KnE Social Sciences

ICTSD 2018
International Conference on Technology for Sustainable Development 2018
Volume 2019

Knowledge E
enriching | engaging | empowering

Conference Paper

Data Transmission Frequency Effect on MQTT Protocol Under Syn Flooding Attack

Muhammad Arrofiq, Hidayat Nur Isnianto, Maun Budiyanto, and Y Wahyo S

Departement of Electrical and Information Engeenering, Vocational College Universitas Gadjah Mada

Abstract

Nowadays, the IoT implementations grow rapidly in most sectors. One of the challenges faced due to this growth is performance of implemented protocol under attack that aims to destroy the system performance. One of the popular IoT protocols is message queuing telemetry transport, MQTT. This research evaluates the performance of MQTT broker under syn flooding attack. The research variable implemented is data transmission frequency. The variation of data transmission frequency is operated in publisher. Publisher sends data to broker under attack. The three difference data transmission frequencies are set representing three different conditions, i.e. high, medium and low frequency. Results show that a pattern is obtained. The higher data transmission frequency is the lower number of packet loss is obtained.

Keywords: MQTT, syn flooding attack

Corresponding Author:
Muhammad Arrofiq
rofiq@ugm.ac.id

Received: 20 July 2019
Accepted: 22 August 2019
Published: 29 August 2019

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICTSD 2018 Conference Committee.

1. Introduction

The trend of devices connectivity shows an increase in business and industries. It starts from monitoring to data processing. It is implemented in agriculture, hospital, smart home, etc. The system reliability is one of the concerns of IoT implementation. The system reliability depends on several aspects. One of the aspect is transmission protocol. The example of several session layers on IoT protocols are message queuing telemetry transport (MQTT), secure MQTT (SMQTT), advanced message queuing protocol (AMQP), constrained application protocol (CoAP), Extensible messaging and presence protocol (XMPP) and data distribution service (DDS) (Salman & Jain, 2017). The MQTT, AMQP, XMPP and DDS employ TCP, while CoAP runs on UDP. The DDS also works on UDP. A comparison between CoAP and MQTT has been conducted in (World, 2018). MQTT implements a broker to receive data from publisher and send data to subscriber based on topic. A security issue happens in IoT as well due to attacker. The more the number connected devices means the more potential vulnerabilities are. Attacks to IoT now become worse (NG, 2018). Attention should be paid more on this issue. This research

investigates the effect of data transmission frequency to performance of MQTT broker under syn flooding attack.

2. Literature Review

The IoT developments face at least three main challenges i.e. technology, business and society (Banafa, Three Major Challenges Facing IoT, 2017). In terms of technology, it has at least 5 (five) aspects, i.e. security, connectivity, compatibility and longevity, standards and intelligent analysis and actions (Banafa, IoT implementation and Challenges, 2016). In security concern, attack to IoT system has high chance to disturb the IoT system performance. This threat leads to hamper (Abdul-Ghani, Konstantas, & Mahyoub, 2018). Syn flooding attack is one of most widely used method for large scale attack (Fehrenbach, 2018). It sends multiple syn message and is commonly called syn flooding attack. One of the attack scenario against MQTT protocol is sending multiple syn message. It can exhaust MQTT broker (Firdous, Baig, Valli, & Ibrahim, 2017).

3. Methods

This research is initiated by designing the model of experiment. The experiment setup needs several devices as follow:

1. Arduino Uno board,
2. Arduino Wifi module,
3. mini PC,
4. Notebook,

The experiment setup consists of the four parts as shown in Figure 1. The first part is a microcontroller based MQTT publisher which sends data continuously to MQTT broker. The data transmission frequency is set in the difference value of 10 Hz, 2 Hz, and 1 Hz separately. MQTT broker is the second part. MQTT broker receives data from publisher and sends data to MQTT subscriber. The broker operated is mini PC based in linux environment. The third part is MQTT subscriber. It subscribes data in certain topic to broker and receives data. It also provides data information to end user. The last part is a machine which plays as an attacker. It attacks the broker by sending syn flooding messages.

The experiment evaluates the MQTT broker performance. It is based on successfully data received by broker and subscriber.

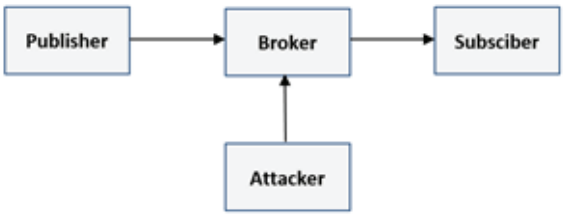

Figure 1: Block diagram of experiment.

4. Results and Discussions

The experiment varies the frequency of data transmission operated in publisher. The period of attack during test were 10s, 30s and 50s. Table 1 shows broker data comparisons between normal and under attack situations when data transmission frequency was 10 Hz. When broker is in normal condition, no attack injected, all the data packet sent by publisher is received by broker and subscriber. Under attack, for example in period of attack 10s, the number of data sent by publisher was 93 while data received by broker was 11. Finally the data received by subscriber was 6. Packet losses calculated from broker to subscriber was 45%. This condition is clear and caused by syn flooding attack. Syn flooding attack makes broker exhausted.

TABLE 1: Data comparison between normal condition and under attack when data transmission frequency was 10Hz.

Test and Attack Period (s)	No Attack			Under Attack		
	Nb. Data Packet Received by		Packet Loss (%)	Nb. Data Packet Received by		Packet Loss (%)
	Broker	Subscriber		Broker	Subscriber	
10	93	93	0	11	6	45
30	287	287	0	17	5	71
50	287	287	0	105	30	71

Table 2 and 3 show data comparisons between normal and under attack when data transmission frequencies were 2 Hz and 1 Hz respectively. The extreme condition happened when data transmission frequency was 1 Hz and period of attack was 30S. Subscriber did not receive data and packet loss was 100%.

TABLE 2: Data comparison between normal condition and under attack when data transmission frequency was 2Hz.

Test and Attack Period (s)	No Attack			Under Attack		
	Nb. Data Packet Received by		Packet Loss (%)	Nb. Data Packet Received by		Packet Loss (%)
	Broker	Subscriber		Broker	Subscriber	
10	19	19	0	9	1	89
30	59	59	0	15	2	87
50	98	98	0	19	3	84

TABLE 3: Data comparison between normal condition and under attack when data transmission frequency was 1Hz.

Test and Attack Period (s)	No Attack			Under Attack		
	Nb. Data Packet Received by		Packet Loss (%)	Nb. Data Packet Received by		Packet Loss (%)
	Broker	Subscriber		Broker	Subscriber	
10	9	9	0	2	1	50
30	29	29	0	10	0	100
50	50	50	0	8	0	100

5. Conclusion

As shown in the data and discussion for 3 different transmission frequency, syn flooding attack disturbs, in this case reduces the number of packet received by broker and subscriber. The lesser data transmission frequency is, the more packet losses.

Acknowledgement

We thank Zulfikar Alvin F, Della Vinka S, and Anggayasti Ariane Z for helping with data collection.

References

[1] Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 355-373.

[2] Banafa, A. (2016). *IoT implementation and Challenges*. Retrieved from Linked in: https://www.linkedin.com/pulse/iot-implementation-challenges-ahmed-

banafa?trk=mp-author-card

[3] Banafa, A. (2017, March 14). *Three Major Challenges Facing IoT*. Retrieved from iot.ieee.org: https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html

[4] Fehrenbach, P. (2018, 9 30). *Messaging Queues in the IoT under pressure*. Retrieved from https://blog.it-securityguard.com: https://blog.it-securityguard.com/wp-content/uploads/2017/10/IOT_Mosquitto_Pfehrenbach.pdf

[5] Firdous, S. N., Baig, Z., Valli, C., & Ibrahim, A. (2017). Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol. *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 748-755). IEEE.

[6] NG, A. (2018, 3 15). *IoT attacks are getting worse – and no one's listening*. Retrieved from www.cnet.com: https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/

[7] Salman, T., & Jain, R. (2017). A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications*, 1-20.

[8] World, R. W. (2018, 9 30). *COAP vs MQTT | Difference between COAP and MQTT protocols*. Retrieved from Home of RF and Wireless Vendors and Resources: http://www.rfwireless-world.com/Terminology/COAP-vs-MQTT.html