ISSN 2581 – 3781

AJCSE ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info

Asian Journal of Computer Science Engineering 2019;4(4):1-7

REVIEW ARTICLE

Study on Messaging Protocol Message Queue Telemetry Transport for the Internet of Things

Roaa Wadullah Tareq, Turkan Ahmed Khleel

Department of Computer Engineering, University of Mosul, Mosul, Iraq

Received on: 20-10-2020; Revised on: 25-11-2020; Accepted on: 10-12-2020

ABSTRACT

With the proliferation of the number of Internet of things (IoT) devices, the volume and speed of data are increasing rapidly. IoT systems mainly depend on the use of messaging protocols to exchange data. Because IoT devices often contain limited computational resources and processing power, a lightweight, reliable, scalable, interoperable, scalable, and secure messaging protocol must be chosen. Data within IoT systems indicate interoperability. Given that, IoT systems help facilitate this bonding between heterogeneous components. Messaging protocols will play an important role in propagating and developing IoT systems. In this paper, we present a review of the Message Queue Telemetry Transport protocol for its importance in the present day of IoT systems about the structure and method of communication using it. We highlight the pros, strengths, and cons. Furthermore, mention the important survey researches in this field.

Key words: Internet of things, message queue telemetry transport protocol, publish/subscribe, broker

INTRODUCTION

In our modern era, Internet of Things (IoT) systems have become important and have an effective impact in the various areas of life, whether in the health,[1] industrial, and agricultural fields, as well as smart cities and many other areas. The IoT is the linking of physical parts to the virtual world to obtain data by connecting these parts, it is a platform that allows the user to read and monitor data, all of this happens electronically.[2]

The ability of these systems to develop is great, but, on the other hand, many challenges meet, the most important of which is that their components are not homogeneous (heterogeneous systems).[3] In addition to availability, performance, reliability, interoperability, scalability, security, trust, mobility, and management all of these need to be solved.[4]

As well as what has been mentioned, the issue of data security is considered the most important for maintaining privacy as well as protection from threats that may be exposed to these systems.[5] The growth and development of IoT application areas rely heavily on many major factors, like:[6] General developments available in electronic parts, User-friendly environments and Software solutions available, Applications related to sensor, and data collection technologies, Network efficiency, that is, network and infrastructure accessibility and adequate supply of energy for IoT production and service appliances. An important aspect of the IoT is the application layer protocols responsible for transmitting data, the transmission of IoT sensor data requires a lightweight protocol and shows bandwidth efficiency. In addition, it must be energy efficient and able to operate with bounded hardware resources (such as, power supply and main memory).[7] In IoT, transmission of messages or data between various devices is important because an IoT system needs to deliver an instructions for an extra system management unit.[8] One of the most important protocols used in this field:[9]

Message queue telemetry transport (MQTT): This protocol conceived for resource-constrained appliances.[10] MQTT is one of the Machine-to-Machine (M2M) communication protocols based on IoT devices,[11] which was founded in 1999.[12] Arlen Nipper of Arcom Control Systems

Address for correspondence:
Turkan Ahmed Khleel,
E-mail: turkan@uomosul.edu.iq

and Andy Stanford-Clark of IBM developed it. A new protocol for linking oil pipelines over satellite networks had to be developed.[13] It has become an Organization for the Advancement of Structured Information Standards standard.[14] In the application layer above the TCP/IP stack, MQTT resides.[15] Figure 1 shows the MQTT Top on TCP/IP. To ensure safety and privacy, the connection of TCP can be encrypted with Transport Layer Security/Secure Sockets Layer (TLS/SSL).[16] MQTT features various security mechanisms, however, most of them are not provided or not configured by default such as entity authentication or data encryption.[17]

MQTT is used as the publish/subscribe model that makes it suitable for M2M messaging.[18] An MQTT Client publishes messages or data to an MQTT Broker which other Clients subscribe to or may be reserved for a future subscription.[19] Each message is published using an address called Topic. Clients can subscribe to multiple Topics. Figure 2 shows a comparison of the protocols used worldwide. In this study, we will focus on the MQTT Protocol. The protocol structure that consists of a publisher client, a subscriber client, and a broker will be reviewed. Also what protocol message format it consists of? In addition, to knowing the benefits of this protocol and the difficulties and challenges it faces.

COMMUNICATION ARCHITECTURE OF MQTT

The architecture of MQTT contains three parts. Those are a subscriber, a publisher, and a broker. The Publisher or Subscriber Client can be any device. The device which is interested in certain topic records on it called Subscriber Client.On the other hand, the device which publish data at the same Topic that subscriber interested it to the Broker is called the publisher client. Authorization of the publisher and the subscriber are examined by the broker to know the related security issues.[4] Figure 3 shows the Architecture of MQTT. We describe the parts as follow:

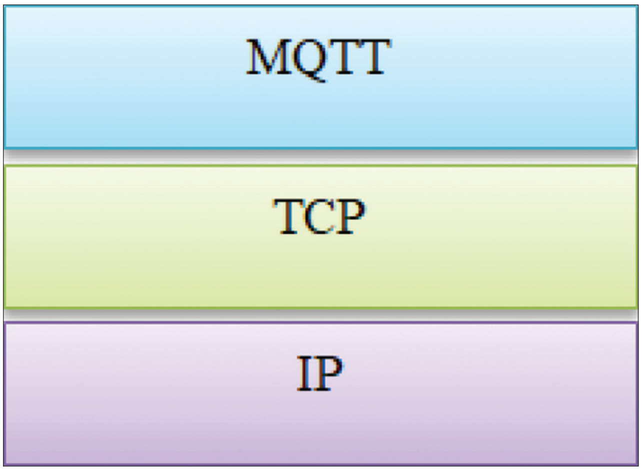


Figure 1: Message queue telemetry transport on top of the TCP/IP

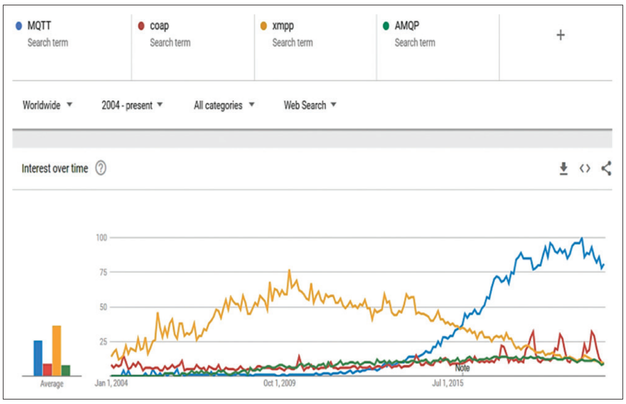


Figure 2: Worldwide compare between protocols from 2004~ to present[20]

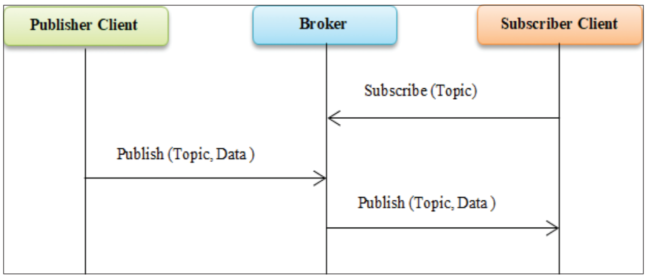


Figure 3: Architecture of message queue telemetry transport protocol

Client (Publisher/Subscriber)

The client for the publisher of MQTT protocol in the IoT is in most cases sensors, and depending on the type of application designed, it may be a sensor for measuring temperature and humidity, or it may be a sensor for a health system to measure heart rate and other applications.

Through this client, the data are published to the broker through a specific topic to be obtained by the subscriber client, who can be more than one subscriber through the same topic on which the data were published. The type of MQTT client relies on its function in the application of IoT whether it is a publisher or a subscriber.[21]

Topic

IoT sensor data are published in a specific address called topic to broker to be subscribed by the subscriber on the same topic to obtain the data that have been published.

Broker

It is a central device and part of the cloud for the IoT system that receives data from the sensor (publisher client) and in turn sends the data to the subscriber. It may be more than one subscriber client according to the designed system. The major broker's responsibilities are processing the communications among MQTT clients and distributing the data among them based on their topics.[22] The default port of MQTT that is used is TCP/IP port 1883. MQTT has various types such as Mosquito, Paho MQTT, and Hive MQ.[23] There are many MQTT brokers open source as follows in Table 1.

MQTT MESSAGE ANALYSIS

The MQTT message format consists of, a payload (Optional), a variable header (Optional) with a fixed header. The fixed header exists in all types of MQTT messages, but the variable header with payload exists in some of the MQTT message types.[24] Table 1 show the fixed header of the MQTT protocol. In Fixed Header contain 2 Bytes, First Byte contains 4 bit for message type (there are 14 types of MQTT control messages) and 4 bits for flags. 14 types of MQTT control messages are shown in Table 2:

The Duplicate (DUP) flag bit is set to 0, which means that this is the 1st time this MQTT PUBLISH Packet has been attempted to be transmitted by the Server or Client. However, if the DUP flag bit is set to 1, this means that an earlier attempt to send the packet could be re-delivered.

The field of quality of service (QoS) contains 2 bits that indicate the level of confirmation for transmission of a Message. RETAIN field this bit determines whether to keep the message when published. At Second Byte start The Remaining Length is the number of bytes remaining within the current packet, including the data that exist in payload and variable header. Figure 4 shows a control message of the MQTT protocol.

Table 1: MQTT brokers open source

Broker	Built on	Operating system	QoS
Mosquitto	C language	Linux, Mac OS, Windows, and BSD	Support QoS_0, QoS_1, QoS_2
Hive MQ	Java	Linux, Windows, and OS X	Support QoS_1, QoS_2
Active MQ	Java	Linux, Unix, and Windows	Support QoS_0, QoS_1, QoS_2
Mosca	Java Script	Linux, Mac OS, and Windows	Support QoS_0, QoS_1
EMQ X	Erlang/ OTP	Linux, Mac OS, windows and BSD	Support QoS_0, QoS_1, QoS_2
Verne MQ	Erlang/ OTP	Linux, Mac OS	Support QoS_0, QoS_1, QoS_2
Rabbit MQ	Erlang	Linux, Mac OS, Unix, Windows and BSD	Support QoS_0, QoS_1

MQTT: Message queue telemetry transport

Table 2: Types of MQTT control messages

Value	Name	Description
0	RESERVED	RESERVED
1	CONNECT	Client demand Connect to Server
2	CONNACK	Connection Acknowledgment
3	PUBLISH	Publish Message
4	PUBACK	Publish Acknowledgment
5	PUBREC	Publish Received
6	PUBREL	Publish Release
7	PUBCOMP	Publish Complete
8	SUBSCRIBE	Client subscribe request
9	SUBACK	Subscribe Acknowledgment
10	UNSUBSCRIBE	Unsubscribe Request
11	UNSUBACK	Unsubscribe Acknowledgment
12	PINGREQ	PING Request
13	PINGRESP	PING Response
14	DISCONNECT	Client is Disconnecting
15	RESERVED	RESERVED

MQTT: Message queue telemetry transport

MQTT QOS LEVEL

There are three levels for various scenarios[21] that MQTT provides as follow:

QoS_0

At this level, the message is delivered 1 time at most, and confirmation (Acknowledgment) of receipt is not required. This level is the simplest. The transmission of the message may be a successor may be lost.

QoS_1

Each message in this level is delivered 1 time at least and it is required to confirm (Acknowledgment) receipt of the message. When receiving the message, the recipient must return an acceptance (ACK packet), and when the message sender will not receive the reply (ACK packet) within a certain time and will send the current message again even the other party receives a confirmation.

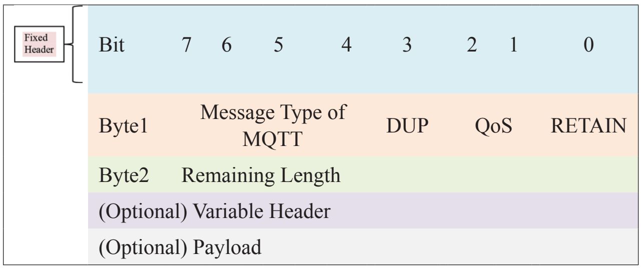
QoS$_2$

Exactly once transmission, four data packets are exchanged between the sender and the recipient to confirm the sending of the message, as it is appropriate in cases of message loss or case duplication of transmission is not allowed.

To summarize, the properties and characteristics of the MQTT protocol are shown in Table 3.

ADVANTAGE OF MQTT PROTOCOL

Many IoT applications in different fields utilize MQTT. For instance, it is being utilized in Facebook notifications, health-care surveillance, the agricultural field, smart homes, and other many applications.[25] Therefore, MQTT is considered the ideal messaging protocol for the M2M communication and in the IoT. The cause behind this is because of its ability to provide low-power routing,[26] small, low memory, lightweight, and inexpensive device is installed in weak networks and low bandwidth. The characteristics of this protocol can be summarized, as shown in Table. The most important benefits that distinguish it as follow:[27]



Bit	7	6	5	4	3	2	1	0
Byte1	Message Type of MQTT				DUP	QoS		RETAIN
Byte2	Remaining Length							
(Optional) Variable Header								
(Optional) Payload								

Figure 4: Control message of message queue telemetry transport protocol

Table 3: Summery of MQTT

MQTT	Characteristics
Format of Encoding	Binary
Model	Publish/Subscribe
Transport Layer	TCP
Security	TLS/SSL
QoS Levels	QoS0, QoS1, QoS3
Size of Packet	Very Small
Primary Target	Lightweight for M2M
Port	(8883) TLS/SSL connection (1883) Non-TLS connection
Size of Packet Header	2 Bytes
Type of Communication	Asynchronous

MQTT: Message queue telemetry transport

1. MQTT Protocol utilizes a publish/subscribe model which has a low overhead that makes the protocol is a lightweight.[28]
2. MQTT reduces the bandwidth of the network.
3. MQTT utilize a broker to deliver the messages among client's authentication may be implemented on the broker that gives security to the messages.
4. Unreliable networks can be handle by utilizing various levels of QoS This is an advantage of this protocol beneficial with that type of networks for various types of data.
5. The multicasting of messaging also can be compatible with MQTT.
6. MQTT is used SSL to encrypt data.[29]
7. MQTT provides less battery power consumption for systems and this makes it suitable for the IoT systems.

DISADVANTAGES OR DRAWBACKS OF MQTT PROTOCOL

1. MQTT utilizes TCP protocol which needs more memory and more processing power. Whereas, devices connected through the TCP protocol tend to keep the sockets open to each other, which leads to increased power/memory requirements.
2. The clients of MQTT must support TCP/IP.
3. MQTT is non-TLS/SSL communication (unencrypted) by default. Instead, MQTT utilizes TLS/SSL communication (encrypted) for security.
4. Another cons part of MQTT does not have interoperability. Because payload is binary, with no existing information on how to encode it, the drawbacks can arise, particularly in open architecture where various applications from various manufacturers are assumed it is worked seamlessly for each other.
5. MQTT protocol does not support the priority feature of sending data (messages). For example, if the system has data from several sensors, there must be a priority for some data in the transmission, for example, fire alarm data have priority from temperature or pressure data.

RELATED WORK

The most important works related to protocol coverage that is currently widely used on the internet are presented in terms of structure and QoS as well as the security aspect of data transmission in addition to the most important intermediaries used. The following Table 4 shows the most important research:

These researches are important for a good knowledge of the MQTT protocol and a beginning to delve into this area but research "The Use of MQTT in M2M and IoT Systems: A Survey[34]" One of the best researches that clarify MQTT protocol and gives a comprehensive overview of the MQTTinM2M/IoT. We analyzed and the MQTT protocol is characterized by simplicity, as it is open-source intermediaries that make it suitable for systems with limited resources such as the IoT, which are characterized by computational capacity and low energy consumption, as well as bandwidth and memory.

Other studies are compared and survey MQTT with other protocols in the application layer, such as HTTP, CoAP, XMPP, and others. Table 5 shows paper survey of MQTT with other protocols.

The most important things that can be analyzed and concluded from the research area in the above table:

1. The MQTT protocol has proven to be more efficient in battery-powered devices and this is what makes it suitable in the IoT systems. If the final applications need massive updates, the protocols of the publish/subscribe model are more appropriate like MQTT.

Table 4: Paper survey of MQTT

Paper name	Year	Topics
Internet of things: Survey and open issues of MQTT Protocol[25]	2017	This paper introduces the most common MQTT protocol, which is a lightweight protocol that works as a Binary pipe for data delivery in addition to its architecture and Quality of Service (QoS)
A Survey On MQTT: A Protocol Of Internet of Things (IoT)[30]	2017	In this paper, the importance and evolution of MQTT protocol in the Internet of things and described as well as the general architecture of the protocol
A Comparative Analysis of Security of MQTT Brokers[31]	2019	In this paper, the different brokers available online are analyzed from Side of the security outlook by implementing a DoS attack techniques for gathering information on a mediator, the results are compared and trying to find out the mediator is the least vulnerable To be used for secure communication in IoT devices
Security, Privacy and Forensic Concern of MQTT Protocol[32]	2019	In this paper, an overview is given of the privacy and security concerns of the Internet of Things through the MQTT protocol, as well as some of the proposed improvements in MQTT deployment and security solutions
MQTT Protocol: Fundamentals, Tools and Future Directions[33]	2019	MQTT protocol is discussed and is also compared to other IoT application layer protocols, such as Constrained Application Protocol (CoAP)
The Use of MQTT in M2M and IoT Systems: A Survey[34]	2020	The advantages and limitations of the MQTT protocol are explained and it is the most widely used in M2M/IoT, The features of the most important brokers were also presented, with which to start execution. MQTT

MQTT: Message queue telemetry transport

Table 5: Paper survey of MQTT with other protocols

Paper Name	Year	Topics
A Survey on Application Layer Protocols for the Internet of Things[35]	2015	The paper presents a comparison in the application layer of the Internet of Things for several protocols (MQTT, CoAP, and XMPP) in terms of energy consumption, reliability, and security aspects
Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP[13]	2017	The paper presents an assessment of the Internet of Things (IoT) protocols (MQTT, CoAP, AMQP, and HTTP) in terms of limitations and strengths
Communication Protocol Stack for Constrained IoT Systems[36]	2018	This paper provides an overview of IoT protocols (MQTT, CoAP, XMPP, and RESTFUL) and an analysis the efficacy and reliability of these protocols are based on energy efficiency, security, and lightweight nature of protocols
Performance Evaluation of Application Layer Protocols for the Internet-of-Things[37]	2018	This paper provides a comparison of the performance of several Internet of Things (IoT) protocols (MQTT, AMQP, and XMPP)
Internet of Things: A Survey on IoT Protocols[38]	2018	The major objective of this paper to review is to provide a critical review of IoT protocols (MQTT, AMQP, and CoAP), architecture, and standards
A Survey of Communication Protocols for the Internet of Things and Related Challenges of Fog and Cloud Computing Integration[39]	2019	In this paper survey on protocols in application layer (HTTP, CoAP, MQTT, XMPP, DDS, and AMQP) for IoT The possibility of implementing these protocols in the Internet of things systems based in cloud and fog
IoT Application Layer Protocols: A Survey[40]	2020	This paper provides a survey of several IoT application layer protocols such as (CoAP, MQTT, XMPP, DDS, REST, AMQP, JMS, and WebSocket)

2. To choose any protocol suitable for the system, the user must determine their pertinent purpose in IoT systems based on accordingly, their suitability and requirements.
3. The results present MQTT and CoAP as the empowering protocols of the application layer for battery-operated and mobile systems primarily.
4. The results show that the MQTT protocol is better than the AMQP protocol with relevance to message delivery rate and bandwidth usage. It also showed that all protocols have the same reliability that they do not utilize process own retransmission.
5. Currently, the standard is evolving, and there are challenges including short-term interoperability. When choosing the appropriate protocol, major factors must be taken into account, including the possibility of unifying the various interfaces and structures to achieve joint management of the IoT, the fog, and the cloud.

CONCLUSION AND FUTURE WORK

The MQTT protocol is intended for asynchronous communication, where publishing or subscriptions to various entities happen in parallel order. As we mentioned earlier, the MQTT protocol is can provide reliable delivery by choosing among three types of mechanism, called QoS. When we are compared MQTT with other protocols such as HTTP, the MQTT has quite smaller, this makes MQTT, much more appropriate for a resource-restricted environment like the IoT. By default, the broker does not provide security to messages authentication information and the messaging scheme is delivered in plaintext; thus, it needs security to protect the transported information. There are many factors for choosing the IoT protocol in the application layer, including the communication and computational capacity of the devices as well as memory and power consumption. As part of our future work, the implementation of the MQTT protocol for the IoT system, the use of sensors to spread the data of the system to an open-source medium, and the implementation of a common client to obtain the system data, and we will work to conduct some tests on it to highlight the advantages of this protocol in this field.

REFERENCES

1. Houimli M, Kahloul L, Benaoun S. Formal Specification, Verification and Evaluation of the MQTT Protocol in the Internet of Things. In: 2017 International Conference on Mathematics and Information Technology; 2017. p. 214-21.
2. Al-Fuqaha A, Khreishah A, Guizani M, Rayes A, Mohammadi M. Toward better Horizontal Integration among IoT Services. IEEE Communications Magazine; 2015. p. 72-9.
3. Kruger CP, Abu-Mahfouz AM, Hancke GP. Rapid Prototyping of a Wireless Sensor Network Gateway for the Internet of things Using off-the-shelf Components. In: 2015 IEEE International Conference on Industrial Technology; 2015. p. 1926-31.
4. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials; 2015. p. 2347-76.
5. Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures, and security issues: A comprehensive survey. Sensors 2018;18:2796.
6. Nižetić S, Šolić P, González DL, Patrono L. Internet of things (IoT): Opportunities, issues, and challenges towards a smart and sustainable future. J Cleaner Prod 2020;274:122877.
7. Thangavel D, Ma X, Valera A, Tan HX, Tan CK. Performance Evaluation of MQTT and CoAP via a Common Middleware. In: 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing; 2014. p. 1-6.
8. Kraijak S, Tuwanut P. A Survey on Internet of things Architecture, Protocols Possible Applications, Security, Privacy, Real-world Implementation and Future Trends. In: 2015 IEEE 16th International Conference on Communication Technology; 2015. p. 26-31.
9. Al-Masri E, Kalyanam KR, Batts J, Kim J, Singh S, Vo T, *et al*. Investigating Messaging Protocols for the Internet of Things (IoT). IEEE Access; 2020. p. 94880-911.
10. Prada MA, Reguera P, Alonso S, Morán A, Fuertes JJ, Domínguez M. Communication with Resource-constrained Devices through MQTT for Control Education. IFAC-PapersOnline; 2016. p. 150-5.
11. Biju S, Shekokar N. Security Approach on MQTT Based Smart Home. In: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering; 2017. p. 1106-14.
12. Sugumar K. MQTT-A Lightweight Communication Protocol Relative Study. Authorea Preprints; 2020. p. 1-5.
13. Naik N. Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP. In: 2017 IEEE International Systems Engineering Symposium; 2017. p. 1-7.
14. Standard O. MQTT Version 3.1. 1; 2014. Available from: http://www.docs.oasis-open.org/mqtt/mqtt/v3.
15. Khalil K, Elgazzar K, Bayoumi M. A Comparative Analysis on Resource Discovery Protocols for the Internet of things. In: 2018 IEEE Global Communications Conference; 2018. p. 1-7.

16. Jaffey T. MQTT and CoAP, IoT Protocols; 2014. Available from: https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php.
17. Dinculeană D, Cheng X. Vulnerabilities and limitations of MQTT protocol used between IoT devices. Appl Sci 2019;9:848.
18. Heđi I, Špeh I, Šarabok A. IoT Network Protocols Comparison for the Purpose of IoT Constrained Networks. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics; 2017. p. 501-5.
19. Tang K, Wang Y, Liu H, Sheng Y, Wang X, Wei Z. Design and Implementation of Push Notification System Based on the MQTT Protocol. In: 2013 International Conference on Information Science and Computer Applications; 2013.
20. Google Trends, Compare; 2020. Available from: https://www.trends.google.com/trends/explore?geo=us&q=mqtt,coap,xmpp,amqp. [Last accessed on 2020 Dec 19].
21. Grgić K, Špeh I, Heđi I. A Web-based IoT Solution for Monitoring Data Using MQTT Protocol. In: 2016 International Conference on Smart Systems and Technologies; 2016. p. 249-53.
22. Durkop L, Czybik B, Jasperneite J. Performance Evaluation of M2M Protocols Over Cellular Networks in a Lab Environment. In: 2015 18th International Conference on Intelligence in Next Generation Networks; 2015. p. 70-5.
23. Upadhyay Y, Borole A, Dileepan D. MQTT Based Secured Home Automation System. In: 2016 Symposium on Colossal Data Analysis and Networking; 2016. p. 1-4.
24. Liu X, Zhang T, Hu N, Zhang P, Zhang Y. The method of Internet of Things access and network communication based on MQTT. Comput Commun 2020;153:169-76.
25. Yassein MB, Shatnawi MQ, Aljwarneh S, Al-Hatmi R. Internet of Things: Survey and Open Issues of MQTT Protocol. In: 2017 International Conference on Engineering and MIS; 2017. p. 1-6.
26. Caro ND, Colitti W, Steenhaut K, Mangino G, Reali G. Comparison of Two Lightweight Protocols for Smartphone-based Sensing. In: 2013 IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux; 2013. p. 1-6.
27. Stanford-Clark A, Truong HL. MQTT for Sensor Networks (MQTT-sn) Protocol Specification. International Business Machines (IBM) Corporation Version; 2013. p. 1-27.
28. Sankar PS. A secure and fast authentication implementation between the entities using trust aware algorithm. Int Innov Res J Eng Technol 2016;2:34-40.
29. Krishna PG, Ravi KS, Kumar V, Kumar MS. Implementation of MQTT protocol on low resourced embedded network. Int J Pure Appl Math 2017;116:161-6.
30. Soni D, Makwana A. A Survey on MQTT: A Protocol of Internet of things (IoT). In: International Conference On Telecommunication, Power Analysis and Computing Techniques; 2017.
31. Kotak J, Shah A, Rajdev P. A Comparative Analysis on Security of MQTT Brokers. 2nd Smart Cities Symposium (SCS 2019); 2019.
32. Anthraper JJ, Kotak J. Security, Privacy and Forensic Concern of MQTT Protocol. In: Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM). Jaipur, India: Amity University Rajasthan; 2019. p. 876-83.
33. Quincozes S, Emilio T, Kazienko J. MQTT Protocol: Fundamentals, Tools and Future Directions. IEEE Latin America Transactions; 2019. p. 1439-48.
34. Mishra B, Kertesz A. The Use of MQTT in M2M and IoT Systems: A Survey. IEEE Access; 2020. p. 201071-86.
35. Karagiannis V, Chatzimisios P, Vazquez-Gallego F, Alonso-Zarate J. A Survey on Application Layer Protocols for the Internet of Things. Transaction on IoT and Cloud Computing; 2015. p. 11-7.
36. Sharma C, Gondhi NK. Communication Protocol Stack for Constrained IoT Systems. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU); 2018. p. 1-6.
37. Pohl M, Kubela J, Bosse S, Turowski K. Performance Evaluation of Application Layer Protocols for the Internet-of-Things. In: 2018 6th International Conference on Enterprise Systems (ES); 2018. p. 180-7.
38. Pathaka AD, Tembhurne JV. Internet of Things: A Survey on IoT Protocols. In: Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT); 2018. p. 26-7.
39. Dizdarević J, Carpio F, Jukan A, Masip-Bruin X. A Survey of Communication Protocols for the Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Computing Surveys; 2019. p. 1-29.
40. Verma S, Rastogi MA. IoT Application Layer Protocols: A Survey; 2020. p. 57-63.