Review on Communication Protocols Internet of Things (IoT)

Anu Sharma
College of Computing Sciences and IT,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

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. 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: Communication, Internet of Things (IoT), Protocols, SigFox, ZigBee, Wireless systems.

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 [1]. The name of this new technology "Anything connectivity." It will connect anywhere and anything and anything there is a great range of IoT worlds intelligent computers, but with plenty of limitations. Care storage space volume, battery life and radio range short these restrictions are among them. Therefore, a communication protocol is required to implement IoT [2].

Manage these specifications effectively this article also discusses and contrasts IoT contact protocol that is applied as a straightforward insight vision of numerous IoT contact protocol readers, its pros and cons, pace and range of control consumption [3]. This article is an effort to examine various IoT correspondence protocols. Furthermore, it compares protocols widely used for IoT communication with highlighting the key traits and conducts in different steps protection of the spread of data and other energy use functionality. The purpose of this analogy is to present recommendations for the researchers should pick the required protocol applications.

DISCUSSION

1. IoT Communication Protocols:

This section provides a brief overview of each of them protocol to interact. Communication, normally IoT protocols can be defined as: (1) LPWAN and (2) network Short Scope

2. Low Power Wide Area Network (LPWAN):

A low-power wide-area network or low-power wide-area network or low-power network is a type of wireless telecommunication wide area network designed to allow long-range communications at a low bit rate among things, such as sensors operated on a battery.

A. SigFox:

SigFox is an inefficient wireless technology contact of a number of items of low energy as M2M software and sensors. It permits transport limited volumes of data up to 50 kilometers. FoxSig uses technologies for Ultra Narrow Band (UNB). This technique only low data transmission rates of 10-1 are handled. The tiny battery will run on a 000 bits per second. NFC Network in smart metres, patient monitors, technology is used on farms, protective facilities, street lighting and environmental conservation sensors. Start network topology support for SigFox [4].

B. Cellular:

Cell technology is great for technologies that need to be applied to high output data and IoT power supply application involving long distance service. It is likely to provide broadband connectivity with GSM/3G/4G it will provide secure high-speed connectivity however, the internet needs a high energy consumption. Therefore, M2M or local network is not appropriate communication. Mobile protocol is used as well particularly for applications containing multiple applications mobile machinery. The topology of cells relies on different bases technique [5].

3. Short Range Network:

Although there is no detailed classification for short-range wireless communication, it generally refers to communication distances on the level of WPAN and WLAN. Recently, there has been a shift to wide range wireless communications such as FAN (Field Area Network) utilizing multi-hop technology

A. 6LoWPAN:

6loWPAN is the first standard and most widely used IoT protocol for connectivity and it's an IP-based protocol of Internetworking. It can be directly connected to another intermediate entity-free IP network gateways or proxies for translation. It was this normal that the Internet Task Force (IETF) was created, a IEEE802.15.4 low power wireless network using IPv6 basic Internet Protocol (IP) communication. It endorses the number of addresses is more than 2128 IP addresses enough this helps to support multiple durations addresses [6]. The bandwidth is also low in cost, low consumption. 6loWPAN supports various topology types including topology mesh and star. 6loWPAN presents a transition layer between layer MAC and layer network (IPv6) to work with IEEE 802.15.4 and interoperability IPv6. IPv6. 6LoWPAN is the most affordable choice. They both do the same thing physical layer IEEE protocol 802.15.4.

B. ZigBee:

ZigBee Protocol ZigBee Alliance was established based on IEEE802.15.4 networks of low power wireless norm. - standard. ZigBee is a practise for high-level suites of low cost protocols for personal area formation, low power digital radios, small-sized networks for longer distances transfer data [7]. That will be concurrently for apps with a low data rate, longer battery Life, and secure computers for networking. ZigBee can also In addition help various topology styles such as mesh, star, and tree topology Network.

C. Bluetooth Low Energy (BLE):

BLE is also regarded as an intelligent Bluetooth Essential IoT programme protocol. It is planned and designed to be improved for fast, low bandwidth and low latency IoT applications. IoT applications. BLE classic Bluetooth advantages include reduced power usage, less installation time and support the topology of the star network with infinite amount of Nuclei [8].

D. Radio Frequency Identification *(RFID):*

RFID has several different standards (ISO, IEC, etc.). The DASH7 Partnership and the EPC-global ASTM International. RFID structures composed of a reader interface, and a tiny transponder for the radio frequency called RF tag. Tag is coded electronically with specific details and has a characteristic reading distance. RFID tag systems technologies: the first is known as active reader and other tags are called passive reader tags systems. Active tags are costlier, battery driven and using higher frequencies when using lower passive tags frequencies without an existing source of fuel. Due to the static RFID knowledge and programming required. Can't be used for weighing or explicitly in the tag some IoT programmers use RFID to provide diagnostic details. Intelligent shopping, fitness, national security and farming RFID supports the topology of the P2P network [9].

E. Near-Field-Communication (*NFC*):

NFC is a wireless contact of very short range technology for transmitting data between devices, touching them or no longer putting them together Just a couple of inches. NFC uses similar concepts in technology RFID, for starters. It is used not only to describe but also to connect more elaborately in two ways. NFC is marked and may contain little data. You should read this tag Just (similar to or may be able to distinguish RFID tags) be rewritable and later updated by the computer. NFC three major modes of operation: card emulation mode mode reader/writer (active mode) and mode peer-to peer (passive mode). NFC is commonly used for smartphone applications. Phones, industrial and contactless payment applications systems. Likewise, NFC makes communicating simpler, IoT systems in various commissions and power home, factory and work worlds. Support for NFC topology of the P2P network [10].

F. Z-Wave:

Z-Wave is generated by a low energy MAC protocol that connects 30-50 with wireless home automation nodes and IoT connectivity has been used, in particular for intelligent homes and small business realms. This is what we are talking about. Technology is optimized for very limited data packets speeds of 30 metres per point up to 100 kbps contact. It is therefore sufficient for small messages IoT uses, such as light monitoring, energy conservation, healthcare checking two unit types (controlling) depend on Z-Wave and slave. The low-cost machines cannot be used for slave nodes to have messages started. It can only respond and perform commands and send out messages inside the control devices network.

Communization between Communication Protocols in IoT:

This segment intends to give a rule to research to select the correct correspondence convention by giving an examination between the previously mentioned correspondence conventions. Various rules are utilized to benchmark the contrasts between the correspondence conventions. Such measures incorporate norm, organization, geography, power, range, cryptography, spreading, tweak type, coexistence in terms of security, all the nine correspondence conventions have the encryption and validation components. 6LoWPAN, ZigBee, BLE, NFC, Z-Wave utilize the High level encryption Standard block figure with counter mode, while Cell and RFID use RC4. Nonetheless, a few genuine shortcomings were distinguished. AES is incredibly secure while RC4 isn't. RC4 is quick contrasted with AES. As far as force utilization, 6LoWPAN, ZigBee, BLE, ZWave and NFC are intended for convenient gadgets and restricted battery power.

Consequently, it offers low force utilization. On the other hand, Cell high force utilization is in the rundown. In term of information rate, 6LoWPAN, ZigBee, BLE, NFC, SigFox furthermore, Z-Wave have information rate < = 1 Mbps. Nonetheless, RFID has the most noteworthy information pace of 4 Mbps in terms of reach, SigFox and Cell range longer than the inclusion of a few KM. In any case, 6LoWPAN, ZigBee, BLE, NFC, Z-Wave, and RFID are range more limited that cover not as much as KM. As indicated by the examination of correspondence convention in IoT, 6LoWPAN will be the future convention since it is IP based WSN. It permits an immense number of keen gadgets to be conveyed over the web effectively by utilizing the immense location space of IPv6 for information and data assembling through highlights and practices of different measurements, including low data transmission, various geographies, and star or lattice, power utilization, ease, versatile organizations.

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] B. L. Risteska Stojkoska and K. V. Trivodaliev, “A review of Internet of Things for smart home: Challenges and solutions,” *Journal of Cleaner Production*. 2017, doi: 10.1016/j.jclepro.2016.10.006.

[2] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2017.11.022.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet Things J.*, 2014, doi: 10.1109/JIOT.2014.2306328.

[4] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” *Ad Hoc Networks*, 2015, doi: 10.1016/j.adhoc.2015.01.006.

[5] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols: Review,” 2017, doi: 10.1109/ICITECH.2017.8079928.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2444095.

[7] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” 2012, doi: 10.1109/ICCSEE.2012.373.

[8] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, “Middleware for internet of things: A survey,” *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2498900.

[9] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, 2015, doi: 10.5120/19787-1571.

[10] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: A standardization perspective," *IEEE Internet Things J.*, 2014, doi: 10.1109/JIOT.2014.2323395.