IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 1, January 2022

DOI: 10.17148/IARJSET.2022.9136

A Study on MQTT Protocol and its Cyber Attacks

Abhay Pratap Singh[1], **Amit Kumar**[2], **Vipin Kumar**[3]

Research Scholar, Department of Computer Science, Gurukula Kangri (Deemed to be University), Haridwar, India [1,2,3]

Abstract: The Internet of Thing (IoT) is a model of interconnected objects, devices, systems, and other items which are embedded with communication hardware, software, processors and network connectivity, which enables these objects to congregate and swap information. Fast revolution in the field of information communication, technologies, and digital things, are compelling quick information of IoT over the world. In IoT, device to device communication is considered through either Pushing or pulling protocol. Push protocol is more suitable for IoT devices because of its lightweight and high productivity. There are many push protocols available for IoT, where a user does not look for any kind of information. In which MQTT is widely utilized because of its frivolous and bandwidth efficiency. Security is one of the main cares with regards to IoT networks. Since it is not easy to implement robust security mechanism in most of IoT devices because of its restriction in resources and power consumption. MQTT protocol has been implemented because of its little cost and ease software platform which is appropriate for IoT application. This paper gives idea about various attacking scenarios in MQTT protocol and its introduction.

Keywords: IoT, MQTT, Push protocol, Publish/Subscribe, Attacks, Security.

I. INTRODUCTION

The world ‘smart’ used before the name of IoT devices such as smart TV, Smartphone which means that these devices are connected to the internet and the capability to transmission data over a network [1]. The IoT has been developed expressively and is progressing towards maturity. Through this maturity it is possible to blend anything, from something as small as a needle to something large as an aeroplane. It can be looked as “a global network which provides the communication between human-to-human, human-to-things, things-to-human, and things-to-things through constructing a unique identity for each object”. For making the network IoT, various objects which include embedded sensors, software, wireless communication, processors, and electronics can be connected together.

The IoT has amalgamation of two terms. The first term arises from the word ‘Internet’, which be integrated the billions of user, devices, personal system and even the business organizations. The second term is Thing, which informs to intelligent item. From past few years the world has practiced dashing enhancement and functionality in technology, which has had a treasured impact on our daily lives.

In IoT, there are some important prominent protocols used as a communication protocols given as HTTP, MQTT, AMQP, and XMPP. While selecting protocols for communication, we will have to look at some considerations; energy, efficiency, performance, resource usage, and reliability. MQTT is considered as best protocol because of its reliability, advanced functionality and able to secure multicast messages [2]

The crescent number of incident of cyber criminals is compromising IoT devices. The prejudicial impact of security threats indicates by cyber-attacks in the IoT. In the IoT bionetwork, users can distantly retrieve IoT devices through using the application broker or middleware technologies [3]. The major security risk is straight revealing IoT devices to the internet for message transmission and remote control. Most of the IoT devices use middleware or message broker for bidirectional communication and remote control. These IoT devices function from behind firewalls. Several protocols have been evolved to accomplish the bidirectional communication and data transfer between IoT devices (D2D) and between devices and server/cloud (D2S). Among them, MQTT has appeared as the widely embraced protocol. An internet facing broker server uses to enable the exchange of information and messages between clients by this protocol, which are Smartphone, system and IoT devices. So far protecting the IoT environment, the security attacks in MQTT protocol needs to be recognized, that is already built on this protocol.

On the month of September 2016, a massive Distributed Denial of Service (DDoS) attack was launched by the largest attack, exceeding 620 gigabits per second (Gbps). This DDoS attack has been carried out using named, Mirai. In early October, Krebs on Security narrated attack based on a separated malware family, which was responsible for other IoT botnet attack. Source code of this malware is not yet revealed public, is named Bashlite.

Few security mechanisms are provided by this paper. Since IoT consist of several numbers of heterogeneous things, a dominant security mechanism should be lightweight for approbation. Hence in TLS, for each session key exchanges and collecting certificates is very heavy to secure MQTT protocol.

DOI: 10.17148/IARJSET.2022.9136

The remaining part of the paper is organized as: Section II discusses the introduction of MQTT protocol. Section III introduces the common cyber-attacks on MQTT and security explication. Finally the conclusion is discussed in last section.

II. INTRODUCTION TO MQTT PROTOCOL

MQTT is an oasis standardized Publish/Subscribe Push protocol that was introduced by IBM in 1999. MQTT exchanges a range of control packets in a particular manner for communication. There are fourteen control packets which exchange by the MQTT. Each packet comprises three parts as illustrated in below Table 1

Table 1 Common Control Packet Format

Fixed header exist in all MQTT Control Packet
Variable header exist in some MQTT Control Packet
Payload exist in some MQTT Control Packet

A. Publish/Subscribe

MQTT utilizes publish (send the message) subscribe (wait for the message) model. In Publish Subscribe model, the connection between the components is operated through the third party component called a broker. Each message has an own address, known as Topic. Topics are the way how to specify where to publish the message. In Publish Subscribe model, a device can publish a message on a topic to receive messages.

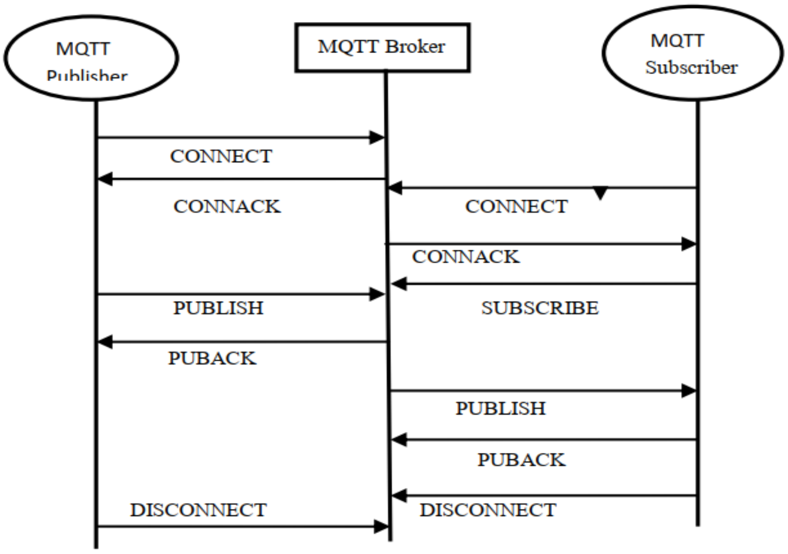

Fig 1 MQTT Protocol Publish-Subscribe model

B. Quality of Service Levels

MQTT operates over the TCP protocol that is the reason it provides reliable messaging service, but on the other hand it provides the Quality of Services (QoS) levels that are a deal with the guarantee of delivering a message between the sender and receiver. It supports the following three levels of Quality of Service.

- **At most once (QoS0) -** The minimal QoS level is zero. This QoS0 level does not provide any guarantee of delivery. Receipt of the message does not acknowledge by the recipient. The sender does not store and re-transmit the message that’s why this QoS0 level is often called “Fire and Forget”.
- **At least once (QoS1)** - This QoS1 level provides the guarantee that a message is delivered at least one time to receiver. The sender stores the message, acknowledge and retransmit till it does not get PUBACK packet from the receiver.
- **Exactly once (QoS2)** - In MQTT, this QoS2 level is the highest level of service. The message is delivered exactly once without any type of loss or duplication by the sender. This level provides the safest and leisureliest quality of service level.

C. MQTT Architecture

MQTT architecture describes MQTT message flow between the broker and clients (shown in fig 2). So it can be classified into two main components which are described below.

DOI: 10.17148/IARJSET.2022.9136

- **Client** - Both publishers and subscribers can be MQTT clients. MQTT client is any system or device that runs on MQTT library and establishes the network connection to an MQTT broker over a network.

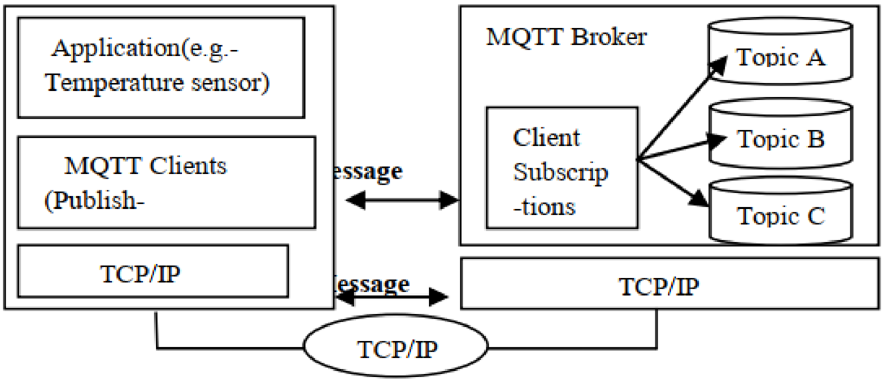

Fig 2 MQTT Architecture

- **Broker**- MQTT broker is a server that responsible for receiving all message packets from the source clients and then routes those packets to the suitable destination clients. A broker can maintain up to millions of concurrently connected MQTT clients.

III COMMON CYBER ATTACKS ON MQTT

MQTT is an application layer protocol that is penetrable to various known and unknown security issues. Because of its simplicity and scalability, MQTT transfers data among any IoT devices through the application layer protocol, compared to all other protocols. MQTT is a lightweight protocol design for low-bandwidth, high latency, reliable networks and lightweight communication between constrained resource devices such as mobile phone and servers. There are some attacks which are illustrated in below figure 3.

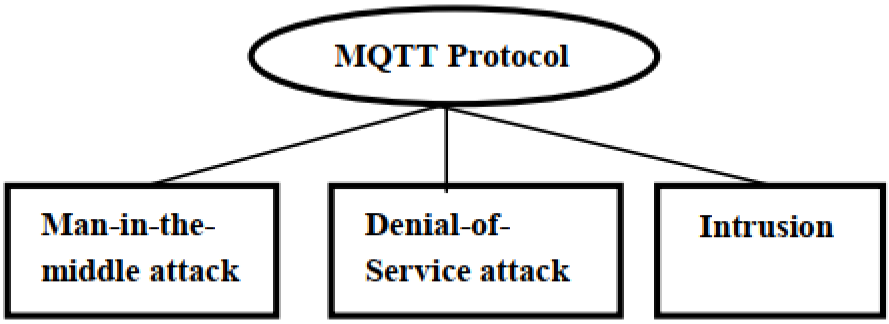

Fig 3 Attacks on MQTT

A. Man in the Middle Attack

A man in the middle hand (MitM) attack is a general system for when hacker stay himself in the middle of a conversation between a user and an application- either to overhear or to act one of the parties. The main motive of this attack is to drag out personal information, such as login credentials, password and credit card numbers. The hacker can redirect the same message to another user or can stop data transfer between sender and receiver. In MQTT, process of MitM is done between a broker and the sensor by manipulating the sensor data. Attack accomplishing tools are distribution kali Linux and the tool Ettercap.

MQTT protocols enable a two way handshake by allowing client authentication. This two way handshake is penetrable to man-in-the-middle attacks. Both authentication and encryption are needed to avoid MitM attacks. For preventing MitM attacks before they occur rather than trying to detect them while they are actively occurring, it is important to take safety measure. Packet Injection, Session, SSL Stripping, SSL Hijacking, and Sniffing are some attacking techniques to prevent MitM attacks.

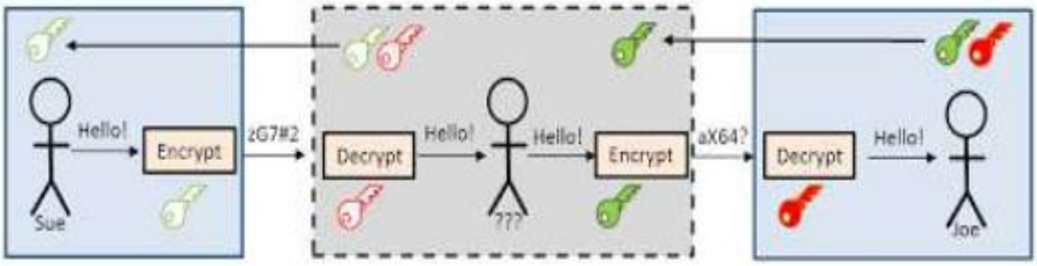

Fig 4 Man in The Middle attack in MQTT

B. Denial of Service Attack

A Denial-of-service attack is a kind of cyber-attack meant to shut down a machine, system or network to its intentioned users by disturbing the machine's general functioning [4]. This attack is typically implemented by overwhelming or flooding a targeted system with requests till normal traffic is not unable to be processed.

The MQTT broker has to be explored by receiving the network traffic. DoS attacks start from the broker by sending continuously multiple connection requests. Motive of this attack is to make broker busy as in flooding attack. As multiple connection requests continuously arise at the same time, the buffer will be faded and it will be hard to handle with new incoming connection requests for broker. It will be difficult to differentiate between normal and hoax CONNECT message packets for broker. After getting flood request messages, broker will start to acknowledge with CONNACK message. And due to this reason, there will be a rapid rate of increasing the number of CONNECT and CONNACK packets. The main motive of this attack is to overwhelm the capacity of targeted system, resulting in Denial-of-service to additional requests.

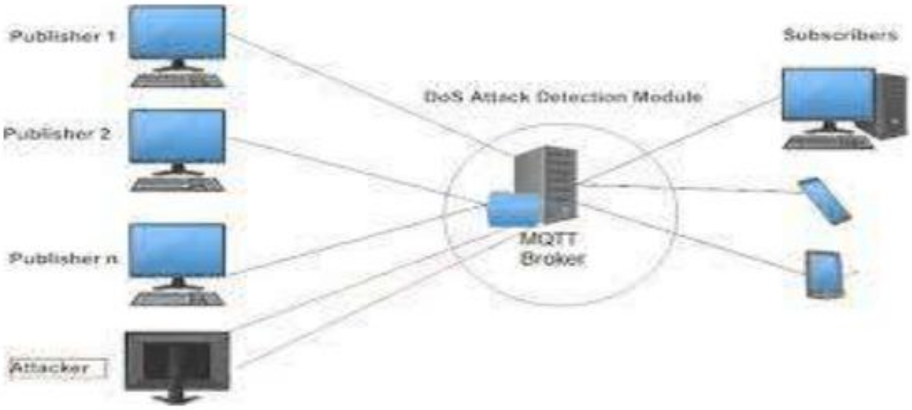

Fig 5 Denial of Service Attack in MQTT

C. Intrusion

Any unauthorized activity on computer network, known as the network Intrusion. Intrusion attacks based on the understanding of how to attacks work. Computer hackers use automated computer programs [5]. At that time they try to compromise a security of computer. Properly designing and deploying a network IDS (Intrusion Detection System) is main factor for security of MQTT. It will help to block the intruders. Intrusion attack combines of making use the renowned port for this protocol and a command that uses the special character "#" are often employed by an external hacker for getting the information of active topics existing for being subscripted.

D. Security explication on MQTT

An attack can damage the user in different domains. MQTT provides different security mechanism such as authentication but by default it does not encrypt the data in transit. That is the main reason of authentication, data privacy and data integrity become problems in MQTT implementation. During this authentication mechanism, when system tries to connect with MQTT broker, the broker registers all information of system that includes physical address of system (MAC). A broker can access authorization using Access Control List (ACL). The ACL consists of information that contains password and identifier of the different clients. It can access different objects and also specify the client which function it needs to be performed.

Data security is the most important constraint to be considered for selecting protocol for IoT devices. These components are very important for data security: which are data confidentiality, data availability and data integrity [6-7]. Authentication and authorization are also additional security requirement to provide access. But complete security mechanism is not available in MQTT protocol; it provides only authentication mechanism without encryption capabilities.

IV. CONCLUSION

In this paper, we briefly described the information about MQTT protocol and its architecture. This protocol is generally utilized for exchanges the messages between devices. Furthermore, it operates in TCP/IP protocol layer. It provides efficient data transmission between devices and utilizes very less amount of power, which is good for the wireless devices. It also reduces the network bandwidth while communication. We had also discussed the common cyber security attacks in MQTT protocol which will be helpful for detecting the attack pattern.

REFERENCES

[1]. Xi Chen. “Constrained Application Protocol for Internet of Things”. https://www.cse.wustl.edu/~jain/cse570-19/ftp/m_12lpn.pdf

[2]. S. Kraijak and P. Tuwanut. “A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends”. In: 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015). Sept. 2015, pp. 1–6. DOI: 10.1049/cp.2015.0714.

[3]. Hwang, H. C., Park, J., & Shon, J. G. (2016). Design and implementation of a reliable message transmission system based on MQTT protocol in IoT. Wireless Personal Communications, 91(4), 1765-1777

[4]. Kumar, A., & Singh, A. P. (2019). Malware Analysis and Tools: A Survey: International Research Journal Of Modernization In Engineering Technology And Science.

[5]. Singh, A. P. (2015, September). Improving the malware detection ratio using data mining techniques. In Second International Conference on Science, Technology and Management.

[6]. Singh, A. P. (2017). A study on zero day malware attack. International Journal of Advanced Research in Computer and Communication Engineering, 6(1), 391-392.

[7]. Singh, A. P. (2017). Ransomware: A high profile attack. International Research Journal of Engineering and Technology, vol 04, issue 02, https://irjet.net/archives/V4/i2/IRJET-V4I2365.pdf.