RESEARCH ARTICLE | JUNE 15 2023

Comparison of session layer communication protocols in IOT - A review

Navpreet Kaur ✉; Inderdeep Kaur Aulakh; Raman Chadha

AIP Conf. Proc. 2782, 020104 (2023)
https://doi.org/10.1063/5.0155197

Comparison of Session Layer Communication Protocols in IOT - A Review

Navpreet Kaur[1, 2, a)], Inderdeep Kaur Aulakh[1, b)], Raman Chadha[2, c)]

[1]*I.T. Department, UIET, Chandigarh, India*
[2]*Department of Computer Science & Engineering, Chandigarh University, Gharuan, Chandigarh, Punjab, India*

[a)] *Corresponding author:* [a)] *nvprtkr7@gmail.com, navpreet.e9024@cumail.in*
[b)] *ikaulakh.pu@gmail.com, ikaulakh@pu.ac.in*
[c)] *dr.ramanchadha@gmail.com*

Abstract. Internet of Things (IoT) is one of the emerging technologies. It can be defined as wireless connection among multiple devices. The IoT can be classified in two different classes i.e. Inner layout of IoT and Outer Layout of IoT. The inner layout covers the concepts such as communication protocols etc and outer layout of IoT covers the devices like actuators, sensors etc. The communication protocols in IoT is implemented on different layers of OSI (Open System Interconnection) model. This study highlights the session layer based IoT communication protocols such as MQTT, AMQP, CoAP and LoRaWAN.

Keywords. Internet of Things, Smart Devices, Sensors, Communication Protocols, MQTT, AMQP, CoAP, LoRaWAN.

INTRODUCTION

Now days, the IoT has become most advanced and prominent technology of communication. The IoT allows the machine to machine, machine to device, machine to human and vice versa communication without any intervention of human, all it need is just a connection of internet to transmit data among the connected devices [1]. It is a platform where multiple heterogeneous devices are interconnected to each other and forms a single network platform that is named as Internet of Things (IoT) [2]. IoT has been assured a deep impact on human life in the form of various facilities like smart homes which allows the users to control or manage the home appliances remotely and automatically [3]. The IoT technology comes to the existence many years ago but was avoided due to its high maintenance cost, high energy consumption etc [4]. Such issues have been acted as arguments among its critics. Although the advancements in the internet technology enables anyone to deploy their own IoT based smart home. The devices used in IoT communicate to each other by using a sort of communication rules in the form of protocols. The communication protocols for IoT are specific [5].

Further this study is organized to give a brief introduction to the communication protocols in Section 2. The Section 3 explains the types of IoT communication protocols such as MQTT, CoAP, LoRaWAN and AMQP along with their pros and cons. The Section 4 delineates the comparison of defined communication protocols. The work that has been done in this domain by various research scholars in listed in Section 5. The Section 6 concluded the driven survey briefly.

COMMUNICATION PROTOCOLS

Communication protocols are kind of metaphors for designs and rules of a digital message. The role of communication protocol in a communication process is to empower the users to share the message among connected devices [6,7]. The communication protocols are mandatory in telecommunication. The concept of communication protocols swath a variety of applications such as user authentication, message signaling and error detection and correction. Communication protocols are mandatory in every kind communication technology such as wireless, fidelity, Long Term Evaluation (LTE), IoT etc [8].

Recent Advances in Sciences, Engineering, Information Technology & Management
AIP Conf. Proc. 2782, 020104-1–020104-6; https://doi.org/10.1063/5.0155197
Published by AIP Publishing. 978-0-7354-4539-0/$30.00

The communication protocol for IoT is one of the hottest topic for research work in industries as well as academics nowadays. The hasty progress in communication technologies such as machine to machine, micro computing etc has results to the development of IoT communication. IoT is not a single technology in itself as it can be defined as a bundle of multiple technologies such as sensors, actuators etc. The next section defines the types of communication protocols that are used in IoT [9].

TYPES OF PROTOCOLS

MQTT

It is a "Machine to Machine" lightweight communication protocol. It supports data transmission to multiple nodes. MQTT is developed by IBM, but it becomes an open standard protocol. It utilizes the TCP protocol to develop a connection among clients. The use of TCP protocol makes it more reliable and connection-oriented communication protocol. MQTT suffers from minimum overhead and traffic during data transmission. The minimum overhead is achieved in MQTT as it follows publish-subscribe model. The foremost feature of MQTT is that all the sensor nodes are kind of information independent nodes [10]. In MQTT, the respective information is required for both sensor node and subscribe node. Every connected device is allowed to send the data and have permission to ask for information of other nodes. This information sharing is feasible because a centralized server is used to which all the nodes are connected. Thus, it reduces the overhead and conversely enhances the TCP requests. Another feature of MQTT is Time decoupling. In MQTT some nodes are in sleep mode and some are in active mode. The nodes which are not in operation mode fall under the category of sleep node and thus reduce the energy consumption. Thus the data transmission is done when the nodes wake up from sleep mode [11, 12]. Therefore, the publisher and subscriber are not required to run at the same interval.

Advantages

- It supports the three levels of Quality of Service (QoS).
- If any client gets disconnected then he can register himself by simply generating a message by the broker. This is known as Last Will and Testament.
- The message sending over a limited bandwidth is simple and straightforward due to a TCP connection.
- The authorization is only given to the users who have user name and password. Thus, it maintains the authenticity and confidentiality.

Disadvantages

- It is mandatory for each and every client node to have compatibility with TCP protocol and should keep the connection always open. This can lead to an issue in a case where the packet loss is higher than the computing resources [13].
- To keep the connection always open and restricts the sleep time for a device which can directly lead to the high energy consumption and sometimes the MQTT protocol need to be replaced with MQTT-SN which supports the USP protocol instead of TCP.
- It did not support the 802.15.4 as too long strings are required for naming a topic.

CONSTRAINED APPLICATION PROTOCOL (CoAP)

This is one of the most popular IoT communication protocol that supports peer to peer response, request structure and works as per IETF standard [14]. It is applied to User Datagram Protocol and hence supports the connectionless networks. It depends upon the redundant way of communication connections instead of standard connections. The CoAP also empowers communication for multi node and from single node to multi node as well. The use of IPv6 protocol makes the CoAP to support such a variety of communications as IPv6 supports multi node transfer by default. It also supports the asynchronous data transmission. CoAP utilizes the Uniform Resource

Identifier to employ a standard communication interface corresponding to the available number of nodes in the network [15]. Following are advantages and disadvantages of CoAP protocol:

Advantages

- The packet size in CoAP is smaller, thus it takes less time to generate the packets and also consumes less memory space for storage purpose.
- It uses the UDP protocol which makes it capable to use in packet based technologies such as Short Messaging Service.
- The request and response strategy of messages is a major advantage of CoAP. As in this strategy, the messages are labeled by using two labels i.e. confirmable and non-confirmable. These tags indicate that the confirmable messages need to acknowledge whereas the non-confirmable messages are not required to acknowledge.

Disadvantages

- The use of UDP limits the CoAP to provide security to the data. Whereas it uses the Data Transport Layer Security (DTLS) to provide security but only for UDDP data transmission. It did not assure the security of data over other data transmission protocols.
- The CoAP is peer-to-peer protocol which is another lacking point of it. Although the enhancements which create a group for broadcast are possible [13], but the capabilities are inherited from the protocol. Thus it makes it little difficult
- It did not provide any CACHE control option to retain the integrity and confidentiality of data.
- It is highly prone to data threats like attacks and spoofing.

AMQP

Advanced Message Queuing Protocol supports the message oriented middleware [16]. The AMQP is an open standard application. Following are the defined features of AMQP:

1. Message oriented Queuing
2. Routing
3. Reliability
4. High security
5. Modeled to support finance industry
6. Runs over TCP protocol and follows the publish and subscribe topology

The working criteria of AMQP are similar to the SMTP, HTTP and FTP etc [17]. It authorizes the nature of client and message publisher in order to enhance it to the various vendors which are capable to exchange and use the information.

LoRaWAN

It is used to arrange the communication between LPWAN gateway and end-to-end devices at media access control layer. It is managed by LoRa Alliances. LoRaWAN and LoRa, both are different from each other [18, 19]. The LoRaWAN is notated as communication protocol and system layout for network whereas the LoRaWAN physical layer sanctioned the long-range data transmission.

The major role of LoRaWAN is to manage the data rate, bandwidth frequencies and energy level of all connected devices. The features of LoRaWAN are as follows:

- It is specifically modeled for Low-Power Wireless Area Network at the cost of low power, high mobility and cheap cost.

- It offers bi-directional communication to IoT applications.

COMPARISON OF PROTOCOLS

This section draws a comparison study among the protocols that are defined in previous section [20]. The comparison is derived on the basis of the various parameters. The table 1 represents the comparison between MQTT and AMQP whereas the table 2 delineates the difference between CoAP and LoRaWAN.

TABLE 1. Comparison of MQTT and AMQP [21]

Parameter	MQTT	AMQP
Origin	Vendor driven	Customer driven
Intended Use of Protocol	Suitable to small devices to send small messages	Support full vibrancy of messages
Optimization of Framing	Use Stream Oriented Approach	Use Buffer Oriented Approach
Messaging Scenario	Support, Publish and Subscribe message	Support all type of messages
Connection Security	Does not support	Specifically worked to indicate TLS and SASL
User Security	Need Short name and passwords	Need SASL mechanism allowing organization to choose security
Message Matter	It is Opaque	It is not Opaque
Last Value Queue	With its RETAIN command, able to support last value queues	---

TABLE 2. Comparison of CoAP and LoRaWAN [22]

Parameter	CoAP	LoRaWAN
Intended Use	Designed to use constrained nodes and network	Designed to use for secure bi-directional communication.
Associated Layer	Service Layer	Media Access Control Layer
Transaction Messages	Request and Response	MAC message type depends on purpose like join request, join, accept etc.
Bandwidth	Less than LoRaWAN	More than CoAP
Data Rates	----	0.3kbps-50kbps
Message Transmission	Asynchronous	Synchronous
Applications	Smart grid and Building Automation	IoT and Smart Sensor Application

RELATED WORK

Tianyi Song et al. [8], defined that the advancements in the recent technology leads to the enhancements in both academic and industrial domains. The smart home device is the major example and application of internet of things and is manufactured by a large number of companies now a day. Though, the features of the smart devices certainly

enhance the security and privacy. This work was organized to develop a improved energy efficient secure communication protocol for smart home device. For providing security the key based symmetric encryption technique was employed in this work. The key generation was done by using chaotic system. In order to assure the data integrity and security the message authentication code was integrated with the proposed technique. The performance of the proposed technique was evaluated in terms of cost incurred for memory, system complexity and communication overhead.

Valentin Stangaciu et al. [9], designed a novel communication structure to collaborate the two most prominent technologies i.e. wireless sensor network and IoT. The major concern of the work was to provide connection among smart devices and central devices by using an efficient communication protocol. For the purpose of performance evaluation, the proposed work was tested and observed that it was capable enough to integrate both technologies on the cost of smallest embedded system with respect to cost and storage.

Gary Steri et al. [11], represented the significance of communication protocol and connectivity of devices in IoT. The author betokened that in IoT the flexible communication protocols for machine to machine communication are mandatory and device to device property of 4G devices act as a prominent solution to this requirement. The author developed this study with an aim to collaborate the IoT and WSN by introducing a D2D communication protocol. The proposed protocol makes the connected user devices to act as a hub. This was done to upload the data packets on Web through available mobile network. The proposed protocol was designed for establishing the secure D2D multi hop communication. The protocol fulfills the communication need of connected user devices. A proper connection and security analysis was done with respect to the interruption generated during set up phase of network.

Riccardo Bonetto et al. [14], discussed the security for user devices of IoT. This study discussed the security architecture along with its working, interaction among the connected devices and advantages or disadvantages of most prominent security mechanisms with respect to the layers of OSI model. An example for creating the peer to peer secure transmission from constrained devices to unconstrained devices in the network. The proposed technique implemented the encryption for securing the data without performing any heavy or tricky computations.

Zhiyan Liu et al. [15], defined that the rapid enhancements in IoT technology attracts a lot of research scholars to develop or introduce some enhancements in this domain to make it more effective and efficient. As IoT is a novel technology thus it suffers from many issues which need to be resolve. The major issues like communication protocols, used technology standards were highlighted. The author also explains the universal communication process in IoT which included the UID registration, cancellation procedure, user ID searching process etc. The data status and timeliness was considered for employing the relative parameters for unified communication protocol.

CONCLUSION

This paper organizes a detail study on IoT and its communication protocols. The major objective behind conducting this review is to have an insight view to the most prominent IoT communication protocols. The comparison of communication protocol is also presented in this organization. Along with this the pros and cons of each communication protocol is also given. On the basis of provided information it can be concluded that the IoT is quite innovative communication technology. This study can be helpful to the research scholars who are beginners and intend to perform some innovations in this domain. In future more amendments can be done to improve the quality of communication by utilizing the advanced communication protocols.

REFERENCES

1. Jelena Mišić ; M. Zulfiker Ali ; Vojislav B. Mišić, “Architecture for IoT Domain With CoAP Observe Feature”, IEEE, Vol 5, Issue 2, Pp. 1196 – 1205, 2018
2. Ravi Kishore Kodali , Borade Samar Sarjerao, “MQTT based air quality monitoring”, IEEE, 2017
3. Goiuri Peralta , Markel Iglesias-Urkia , Marc Barcelo , Raul Gomez , Adrian Moran , Josu Bilbao, “Fog computing based efficient IoT scheme for the Industry 4.0”, IEEE, 2017

4. Shailaja M. Gunda Nikkam , V. R. Pawar, “Water parameter analysis for industrial application using IoT”, IEEE, 2016
5. Satyavrat Wagle, “Semantic data extraction over MQTT for IoTcentric wireless sensor networks”, IEEE, 2016, M. Rachana , B. Abhilash , P. Meghana , Vijay Mishra , S. B. Rudraswamy, “Design and deployment of sensor system — envirobat 2.1, an urban air quality monitoring system”, IEEE, 2017
6. Dong-Kyu Choi , Joong-Hwa Jung , Seok-Joo Koh, “Enhanced cluster-based CoAP in Internet-of-Things networks”, IEEE, 2018
7. Balu L. Parne ; Shubham Gupta ; Narendra S. Chaudhari, “SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network”, IEEE, Vol 6, Pp 3668 – 3684, 2018
8. Tianyi Song , Ruinian Li , Bo Mei , Jiguo Yu , Xiaoshuang Xing , Xiuzhen Cheng, “A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes”, IEEE, 2016
9. Valentin Stangaciu , Madalina Stanciu , Loredana Lupu , Mihai V. Micea , Vladimir Cretu, “Application layer protocol for IoT using wireless sensor networks communication protocols”, IEEE, 2018