Comprehensive Study & Analysis of Well Known IoT Protocols

Debajyoti Guha [1], Rajdeep Chakraborty[2] ,Debosmita Paul[3],Aheli Acharya[4]

[1]*Dept. of Computer Science & Engineering, Siliguri Institute of TechnologyE-Mail: debajyoti.aec@gmail.com*
[1]*Dept. of Computer Science & Engineering, Netaji Subhash Engineeing CollegeE-Mail: rajdeep.chak@gmail.com*
[1]*Dept. of Computer Science & Engineering, Netaji Subhash Engineeing CollegeE-Mail:debasmitapaul27@gmail.com*
[1]*Dept. of Computer Science & Engineering, Netaji Subhash Engineeing CollegeE-Mail*: aheli.nsec.btech.cse@gmail.com

Abstract
The advent of IoT is prominent to a different age where all objects, devices and sensors are associated over the internet. Physical devices can be controlled & communicated in IoT. This review manuscript defines & relates few leading protocols e.g. MQTT, AMQP, CoAP, XMPP, HTTP/HTTPS. These protocols are then contrasted on some factors such as type of transport, security, architecture & constrained environments, mode of communication etc. With the purpose of improving an effective application, picking the exact architecture is essential. If we see the recent trend, we are proressingtowards IIOT, home automation and smart cities.

Keywords— *Internet of things (IoT), MQTT, AMQP,CoAP, XMPP,HTTP/HTTPS*

I. Introduction:

Since most of the IOT devices are battery operated, hence the architecture must be platform independent and light weight. If data transfer will will take considerable energy, then the concerned application may not survive in thecompetitive market. To develop an application,following important features are required.

1. Architecture- It is the base of an application and hence plays an important part in the progress of theapplication.
2. Communication-To transfer data in between devices, the application should be able to communicate with other devices
3. Lifetime- As most of the IOT devices are battery operated, it is needed that the lifetime of the deviceto be longer.
4. Scalability- Application should be scalable.
5. Security-Security plays an important role in IOT during transfer of data to theauthenticated person.

IoT Protocols:

A. Message Queue Telemetry Transport (MQTT)

Message queue telemetry transport (MQTT) is a widely used, asynchronous publish/subscribe, light weight and open protocol. It uses TCP/IP that provides ordered & bidirectional connections. It has support for low bandwidth& high latency networks. MQTT plays an important role in IoT as messaging protocol among things and servers. Publish/Subscribe protocols convene better requirement of IoT than request/response protocol.

Broker contains topics in MQTT [1]. The client in MQTTcan be publisher or subscriber. A client can publish/send information to the broker as a publisher at specific topic. Aclient as a subscriber can receives automatic messages on every new update in the topic he subscribed. MQTT is usedin Facebook Messenger [2].

It has less overhead in contrast to TCP based protocols [3].MQTT broker may require username/password authentication handled by TLS/SSL. MQTT has greater overhead compared to CoAP. but COAP has more packet loss. For low packet losses, MQTT experiences lower delays than CoAP. Fig. I shows MQTT protocol operation.

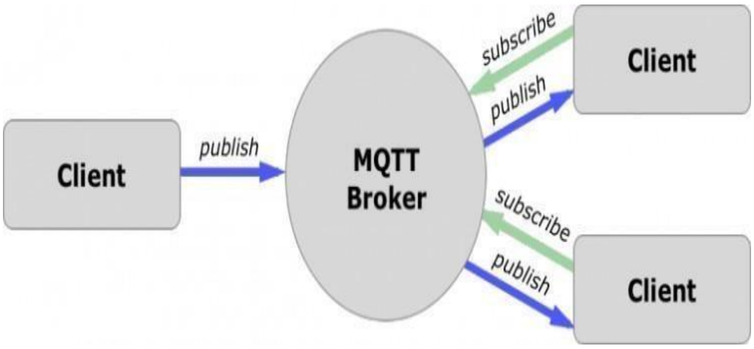

Fig. 1. Operation.in MQTT protocol

Constrained Application Protocol (CoAP)

Constrained Application Protocol, (CoAP) is a messaging & synchronous request- response protocol [4] that uses REST architecture. Many of the IoT devices are resource controlled. CoAP was proposed to transform a few HTTP functions to satisfy the needs for IoT & executed bymeans of HTTP methods like GET,POST,PUT,DELETE[5]. UDP is an unreliable protocol & it is the governing protocol for CoAP that minimizes bandwidth needs by eradicating TCP overhead [6]. Fig.2 reflects the representation of CoAP.

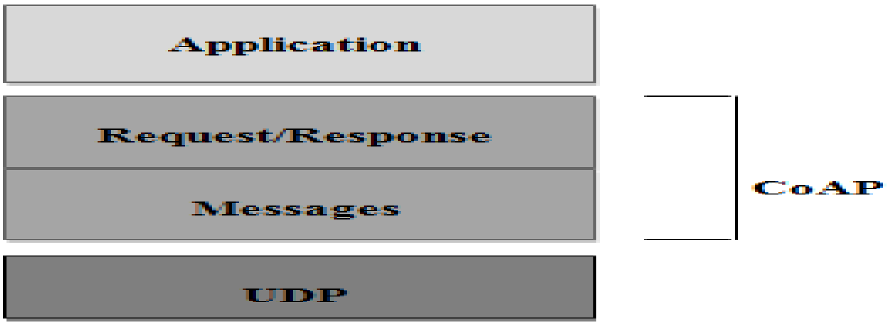

Fig. 2. CoAP Representation

As CoAP runs over UDP, it has support for multicast &unicast, in comparison to TCP. However, CoAP has incorporated its own mechanisms for providing reliability.There is a Stop-and-Wait retransmission methodology for confirmable messages. CoAP’s HTTP mapping permits clients to utilize resources on HTTP servers by reverse proxy used to translate the HTTP Status codes into Response codes [7]. CoAP was devised for the M2M and IoT transmissions. To make CoAP & UDP transmission safe, Datagram Transport Layer Security protocol (DTLS) is employed to provide data integrity, authentication, cryptographic algorithms, confidentiality and automatic key management [8]. DTLS protocol has no support multicasting mechanism. DTLS handshaking [9] involves extra packets to take up methodologies to give trustworthiness for computational resources, enhance network traffic & cut down the lifetime of mobile devices.Being designed for the IoT, CoAP is compatible with HTTP. CoAP satisfies web requirements e.g simplicity, minimized overheads and multicasting.

Extensible Messaging and Presence Protocol (XMPP)

Extensible Messaging and Presence Protocol (XMPP) is comparatively an older protocol devised for message exchanging, video streaming, chatting etc.Of late XMPP has taken over the characteristics of XML protocol imbibing higher scalability, addressing & safety mechanism. XMPP acts as client, server & gatewayServer provides message routing & link management functions. Gateway maintains support for transmissions among all heterogeneous systems. Client can be connectedto server by applying TCP/IP protocol suite. XMPP maintains object to object communication with XML-based text messages. TCP/IP is a governing protocol in XMPP that gives synchronous (request/response) & asynchronous (publish/subscribe) messaging systems. XMPP holds minor latency message swapping & message footprint [10]. XMPP has intrinsic TLS/SSL security mechanism. XMPP supports the publish/subscribe architecture used in IoT in comparison to request/response approach of CoAPs. XMPPhas already provided the protocol which is supported by allover the Internet with regard to the MQTT [11]. XML messages used in XMPP results in overhead and requires XML parsing resulting in additional computational capacity involving enhanced power consumption.

Advanced Message Queuing Protocol (AMQP)

Advanced Message Queuing Protocol (AMQP) is a message-oriented middleware protocol used to give services viz. routing, queuing, security & reliability[12]. Itprovides publish/subscribe (asynchronous) communicationwith messaging. The store-and-forward feature of AMQP gives trustworthiness during network disturbance [15]. Thesecurity in AMQP is given by TLS/SSL over TCP [13]. Success rate of AMQP is directly proportional to its bandwidth. MQTT and CoAP are both functional for IoT with their fundamental disparities. MQTT is a many-to- many transmission protocol for sending out messages among several clients through a central broker whereas CoAP is a one- to- one protocol for transferring state data among client and server. MQTT clients creates TCP connection to a broker. CoAP sends and receives UDP packets among clients and servers. MQTT hasno support for labelling messages to help clients understand it. On theother hand CoAP gives integral support for content negotiation and invention b y allowing devices to explore one another to locate paths of sharing data. [4].Fig 3 reflects the message exchange in AMQP.

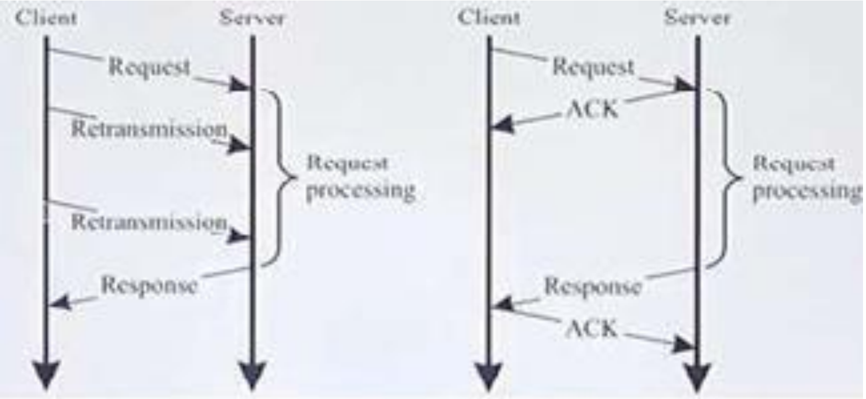

Fig 3. Message exchange phase in AMQP

Hypertext Transfer Protocol (HTTP) & Hypertext Transfer Protocol Secure (HTTPS)

In IoT HTTP is used for communicating large numberof packets. HTTP protocol sends many small packets to theserver leading to high resource utilization and associated network delay. It is governed by TCP/IP. HTTP is astateless protocol. Whenever it is connected to IP/URL, itprovides authentication & hence the session is not stored. Therefore the device closes the connection after getting theresponse creating overhead in network communication. HTTPS provides security associated with SSL/TLS protocol. Protocol overhead in HTTPs is similar HTTP with respect to network resources and delay.

Comparison:

MQTT and CoAP are equally important IoT protocols with some fundamental differences. MQTT is a many-to- many communication protocol for transmitting messages amongg many clients via a central broker. CoAP is a one- to- one protocol for forwarding state information among client and server. MQTT clients creates TCP connectionto a broker. CoAP sends and receive UDP packets among clients and servers. MQTT has no support for labelling messages with types or other metadata to help clients understand it. On the contrary CoAP gives intrinsic support for content negotiation and invention permitting devices to f ind one another to get paths of sharing data. [14]

There is hardly any requirement for broker in the middle incase of AMQP as this is a peer-to-peer protocol & hence can be utilized among two peers. There is no concept of queue inMQTT & it functions as a lightweight protocol only with a broker in the middle. [15] AMQP is more leaning to messaging than MQTT. [16] A comparative study among popular IoT protocols is given below.

Protocols	MQTT	CoAP	AMQP	XMPP	HTTP/HTTPS
Publisher/Subscriber	Yes	No	Yes	Yes	No
Request/Response	No	Yes	No	Yes	Yes
Safety	SSL	DTLS	SSL	SSL	SSL
Quality ofService	Yes	Yes	Yes	No	No
Transport	TCP	UDP	TCP	TCP	TCP

Table I: Comparative Study about IoT protocols

II. Conclusion:

In this manuscript, analysis have been done on five well known IoT protocols that have gained huge significance in IoT. Amid those protocols, CoAP was specified as the onlyone where UDP is the governing protocol thereby making it the most lightweight. It was found in this survey that the transmission & computational ability of the associated devices should be judged while selecting the main suitable protocol. In contrast, MQTT unlike HTTP, can be effectively used for battery devices. Numerous factors like communication, computational ability and of course battery usage are there that controls the choosing of IoT protocols. On the basis of this survey, it can be concluded that MQTT can be a fair choice for small IoT business applications in comparison with CoAP andAMQP protocols.

References:

[1]. Correlation Analysis of MQTT Loss and Delay According to QoS Level, Shinho Lee, Hyeonwoo Kim, Dong-kweon Hong, Hongtaek Ju,,International Conference onInformation Networking (ICOIN),28-30 Jan.

[2]. http://mqtt.org/2011/08/mqtt-used-by-facebook-messenger, cited 28 Jul 2014.

[3]. Performance Evaluation of MQTT and CoAP via a Common Middleware, Dinesh Thangavel, Xiaoping Ma, Alvin Valera, Hwee-Xian Tan, Colin Keng-Yan Tan, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 21- 24 April 2014.

[4]. Firebase: A Platform for your Web and Mobile Applications, Mr. Bhavin M. Mehta1, Mr. Nishay Madhani2, Mrs. Radhika Patwardhan3, December 2017.

[5]. Web Services for the Internet of Things through CoAP and EXI, Angelo P. Castellani, Mattia Gheda, Nicola Bui, Michele Rossi, Michele Zorzi, IEEE International Conferenceon Communications Workshops (ICC), 5-9 June 2011.

[6]. Securing the Internet of Things: A Standardization Perspective, Sye Loong Keoh, Sandeep S. Kumar, Hannes Tschofenig, Internet of Things Journal IEEE (Volume: 1, Issue: 3), June 2014.

[7]. Standardized Protocol Stack for the Internet of (Important) Things, Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, GennaroBoggia, Mischa Dohler Communications Surveys & Tutorials IEEE 15(3), 2013.

[8]. Security Analysis of the Constrained Application Protocol in the Internet of Things, Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash, Second International Conference on Future Generation Communication Technology (FGCT), 12-14 Nov. 2013.

[9]. Lithe: Lightweight Secure CoAP for the Internet of Things, Shahid Raza, Hossein Shafagh, Kasun Hewage, Ren Hummen, Thiemo Voigt Sensors Journal, IEEE 13(10), Oct. 2013.

[10]. A Service Infrastructure for the Internet of Things based on XMPP, Sven Bendel, Thomas pringer, Daniel Schuster, Alexander Schill, Ralf Ackermann, Michael Ameling, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 18- 22 March 2013.

[11]. Unify to Bridge Gaps: Bringing XMPP into the Internet of Things, Michael Kirsche, Ronny Klauck, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 19-23 March 2012, pp. 455-458.

[12]. Evaluation of Transport Protocols for Web Services, Frank T. Johnsen, Trude H. Bloebaum, Morten Avlesen, Skage Spjelkavik, Bjørn Vik, Military Communications andInformation Systems Conference (MCC), 7-9 Oct. 2013.

[13]. http://en.wikipedia.org/wiki/Advanced Message Queuing Protocol, cited 28 Jul 2014.

[14]. Performance evaluation of MQTT and COAP via a common middleware in

[15]. *Intelligent Sensors, Sensor Networks and Information Processing,* D. Thangavel, X. Ma,

A. Valera, H.-X. Tan, and C. K.-Y. Tan *(ISSNIP), 2014 IEEE Ninth International Conference on*. IEEE, 2014,pp. 1–6.

[16]. A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks in *Consumer Communications and Networking Conference (CCNC), 2015 12thAnnual IEEE.* IEEE, 2015, pp. 931–936.

[17]. Advanced message queuing protocol, S. Vinoski, ,*IEEE Internet Com- puting,* vol. 10,no. 6, 2006.

Acknowledgement:

The authors are grateful to the Dept. of computer Science & Engineering, Siliguri Institute of Technology under Maulana Abul Kalam Azad University of Technology. They are also grateful to the Dept. of computer Science & Engineering, Netaji Subhash Engineering College Maulana Abul Kalam Azad University of Technology.