International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Energy Efficient and Secured MQTT Protocol using IoT

Selvi M., Gayathri A., Santhosh Kumar SVN, Kannan A.

Abstract: ***Internet of Things is a distributed collection of smart devices, where the smart device communicates with each other using Device to Device (D2D communication. Due to the resource constraint nature of IOT, the lightweight communication protocol is needed. Message Querying Telemetry Transport (MQTT) is one of the lightweight communication protocol which employs publish and subscribe method. The most of existing MQTT protocols are vulnerable to Denial of Service attack. In order to overcome the issues of the existing system, in this work a novel lightweight protocol by name EES-MQTT (Energy Efficient and Secured MQTT) is proposed which can be able to provide efficient authentication during data transmission by identifying the intruders and removing the malicious nodes. Moreover, the proposed protocol can be able to provide security with better energy optimization. The feasibility of EES-MQTT is carried out using MQTT.fx simulation tool and the Eclipse Paho. The results from the simulation proves that the EES-MQTT reduces impact of malicious nodes and optimizes the energy consumption during the data transmission.***

Keywords: Energy efficient and secured, light weight protocol, energy optimization, Message querying and telemetry transport.

I. INTRODUCTION

Internet of Things is a distributed collection of smart devices which can able to collect the data from the sensing domain and transmit the sensed information to other device using M2M communication with Internet as a backbone. Since the devices of IoT [16] is a resource constrained in nature, energy efficient secured communication is a major concern. There are various communication protocols which aims to provide 6LPWPAN (6 Low Power Wireless Private Area Network). Among them MQTT (Message Querying Telemetry Transfer) protocol aims at providing energy efficient communication. In IoT environment, the MQTT protocol [7] has three components namely publisher, broker and subscriber . Initially, in MQTT protocol, the subscriber are the set of devices which are willing to get the new data whenever it is updated. The subscriber module sends the request to the publisher module through a broker for requesting the transmission of new data upon receiving the request from the subscriber module, the publisher module validates the subscriber module and accepts the request. The major limitation in existing MQTT protocol is it is not secure and it is vulnerable to DoS attack [12] [13]. In order to overcome the limitation of existing MQTT protocol, in this paper a novel EES-MQTT(Energy Efficient and Secured Message Querying and Telemetry Transfer) protocol which can able to identify the malicious nodes impact by identifying them in IoT environment.

Revised Manuscript Received on February 28, 2020.

* Correspondence Author
Selvi M*, School of Computer Science and Engineering, VIT University, Vellore, India. selvi.m@vit.ac.in
Gayathri A., School of Computer Science and Engineering, VIT University, Vellore, India.
Santhosh Kumar SVN, School of Computer Science and Engineering, VIT University, Vellore, India.
Kannan A., School of Computer Science and Engineering, VIT University, Vellore, India.

II. LITERATURE SURVEY

The various mechanisms have been proposed by different authors for making MQTT protocol which is energy efficient [14], [15] and secured.

A. P. Haripriya et al [1] has developed a communication protocol which can able to detect the malicious behavior of the devices by using intelligent fuzzy rules. The advantages in their scheme are improvement of security for DoS attack. The limitations are energy optimization is not

D. Soni [2] et al describes the evolution and the importance of MQTT in IoT, the generic architecture of MQTT, numerous possible domains where MQTT is mostly used, various brokers used by MQTT with their limitations and features and current issues that are to be addressed.

B. S. Ullas et al [3] has designed a MQTT client protocol for the smart home and industry automation system. The proposed protocol employs publish – subscribe method to communicate among the other devices. The limitations are security is not considered in their design.

Atmoko et al [4] has done a comparative analysis of MQTT protocol with standard Hyper Text Transport Protocol HTTP for communication among the devices in IOT environment. The results of comparative analysis shows that the data transfer rate of MQTT protocol performs better than HTTP protocol. The limitations are MQTT protocol is vulnerable to various security attacks.

S. Pal et al [5] had attempted to study one such Internet protocol which makes such a communication possible, the MQTT protocol. In their study, Environmental monitoring system, transmit the sensor data and then use the same data to control electronic devices. The MQTT protocol is compared with the traditional HTTP protocol and attempt to find out which protocol is the better one. MQTT protocol used to comparison result shows that MQTT protocol performs better.

M. V. Masdani et al [6] has carried out a comparative analysis based on energy consumption for MQTT protocol and other IOT communication protocols. Comparison study reveals that MQTT protocol performs better than other existing protocols.

Shaout et al [8] designed an embedded based cloud system. In their system, the connection establishment of embedded system and cloud server is done using MQTT protocol. The limitations of their scheme is security is not considered in their design.

S. Hernández Ramos et al [9] has designed a lightweight MQTT protocol for establishing a communication among the IOT devices. The proposed system exchange the data by identifying the optimal path among the devices by using template based fuzzy rules. The limitations are lack of security in their design.

D.Guha [10] has proposed a secured IOT protocol for ensuring security in transport layer. The proposed protocol uses value based HMAC technique to ensure data confidentiality and data integrity in the network. The limitations are protocol suffers from communication and computational overheads.

III. PROPOSED S-MQTT PROTOCOL

The proposed S-MQTT protocol consists of four phases namely, Data generation phase, data transmission phase and data reception phase. The detailed explanation for the various phases are explained as follows.

A. Key generation phase:

In this phase, two keys are generated by the publisher and the broker. One is public key and another is the private key. In this process the non-inverted prime numbers enhance the security of the system by the means of confusion and diffusion. The keys are generated by both the publisher and the broker modules to make the transmission of the data module to more secure for the subscriber. The algorithm for publisher key generation is given as follows.

B. Publisher key generation Algorithm

1. Choose two random prime numbers p, q where $p \neq q$.
2. Choose r, s $\in$ G where G is the generator function.
3. Choose v, u $\in z^*p$
4. Subscriber Public key (SPuK)

   SPuK = R^vmod (1)

5. Subscriber Private key (SPrK)

   SPrK = S^u mod q (2)

The Equation (1) and (2) gives the subscriber generated public key and private key.The algorithm for broker key generation phase is given as follows.

C. Broker key generation.

1. Choose two random prime numbers x, y.
2. From the generator, choose two random elements e, f $\in$ G.
3. Choose g, h from z^*y where z^*y is the set q non-invertible functions.
4. Broker public key = $e^{x(g)}$ mod p (3)

Broker private key = $y^{f(h)}$ mod q. (4)

5. Total public key = Subscriber Public key + Broker Public Key= r^v mod p + $e^{x(g)}$ mod p

TPuK = r^v mod p + $e^{x(g)}$ mod p (5)

6. Total private key = Subscriber Private key + Broker Private Key= s^v mod q + $e^{x(h)}$ mod q

TPrK = s^v mod q + $e^{x(h)}$ mod q (6)

The Equation (5) and (6) gives the total public and private key which has been generated by both publisher and Subscriber

B. Data generation phase:

In data generation phase, the publisher first identifies the registered subscribers in that network.

Once the subscribers of the network is detected, the publisher broadcasts the ID of the publisher module so that the subscribers can subscribe to that publisher by using their subscriber IDs.

S_M = Subscriber Module

1. For all S_M register with P_M with the IDs.
2. P_M checks the validity of S_M in the network.
3. IF the validity of S_M found correct P_M accepts the registration of $S_{M.}$

   ELSE

   Request for S_M registration is declined.

Subscribe to a particular topic

1. For all $S_{M,}$ P_M broadcasts the topic which they are likely to subscribe.
2. S_M based on the integrity of the topic, gives the subscription to the publisher module.
3. D be the data generated by the $P_{M.}$
4. IF new version of data <= Previous version of data, THEN S_M accepts the new data items in the topic

ELSE

S_M discards the data items in topic.

C. Data transition phase:

In this phase, the data is transferred from the publisher to the broker in much secured manner. The publisher send the private key to the broker with the time stamp so that the broker should open the key within the given time stamp. This is done by using the hash function applied to the data.

1. Initially the data is sent to the B_M by the P_M with its private key ie) Encryption.
2. $P_{Pr}K$ || h(data) || $B_{M.}$
3. Broker module authenticates the $P_{Pr}K$ of the P_M and encryptes the data sent to the subscribed $S_{M.}$
4. $P_{Pr}K$ || h(data) || $B_{M.}$ IF the validation of $P_{Pr}K$ is found correct, THEN

   $B_{Pr}K$ || h(data) || t || $S_{M.}$

D. Data reception phase:

The data transfer from the broker to the subscriber who has subscribed to the title. The broker sends the private key to the subscriber so that the publisher can easily identify the subscribed subscribers of that publisher in the network in a more secured manner. If the key does not match with the subscriber then the subscriber declines the data packets sent by the publisher.

1. For all S_M present in the network, S_M validates the B_M with its public key ie)

$B_{Pu}K$ || h(data) || t || $S_{M.}$

2. IF validation of $B_MP_{Pr}K$ of the time stamp is found correct,
   THEN S_M accepts the data
ELSE
 The data will not be received.

IV. EXPERIMENTAL SETUP AND SIMULATION PARAMETERS

The feasibility of proposed protocol is implemented by using MQTT.fx. The simulation parameters for implementing this protocol is given in table1.

Table 1. Simulation Parameters

Network simulator	MQTT.fx version 1.7.1
Simulation_ area	1000 M
Nodes _ density	500
Transmission_ range	50m
Node initial energy	100J
Simulation period	90 minutes
Number of rounds	70
Packet_ size	100 bytes

V. RESULTS AND DISCUSSIONS

The performance of S-MQTT protocol is evaluated by using the performance metrics like device energy consumption, network life time, packet delivery ratio.

A. Node Energy Consumption

Figure1 gives comparison of S-MQTT with MQTT protocol from the graph it is clear that S-MQTT protocol has better node energy consumption when it is compared with the MQTT protocol.

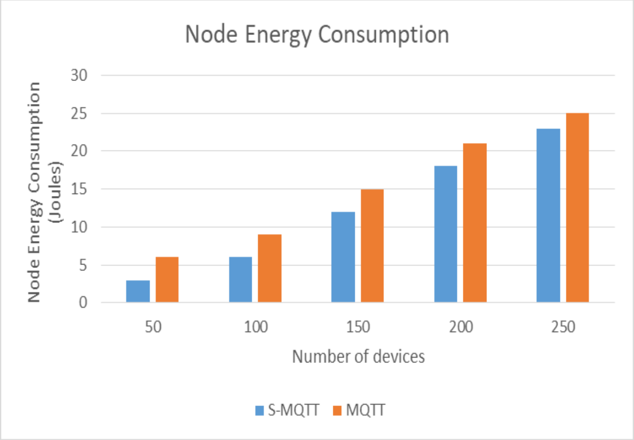

Figure 1 Node Energy consumption

The reason is that S-MQTT protocol, identifies the malicious nodes during the data transmission. By doing so, it reduces the impact of malicious nodes in terms of packet drop. Hence the proposed protocol has better packet delivery ratio when it is compared with MQTT.

B. Node Life time

Figure2, gives the comparison of node life time for S-MQTT and MQTT protocol. The protocol eliminates and identifies the malicious nodes and reduces their impact. Hence the re-transmission or dropped packets has been reduced considers. Hence, the proposed MQTT protocol has better node life time compared with MQTT.

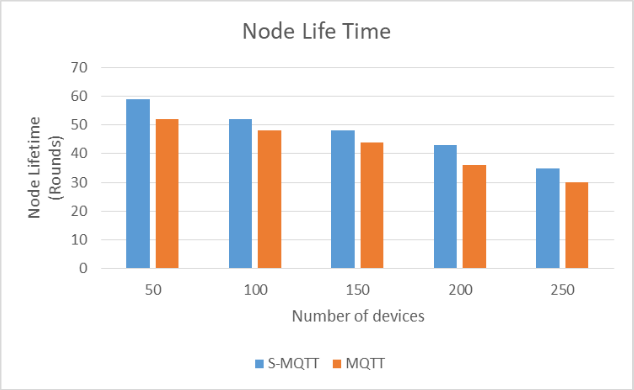

Figure 2 Node life time

C. Packet delivery ratio

Figure3, gives the comparison of packet delivery ratio for S-MQTT and MQTT protocol.
The protocol eliminates and identifies the malicious nodes and reduces their impact. Hence the re-transmission or dropped packets has been reduced considers. Hence, the proposed MQTT protocol has better packet delivery ratio compared with MQTT.

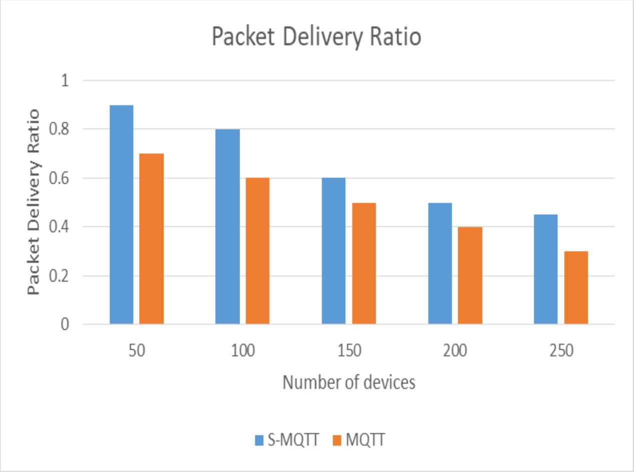

Figure 3 Packet delivery ratio

VI. CONCLUSION AND FUTURE WORK

In this paper, a novel S-MQTT protocol has been proposed for providing reliable secured data transmission in IoT environment. The proposed S-MQTT protocol is implemented in MQTT.fx tool. The simulation results justify that proposed protocol has optimized energy consumption and has better packet delivery ratio compared with MQTT protocol. The scope for future work is to make S-MQTT protocol more lightweight and reliable.

REFERENCES

1. A. P. Haripriya and K. Kulothungan, “Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, 2019.
2. D. Soni and A. Makwana, “A survey on mqtt: a protocol of internet of things(IoT),” *Int. Conf. Telecommun. Power Anal. Comput. Tech. (Ictpact - 2017)*, no. April, pp. 0–5, 2017.
3. B. S. Ullas, S. Anush, J. Roopa, and G. R. M, “Machine to Machine Communication for Smart Systems using MQTT,” *Int. J. Adv. Res. Electr. Electron. Instrum. Energy*, vol. 2014, pp. 8242–8248, 2015.
4. R. A. Atmoko, R. Riantini, and M. K. Hasin, “IoT real time data acquisition using MQTT protocol,” *J. Phys. Conf. Ser.*, vol. 853, no. 1, 2017.
5. S. Pal, S. Ghosh, and S. Bhattacharya, “Study and Implementation of Environment Monitoring System Based on MQTT,” *Environ. Earth Sci. Res. J.*, vol. 4, no. 1, pp. 23–28, 2017.
6. M. V. Masdani and D. Darlis, “A comprehensive study on MQTT as a low power protocol for internet of things application,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 434, no. 1, pp. 0–7, 2018.
7. J. E. Luzuriaga, J. C. Cano, C. Calafate, P. Manzoni, M. Perez, and P. Boronat, “Handling mobility in IoT applications using the MQTT protocol,” *2015 Internet Technol. Appl. ITA 2015 - Proc. 6th Int. Conf.*, no. December 2016, pp. 245–250, 2015.
8. A. Shaout and B. Crispin, “Using the MQTT protocol in real time for synchronizing IoT device state,” *Int. Arab J. Inf. Technol.*, vol. 15, no. 3A Special Issue, pp. 515–521, 2018.
9. S. Hernández Ramos, M. T. Villalba, and R. Lacuesta, “MQTT Security: A Novel Fuzzing Approach,” *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.
10. D. Guha Roy, B. Mahato, D. De, and R. Buyya, “Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT) — MQTT-SN protocols,” *Futur. Gener. Comput. Syst.*, vol. 89, pp. 300–316, 2018.
11. F. Jerald, M. Anand, and N. Deepika, “Design of an Industrial IOT Architecture Based on MQTT Protocol for End Device to Cloud Communication,” no. 6, pp. 552–554, 2019.
12. SVN santhosh kumar, Yogesh Palanichamy, Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN, wireless networks, 24 (4), pp 1343-1360, 2018.
13. Rakesh Rajendran, SVN Santhosh Kumar, Yogesh Palanichamy, Kannan Arputharaj, “Detection of DoS attacks in cloud networks using intelligent rule based classification system”, 22 (1),pp 423-434, 2019.
14. M Selvi, K Thangaramya, Ganapathy Sannasi, K Kulothungan, H Khannah Nehemiah, A. Kannan, “An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks”, Wireless Personal Communication, Springer, Vol. 105, no.4 pp. 1475-1490, 2019.
15. Santhosh Kumar SVN, M. Selvi, A Gayathri, Ruby D, A Kannan, “Energy Efficient Rule based intelligent routing using Fitness Functions in Wireless Sensor Networks”, international Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol 8 (12),PP.5414-5420.
16. K Thangaramya, K Kulothungan, R Logambigai, M Selvi, Sannasi Ganapathy, A Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT", Computer Networks, Elsevier, vol. 151, pp.211-223.