A Comparative Study of Messaging Protocols

Shefali Mahadik, Pragya Maurya, Aditi Jadhav, Suvarna Pansambal*

Atharva College of Engineering, Mumbai, Maharashtra, India

Publication Info

Article history:
Received : 14 February 2020
Accepted : 23 May 2020

Keywords:
AMQP, Facebook, Instagram, MQTT, Protocols, WhatsApp, XMPP.

Corresponding author:
Shefali Mahadik
e-mail: *shefalimahadik007@gmail.com*

Abstract

Messaging Protocols are fundamentally configurations and rules characterized for trading messages between various pieces of a messaging framework. Message passing is a sort of correspondence between processes. Message passing is a type of correspondence utilized in parallel programming and object-oriented programming. The sending of messages processes interchanges through signals, packets of data, and functions to beneficiaries. This work targets examining messaging protocols like MQTT (Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol), and XMPP (Extensible Messaging and Presence Protocol) with respect to their features, application, security angles, confinements, and their use in well-known Social Media and informing applications.

1. INTRODUCTION

The technique of behavior invoking on a computing device over a network is known as message passing. The summoning program messages a process and relies upon that procedure and its supporting association to choose and afterward run its chosen code—message passing contrasts from conventional programming where a subroutine or function is directly summoned by name.

Message passing is utilized generally in PC programming and computer software. It is utilized as a path for the particles that make up a program to work with one another. Different instruments, including channels, might execute message passing.

Communication Protocol can be defined as a predefined set of rules, using which units of a communication system are enabled to use any physical quantity variation to send information. The convention characterizes the principles, syntax, semantics and synchronization of correspondence and gives conceivable mistake recuperation strategies. Conventions might be executed independently over equipment or programming or over a mix of both.

2. MESSAGE PASSING PROTOCOLS:

2.1. MQTT

MQTT is a client-Server publish-subscribe messaging transport protocol. It is welcoming, open, basic, and intended to be anything but difficult to actualize by the publishers as well as subscribers. The qualities of MQTT make it reliable for use most of the time, including controlled conditions, for example, for communication in Machine to Machine (M2M) and Internet of Things (IoT) settings[1]. For instance, Facebook Messenger depends on MQTT. In contrast with some very much utilized conventions like Hypertext Transfer Protocol (HTTP), it has an insignificant overhead. Another significant part of MQTT is that it is very simple to actualize on the customer side. This fits impeccably for controlled gadgets with constrained assets. Its simplicity of execution was one of the objectives that were met when MQTT was invented. MQTT was designed in 1999 with the point of making a convention for negligible battery loss and insignificant data transfer capacity usage. By and large there is a merchant between the customers who encourage and additionally channel the data. This takes into account a loose coupling between units. There are different ways decoupling happens, namely Space, Time, and Synchronization[2].

- **Space:** the publisher and subscriber need not reveal identities by IP address or other ways.
- **Time:** the two clients do not have to be running at the same time.
- **Synchronization:** Operations are not stopped by publishing and receiving.

The MQTT architecture comprises of two units of communication. These units are taking the role of publishers and subscribers, client and server/broker. Messages can be published or subscribed or both by the client. Fig. 1 explains MQTT Interaction model. The messages that the

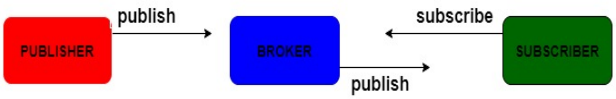

Fig. 1: MQTT interaction model

client publishes are accepted by the broker, who serves as a central component. The broker also performs the function of delivering the messages to the subscribed clients.

2.1.1. Limitations of MQTT

Analyzing the Limitations of the MQTT protocols gives us these outlooks.

- It operates over TCP. TCP requires more time to set up communication, which results in increased communication time and wake-up time [3].
- There is very limited support for the Retained Messages feature of MQTT messaging
- Subscription request from either a device or application is allocated a buffer of 5000 messages. The buffer allows for any application or device to fall a backlog of up to 5000 pending messages for each subscription. When the buffer is full, the oldest messages are discarded when a new message is received [4].
- Some size limitations apply for the message payload on Platform Service.

2.1.2. Protocol Security

MQTT utilizes diverse security processes, yet the majority of them are not composed or given beforehand, for example, information encryption or entity verification. Authentication ways, for example, utilizing the gadget's physical location (MAC), exist and are constrained by the broker by making a note of device data once it attempts to associate. Access approval should be possible by the broker utilizing a component called an access control list (ACL). The ACL contains records of data, for example, the identifiers and passwords of the various clients that are permitted to get to various objects and can likewise indicate what works the client can perform on these.[5][6]

2.2. XMPP

XMPP (Extensible Messaging and Presence Protocol) is an XML-based convention which is open and gives close constant administrations, real-time data and texting and expanding its administrations into the more extensive zone of message-oriented middleware. Being extensible, it can offer several types of services, such as Voice over IP, which is used in social networking sites such as Gtalk, WhatsApp, and Facebook; services such as Google wave and gradient;, and several online customers and technical support administrations. Considering the way that Instant messaging is getting well known among clients alongside the fast advancement of short message administration as a result of the improvement of the information society, the amalgamation of these two technologies can, without much of a stretch, fulfill the clients demand. As clients currently are tending to utilize cell phone at any instant of time and from anywhere, the interconnection of these two advances is another necessity. XMPP, which depends on Extensible Markup Language (XML) tackles the issue that instant informing framework couldn't interconnect with other non-instant Messaging frameworks. The instant and presence message in XMPP are based on XML[7]. For switching between the elements, these messages use XML Stanza. XML is a readable content arrangement which is adaptable, extensible and simple to make and to peruse. It's simple to assemble a gateway through XML to understand the correspondence between XMPP framework and non-XMPP framework. XMPP gateway is a unique element of the server. Its primary errand is to interpret XMPP into the convention that the non-XMPP framework utilizes and do the turnaround process. The architecture of XMPP is decentralized. XMPP utilizes a customer server model which implies that customers don't talk straightforwardly to one another. By structure, XMPP does not have a central server. Every client on the XMPP network has a XMPP address (JabberID) that works like an email address with an IP address/area name and a username for the inhabitant server. XMPP convention is well-suited for any communication platform that underpins the pub-sub configuration design. Pub-Sub configuration design depicts how the message streams between the gadgets and applications. Here, the publisher sends information to the subscriber who gets the information through committed channels. These subscribers get a notice at whatever point another message gets through these channels[8][9].

2.2.1. Limitations of XMPP

- Redundancy of data transmitted: Excess traffic is created due to the presence of data
- Limited scope to scalability: Because of the excessive traffic, XMPP is challenging for the creation of chat rooms and data publishing.
- Inability to send binary data: Because XMPP is encoded as a long XML document, transmission of binary data is difficult [10].

2.2.2. Protocol Security:

XMPP provides numerous levels of security that are inherent in the protocol. Fig. 2 shows XMPP Interaction

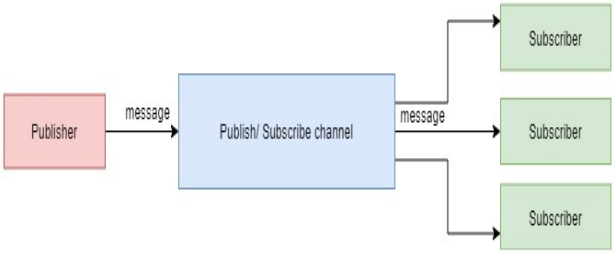

Fig. 2: XMPP interaction model

 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

model. Individual identity in XMPP is stronger compared to WebSockets. To stay away from the risk of spoofing, users need to authenticate both host servers and messages, thereby dealing with the threat of spam. More layers of security can be added by requiring clients to put in a suitable security certificate for identity confirmation[11].The XMPP comprises of two types of encryption. The first encryption takes place at the establishment and authentication using SASL(Simple Authentication and Security Layer). After a connection has been established, all client-server transmissions are encrypted using TLS(Transport Layer Security). As a result, the danger of getting attacked is very small.

2.2.3. AMQP

AMQP(Advanced Message Queuing Protocol) comprises of a network protocol, which specifies what client applications and message servers must send through the wire to work in conjunction with each other, and a protocol model, that with other implementations must perform inter-operable with semantics. AMQP is the final result of a standardized attempt by the major contributors in the messaging sections(e.g. Cisco, Microsoft, Red Hat, banks). In between different messaging systems AMPQ aiming for interoperability. The AMQ convention model comprises of the following key focuses the chain of duty design. Right now, that seem to stream straightforwardly from sender to collector really move through a lot of message processors dwelling between the two. The second significant point to note about the convention model is that it empowers the merchant to settle on steering choices adequately. It gives the definition to a twofold wire convention and a total conveyance semantic, permitting, hypothetically, for an AMQP informing customer to have the option to connect consistently with various dealers' usage which is AMQP agreeable. These days, the appropriation of the most recent stable adaptation[12] of the convention isn't yet broad, yet given that it is as of now upheld by the significant message expedites, an a lot more extensive usage is normal in the up and coming years. In AMQP message is first sent to a part of Message Broker called Exchanges. Trades appropriate message duplicates to lines utilizing rules called ties. At that point AMQP intermediaries either convey messages to buyers bought in to lines, or buyers bring/pull messages from lines on request.

Fig. 3 is an example connection graph on how AMQP functions.

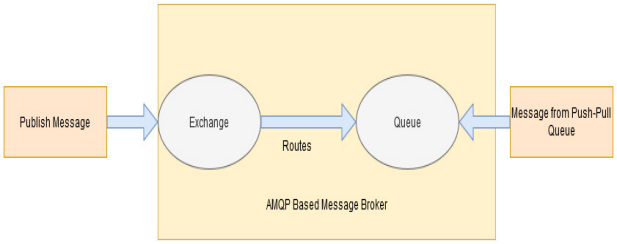

Fig. 3: AMQP interaction model

RESULT

Table 1. Comparison of AMQP, MQTT, XMPP

Criteria	*AMQP*	*MQTT*	*XMPP*
Format	Binary	Binary	XML based
Aim	Replacement of exclusive protocols	To enable message passing in resource-constrained devices	Promotes instant messaging for wider use
Reliability	Publisher subscriber acknowledgments	Acknowledgments	Acknowledgments and resumption
Security	SASL, TLS/SSL	Header authentication	SASL, TLS/SSL
Extensibility	Extension points	None	Extensible
API	Divided into classes	5 operations with 2-3 packet types for each	Different XML items with multiple types
Transport	TCP	TCP	TCP
Interaction model	Point to point	Publisher-Subscriber	Point to point
Resource discovery	No	No	Yes
Message Caching	Yes	Yes	Yes
Scope	Device to Device Device to cloud Cloud to cloud	Device to cloud Cloud to cloud	Device to cloud Cloud to cloud
Interoperability level	Structural	Foundational	Structural
Fault tolerance	Implementation specific	Broker in SPoF	Server in SPoF

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

Table 2: Comparison of WhatsApp, Facebook, Instagram

Criteria	*WhatsApp*	*Facebook*	*Instagram*
Meaning	It is an application which provides users texting services	It facilitates users to connect themselves to the online community and build a social circle	It allows users to build and join communities that share common interest
Security	End to end encryption by default	Have to enable end to end encryption (secret conversation)	End to end encryption not there
Features	The users can chat and call their WhatsApp contacts and share photos, videos and audio, group messaging is also present	The users can chat, call, post.and update pages, play games online, group conversations, etc	Allows sharing of photos, videos and also has facility of direct messages, best for brand promotion, group chat facility available
Protocol used	XMPP	MQTT	AMQP
Like and comment	No	Yes	Yes
Account requirements	Phone number	Facebook account	Instagram account

2.2.4. Limitations of AMQP

The AMQP specifications enforce these limits on forthcoming extensions of AMQP such as limitations on number of channels per connection, number of protocol classes, and number of methods per-protocol class.
The AMQP specification limits data in these classes:

- Maximum size of a short string: 255 octets.
- Maximum size of a long string or field table: 32-bit size.
- Maximum size of a frame payload: 32-bit size.
- Maximum size of content: 64-bit size.

The server or client may in like manner power its own cutoff focuses on resources, for instance, number of synchronous affiliations, number of buyers per channel, number of lines, etc. These don't impact interoperability and are not indicated.[13]

2.2.5. Protocol Security

By utilizing length-determined buffers it guards us against buffer-overflow in all spots. All remotely given information can be checked against most extreme permitted lengths at whatever point any information is perused. Invalid information can be taken care of unambiguously by shutting the channel or the association.

AMQP attacks handle blunders by restoring an answer code and afterward shutting the channel or association. This stays away from vague states after mistakes. The server should expected that remarkable conditions during association arrangement organize are because of a threatening endeavor to access the server. The general reaction to any excellent condition in the association exchange is to stop that association (apparently a string) for a time of a few seconds and later close the network connection. This incorporated larger than usual information, syntax error and failed attempts to verify. The server SHOULD log every single such exemption and block or flag customers inciting numerous disappointments.

3. CONCLUSION

Mesagging is essentially a practical solution to the problem of distributed systems. In this work, we have successfully surveyed application layer protocols, focusing on their application, security aspects, usage, and limitations in a comparative, tabular format. The study found which application-layer protocols are predominantly used in various social media and messaging applications. This study also puts light on the fact that some communication protocols are favored over others by developers. MQTT has be proven to stand the test of time to have excellent performance over constrained devices. Although MQTT is suited for simple clients, any infrastructure using it is exposed to numerous security weaknesses and failure to better use resources. On the other hand, AMQP is suited to these cases and supports better use of resources and a practical security approach with message reliability. AMQP is a simple yet powerful enterprise messaging tool that has bright future in enterprise messaging. XMPP is a near end streaming instant messaging protocol that embeds field and context-sensitive information into XML, enabling communication between systems and people. Thus this study congregates three major communication protocols highlighting their usage and application.

4. ACKNOWLEDGEMENT

We would like to take this opportunity to thank our guide Prof. Suvarna Pansambal for her enormous cooperation and help. We are very thankful to her for instigating within us, the need for this research and giving us the opportunity and time to conduct and present this piece of research. We express our gratitude wholeheartedly towards a person who supported our research with her kind cooperation

and encouragement, which helped us in completion of this research. It was a great experience learning under such a highly innovative and enthusiastic, helpful and hardworking professor. We are also thankful to our Principal, Dr. S.P. Kallurkar, and HOD of Computer Department, Prof. Suvarna Pansambal, project coordinators, Prof. Mamta Meena, Prof. Shweta Sharma and Prof. Samidha Kurle and all the staff members of the Computer Department. They have provided us with various facilities and guided us throughout.

5. REFERENCES

[1] MQTT (MQ Telemetry transport) http://mqtt.org

[2] Bryce, R., Shaw, T. and Srivastava G. (2018) July. Mqtt-g: A publish/subscribe protocol with geolocation. 41st International Conference on Telecommunications and Signal Processing (TSP), IEEE, 1-4.

[3] Dinculeană, Dan, and Xiaochun Cheng. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. Applied Sciences 9, no. 5-848.

[4] Yokotani T and Sasaki Y. (2016). Comparison with HTTP and MQTT on required network resources for IoT, Iinternational conference on control, electronics, renewable energy and communications (ICCEREC) IEEE 1-6.

[5] Katsikeas S., Fysarakis K., Miaoudakis A., Bemten A.V., Askoxylakis I., Papaefsta-thiou I., Plemenos. (2017) A Lightweight & Secure Industrial IoT Communications via the MQ Telemetry Transport Protocol , Proceedings of IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece. 3-6.

[6] Dizdarević J., Carpio F., Jukan A. and Masip-Bruin X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration, ACM Computing Surveys (CSUR). 51(6), 1-29.

[7] Griffin L., de Leastar E. and Botvich D. (2011). Dynamic shared groups within XMPP: An investigation of the XMPP group model, 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops, IEEE, 634-637

[8] Lu X., Lei W. and Zhang W. (2012). The design and implementation of XMPP-based SMS gateway. Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE, 145-148.

[9] XMPP (Extensible Messaging and Presence Protocol) http://xmpp.org

[10] Ozturk, O. (2010). Introduction to XMPP protocol and developing online collaboration applications using open source software and libraries, International Symposium on Collaborative Technologies and Systems, IEEE, 21-25.

[11] AMQP (Advanced Message Queuing Protocol) http://www.amqp.org

[12] S Vinoski, (2006) Advanced Message Queuing Protocol, IEEE Internet Computing, vol. 10, no. 6, 87-89.

[13] Cohn R. (2011) A comparison of AMQP and MQTT, White Paper*, StormMQ*,

