenomena is the Internet of Things (IoT) technology, which aims to create a comfortable life in the form of a smart life. The Internet of things is a new technology used to connect things to each other over the Internet, the aim is to measure and control remotely an objects. The definition of IoT is that they are referred to as a set of things that have a digital identity and users can manage and organize these things using devices such as computers and smartphones and their applications and these things are capable of communicating with users and even with each other. The process of sending data on the Internet of Things does not require things to interact, and the data is sent automatically and based on the initial settings that are made on the hardware. Meanwhile, communication protocols play an important role. Choosing an appropriate communication protocol based on the needs and conditions of the environment is one of the most important issues in the Internet of Things.

In this paper, various communication protocols of the IoT such as 6LowPAN, NFC, BLE, Z-Wave, ZigBee, SIGFOX, Cellular are introduced and compared with each other in the Internet of Things. The goal of this comparison is to provide guidance to researchers who can select the appropriate protocol for different applications.

Keywords: Internet of Things, 6LowPAN, BLE, NFC, Z-Wave, ZigBee, SIGFOX, Cellular

Introduction

The notion of the Internet in our minds is a global network in which computers, phones, humans, and etc., communicate locally with devices connected to the network anywhere. Let's take a world in which the Internet goes beyond its current concept and includes the objects around us. Here is a concept called the Internet of Things (IoT), which can be said to be a network of networks composed of a large number of objects, sensors and devices, etc., that through the communications and information infrastructure to provide services through the processing of intelligent data and management for the different applications are connected [1]. The Internet of Things has strangely evolved over the past years, so that we can say that this is an emerging trend for researchers. Many of the findings in the area of the network indicate that this is a wide range [7]. The Internet of Things is not a single technology, but offers a range of electronics, communications, software engineering, hardware, enterprise analysis and other technologies in the form of an integrated technology. The term "Internet of Things" (IOT) was first introduced by Quinn Ashton in 1999. He describes a world in which everything has a digital identity for themselves and allows computers to organize and manage them [19].

In this paper, Internet of Things communication protocols are reviewed and to enhance readers insights their advantages, disadvantages, speeds, and rates of use are discussed. The paper is as follows: The second part describes the existing IoT communication protocols. In Section 3, the proposed protocols are compared in tabular form, and finally, the conclusions are presented.

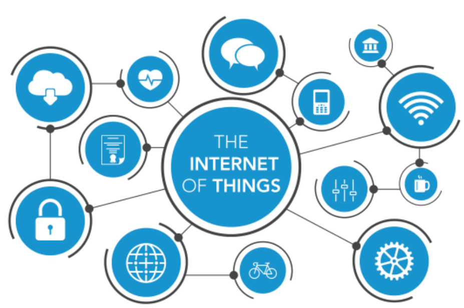

Figure (1) Internet of Things schematic

Method of Work

In this section, some of the common communication protocols of the Internet of Things, such as 6LowPAN, BLE, NFC, Z-Wave, ZigBee, SIGFOX, Cellular are introduced and compared in the following.

• 6lowpan

Before introducing 6lowpan technology, it's best to get acquainted with the concept of pan. Pan is a computer network that provides communications around a person. The range of this personal network is not several meters. The 6LoWPAN protocol, its name is derived from the IPv6 Low Power Wireless Personal Area Network, is a network standard for the Internet of Things that developed in 2007. This protocol is used for low speed and low power in the wireless personal area network (WPAN). In other words, it can be said used for applications that have a lot of nodes and have a battery life of several years [12]. This technology allows IPv6 to be used by 802.15.4 standard. 6LoWPAN is usually used in a wireless sensor network. Also, the Thread protocol uses 6LoWPAN for smart home. Generally it can be said, the 6LowPAN is a network protocol that defines encapsulation and header compression mechanisms. In fact, 6LoWPAN is an IPv6 protocol designed for low power and limited processing capabilities. The 6LoWPAN group defines how to encapsulate and declare the header compression mechanism, thus, IPv6 packets can be sent or received on networks based on IEEE 802.15.4 [3]. The advantages of this protocol are high connectivity and compatibility with traditional architectures and low power consumption.

Figure (2) 6LowPAN Icons

• BLE

Bluetooth low energy (BLE) or Smart Bluetooth is a short-range communication protocol and media access layer and physical layer that is widely used for the carrier's internal network. Bluetooth Low energy is a completely different version of Bluetooth's old radio [17]. This technology is designed with a new protocols and architecture specifically designed to run on low power resources like a coin batteries. It must be understood that this radio technology is not a newer version of the old Bluetooth or it's not the replacement. The technology has three new types of Bluetooth that are interconnected [2]. BLE uses an adaptive frequency hopping algorithm to jump between existing channels, which are just a subset of the available frequencies, and thus can quickly prevent the loss of packets due to the presence of a bad channel. This technique generates less energy on the radio [10]. Like other wireless devices, BLE uses 2.4 GHz ISM band. Unlike the old Bluetooth, it has 79 channels with 1 MHz bandwidth. The main functions of the BLE are GAP and GATT profiles.

Figure (3) BLE Icons

- **NFC**

NFC (Near Field Communication) is a technology that enables simple and safe two-way interactions between electronic devices, and especially applicable for smartphones, allowing consumers to perform contactless payment transactions, access digital content and connect electronic devices. The NFC protocol is used for communication in a very short range (4 cm), such as placing a tag on a tag reader. NFC is commonly used in payment systems, but in presence and absence systems and labels Smart objects are also used to track assets in industrial Internet of things applications [15]. For communication between two devices through the NFC communication protocol, the sender's signal (for example, mobile phone) is received by the receiver antenna. If the receiver is disabled, this induction signal will provide the energy needed for the function of the tag, and the stored information via the receiver antenna will be sent to the sender antenna and thus communicated. If the receiver is also active, Because of the full duplex of this protocol, both will be able to send and receive information at the same time. The advantages of this protocol include; NFC tags and antennas are very inexpensive, small and lightweight and can be installed in very small sizes on posters, credit cards and electronic devices. NFC communication is very simple and fast and does not require information such as username and password [9].

Figure (4) NFC Icons

- **Z-wave**

The Z-Wave protocol was developed in 2001. This protocol is one of the first IoT protocols to be widely commercialized and based on Z-Wave Alliance ZAD12837 / ITU-T G.9959 standard. The Z-Wave protocol is a smart home standard that is implemented for communication with the devices. This protocol enables household products such as locks, lights and thermostats to communicate with each other and uses RF signals to do this.

In this protocol, used by a central controller for local communication with the device, that called the HUB. For communication over the Internet, the hub must be connected to cloud services developed by manufacturer companies and remotely exploited to work from anywhere in the world, and connecting to the hub and the central controller and transferring the commands [11]. The Z-Wave-based products that are in smart homes are stronger and less efficient than home Wi-Fi networks. The Z-Wave protocol optimized for reliable and low-latency communication of small data packets with data rates up to 100 kbps. this protocol operates in the sub-1GHz band and is impervious to interference from WiFi and other wireless technologies in the 2.4-GHz range such as Bluetooth or ZigBee [6]. The advantage of this protocol can be said; because the protocol uses frequencies lower than the frequencies of other devices, the possibility of the interconnection with the frequency of other devices in this standard is greatly reduced. This means that there are fewer devices battle to access and transmit data using that frequency, which results in optimized data transfer and also speeds up the data transmission process. Another advantage of this protocol is that all the devices used in this protocol, regardless of the manufacturer's type, device type and version, can be connected.

Figure (5) Z-wave Icons

- **ZigBee**

ZigBee is a smart grid that is used for high-level communication protocols and low-data data rates. This protocol was conceived in 1998, then standardized in 2003 and modified in 2006. The protocol is used in small and low power personal networks (LANs) and its technology is based on IEEE 802.15.4 standard [14]. This protocol is somewhat similar to Z-Wave and is like one of the most popular smart home protocols. The protocol has been developed primarily for commercial purposes, but is currently being used as a standard language for intelligent communications in domestic and commercial applications. One of the main advantages of this protocol is low energy consumption that it still Z-Wave uses the Deep Sleep technology to reduce power consumption. The security of this protocol is also very advanced and has been used by cryptographic technologies of financial institutions that encrypt network data, drives, and encrypted information [13].

Figure (6) ZigBee Icons

- **SIGFOX**

SIGFOX technology is in the category of LPWAN technologies, which provides low power consumption and, as a result, high battery life for the Internet of objects applications. This technology was introduced in 2009 and then grew rapidly. SIGFOX provides a standard way of collecting data from sensors and devices with a single, standard-based set of APIs. Besides, the SIGFOX disruptive technology complements traditional cellular M2M by enabling global, ubiquitous, ultra-long battery life solutions at the lowest cost [18]. SIGFOX has great potential as a secondary connectivity solution to enable lower battery consumption and better user experience .SIGFOX provides the network, the technology and the expert ecosystem, which are necessary to help companies and organizations make the most of their IoT ambitions [4]. SIGFOX technology utilizes the free ISM band to create the right infrastructure for the Internet of objects. In the SIGFOX network, which is specially designed for the Internet of Things, data is transmitted to 12 bytes in frequency bands without the need for authorization and through ultra-narrow band (UNB) modulation. This technology uses Binary Phase Shift Keying (BPSK) from radio modulation to transmit data. also been used UNB modulation for high permeability in bodies. SIGFOX Network Layer Protocols are confidential and only available to the company [5].

Figure (7) SIGFOX Icons

- **Cellular**

Among the enabling technologies of the IoT, Cellular-based communication is the most promising and more efficient. The Cellular technology is suitable for applications that require high power data and have a power source of IoT application that requires operation over longer distances and based on GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G) standard. A many communication technologies in the LPWAN can overcome the short range constraint of the LAN and still satisfy the power and latency limitation using either proprietor or cellular technologies [8]. Cellular communication protocol is also used for many applications especially for applications that involve mobile devices. Cellular topology depends on various based technology [16].

Figure (8) Cellular Icons

Result

In this part of the paper, the communication protocols introduced in the second part are compared in a table based on frequency criteria, range and data rates. The standard for each protocol is shown and the graph for comparing each criterion is shown.

Table 1- Comparison of IoT communication protocols

Profile	Standard	Frequency	Range	Data Rate
6LowPAN	RFC6282	2.4 GHz	10-30 m	20-250 kbps
BLE	Bluetooth 4.2 core specification	2.4 GHz	50-150 m	260 kbps- 1 Mbps
NFC	ISO/IEC 18000-3	13.56 MHz	10 cm	100-420 kbps
Z-Wave	Z-Wave Alliance ZAD12837 / ITU-T G.9959	908.42 MHz	30 m	9.6- 100 kbps
ZigBee	ZigBee 3.0 based on IEEE802.15.4	2.4 GHz	10-30 m	250 kbps
SIGFOX	Sigfox	900 MHz	3-50 km	10-1000 bps
Cellular	GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)	900-2100 MHZ	35-200 km	35 kbps-10 Mbps

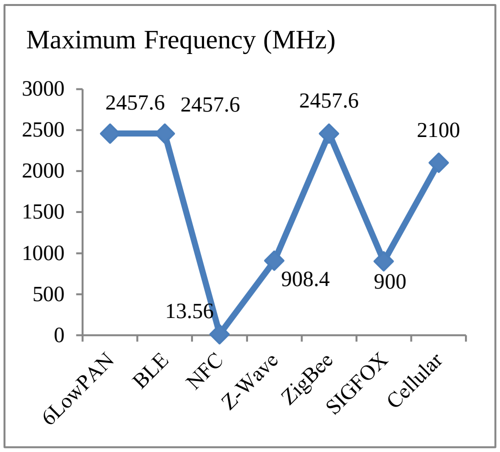

Figure (9) Maximum Frequency (MHz) Comparison of IoT communication protocols

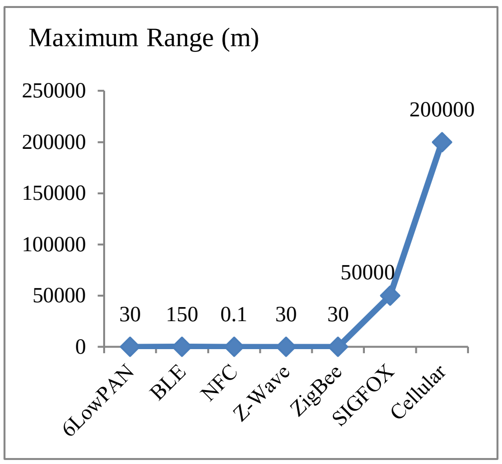

Figure (10) Maximum Range (m) Comparison of IoT communication protocols

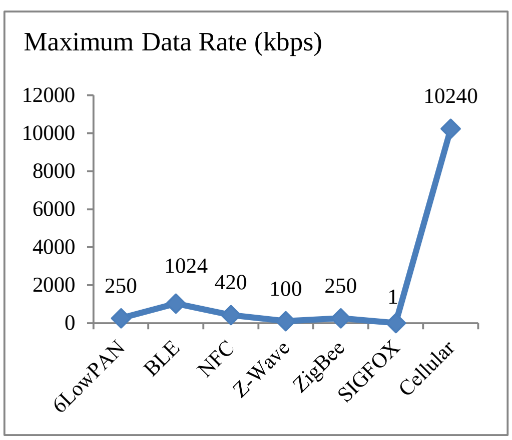

Figure (11) Maximum Data Rate (Kbps) Comparison of IoT communication protocols

Conclusion

The choice of network technology will affect the design of the Internet of things (IoT) components and the affiliations between them. For example, and based on the results obtained in Figure 9 to 11, we can say if the main factor in network design is frequency, the 6LowPAN, SIGFOX and ZigBee protocols will be appropriate for a high frequency response and NFC protocol will be the appropriate choice for low frequency requirements. This is also the case for data rate and range factors. But as noted above, since the design of a network requires the consideration of various factors, selecting the appropriate communication protocol is of high value. Network ranges, data rates, and power consumption are all directly related to each other. If you increase the network range or increase the amount of data sent, the Internet of things piece will require more power for this change. For a smart home-building project, the power consumption criterion is a low priority because we can power the components using a power outlet, and our higher priorities include bandwidth constraints and data loss on the connection. So, we can use Wi-Fi to give us the bandwidth that is acceptable and allow us to connect to the hardware of our project. However, Wi-Fi is not optimal for low-power components and is not suitable for battery-powered pieces. In this paper, we provide an overview of the existing communication protocols of the Internet of things. You should choose the best technology that suits your needs and challenges in the Internet of Things.

Reference

[1] Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The Internet of Things (IoT): An Overview. International Journal of

engineering Research and Applications, 1(5), 71-82.
[2] Aliev, K., Rugiano, F., & Pasero, E. (2016, April). The Use of Bluetooth Low Energy Smart Sensor for Mobile Devices Yields an Efficient Level of Power Consumption. In Proceedings of the 1st International Conference on Advances in Sensors, Actuators, Metering and Sensing (ALLSENSORS'16) (pp. 5-9).
[3] Al-Kashoash, H. A. A., & Kemp, A. H. (2016). Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, 13(4), 268-274.
[4] Arun, M. R., & Kumar, S. S. (2017). Improvement of Security in IOT Sensor Network to Overcome Harmful Intruder by Optimizing the Existing Techniques. International Journal of Sensors and Sensor Networks, 5(6), 70.
[5] Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. IEEE Wireless Communications, 23(5), 60-67.
[6] Collotta, M., & Pau, G. (2015). A solution based on bluetooth low energy for smart home energy management. Energies, 8(10), 11916-11938.
[7] Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). Internet of Things applications: current and future development. In Innovative Research and Applications in Next-Generation High Performance Computing (pp. 397-427). IGI Global.
[8] Elsaadany, M., Ali, A., & Hamouda, W. (2017). Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges. IEEE Communications Surveys & Tutorials, 19(4), 2544-2572.
[9] Fan, K., Song, P., & Yang, Y. (2017). ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. Mobile Information Systems, 2017.
[10] Furst, J., Chen, K., Aljarrah, M., & Bonnet, P. (2016, April). Leveraging physical locality to integrate smart appliances in non-residential buildings with ultrasound and Bluetooth low energy. In 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 199-210). IEEE.
[11] Ishaq Unwala, Jiang Lu. (November 2017). IoT Protocols : Z-Wave and Thread. International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 3 Issue: 11.
[12] Kouka, N., Thalajoui, A., & Meddeb, A. (2016, July). QoS LowPAN for Internet of Things. In New Technologies for Distributed Systems (NOTERE), 2016 13th International Conference on (pp. 1-6). IEEE.
[13] Mounica, A., & Subbareddy, G. V. ZIGBEE TRANSMITTER FOR IOT WIRELESS DEVICES.
[14] Obaid, T., Rashed, H., Abou-Elnour, A., Rehan, M., Saleh, M. M., & Tarique, M. (2014). ZigBee Technology and its application in Wireless Home Automation systems: a survey. International Journal of Computer Networks & Communications, 6(4), 115.
[15] Palma, D., Agudo, J. E., Sánchez, H., & Macías, M. M. (2014). An Internet of Things example: Classrooms access control over near field communication. Sensors, 14(4), 6998-7012.
[16] Ratasuk, R., Mangalvedhe, N., & Ghosh, A. (2015, August). Overview of LTE enhancements for cellular IoT. In Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on (pp. 2293-2297). IEEE.
[17] Singh, B., & Kaur, B. (2016). Comparative study of internet of things infrastructures & security. Global Wireless Submit, 2016.
[18] Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovács, I. Z., Mogensen, P., & Sorensen, M. (2017, June). Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot.

In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia (pp. 4-7).
[19] Xu, K., Qu, Y., & Yang, K. (2016). A tutorial on the internet of things: from a heterogeneous network integration perspective. IEEE Network, 30(2), 102-108.