A MQTT-Based Zero-Knowledge Authentication Algorithm for Internet of Things Networks

Yao-Jen Liang[1], You-Jhen Lin[1], Fang-Chang Kuo[1], Chih-Cheng Tseng[2], Tung-Tsun Lee[1]*

[1] Department of Electronic Engineering, National Ilan University, Taiwan
[2] Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan
{yaojen, r1042011, kfc, tsengcc, ttlee}@niu.edu.tw

Abstract

Message Queuing Telemetry Transport (MQTT) is a widely used lightweight standard for the Internet of Things (IoT) and IoT applications. It offers some advantages such as minimal control message overhead, a concise publish/subscribe mechanism, reduced computational requirements, low transmission latency, and low power consumption for resource-constrained devices. However, MQTT itself just provides limited security-related functionalities, message security can only be ensured by configuring Transport Layer Security (TLS). Nonetheless, the computation resources and transmission latency required for TLS encryption may impose a burden on these devices. This paper proposes ZK-MQTT, an identity authentication mechanism for resource-constrained devices in IoT. It combines Zero Knowledge Proof (ZKP) and Diffie-Hellman key exchange (DHKE) to achieve low computational requirements, low transmission latency, device authentication, and encryption. The proposed ZK-MQTT utilizes an access control memory (ACM) for authorization and authentication, allowing only authorized devices to access the broker service. The proposed method effectively authenticates connecting devices and prevents malicious connections. Experimental results show that our method reduces authentication time by 11% compared to ZKP with Schnorr signature-based framework. By leveraging the allowance of device ID validation and anonymous device access, the proposed method is suitable for service scenarios that require low authentication time and/or anonymous device access.

Keywords: Zero Knowledge Proof, Authentication, Message Queuing Telemetry Transport (MQTT), Internet of Things (IoT)

1 Introduction

IOT, which is a promising future network paradigm that enables communication among heterogeneous smart devices, has raised the question of implemented technology security. The main difference of the equipment used in the IoT from the conventional one is that it is capable of making decisions based on the input data and the communications linkage via the Internet, although it has limitations in computational performance and energy storage of the independent power supply source [1]. Several protocols such as Message Queuing Telemetry Transport (MQTT) [2], Constrained Application Protocol (CoAP) [3], Extensible Messaging and Presence Protocol (XMPP) [4], and Advanced Message Queuing Protocol (AMQP) [5] are introduced to transfer the message in the IoT network. Compared to CoAP, XMPP, and AMQP, MQTT leverages its lightweight characteristic to work efficiently in low-power, limited memory devices.

MQTT brokers are considered the main service providers to the clients of any IoT-based applications [6], while they lack basic security functionalities such as access control, and mutual authentication. The only security functionality provided in MQTT standard is unilateral authentication based on pre-shared key/password [7]. To bridge this gap of security functionalities, current implementations of MQTT suggested transport layer security (TLS) for providing a secure channel between each client and MQTT broker. Fremantle et al suggested employing the OAUth2 protocol to enforce the MQTT security [8]. [9] further implemented MQTT-TLS profile authentication and authorization scheme employing the OAUth2 tokens. In [10], the authors suggested an M2M authentication scheme where a device graph with media access control (MAC) addressed was created as the key field based on zero knowledge algorithm. Another multi-graph zero knowledge-based authentication scheme for IoT was suggested in [11]. The authors in [12] presented a different approach to authentication based on asymmetric encryption on elliptic curves. However, the computation of this approach is labor and resource intensive. In [13], the authors proposed to use password authentication scheme for M2M communications on the application level. This scheme is based on one-way hash functions, exclusive-OR (XOR) operations and a symmetric encryption procedure with two request-response cycles. [14] presented a lightweight algorithm for M2M authentication by leveraging an authority center to authenticate the device and the gateway between each other. Furthermore, the authors in [15] developed an MQTT-integrated secure authentication scheme for M2M communication in a single request-response cycle by generating a common session key for asymmetric encryption. This allows it to use authentication through the MQTT protocol and makes

*Corresponding Author: Yao-Jen Liang; Email: yaojen@niu.edu.tw
DOI: https://doi.org/10.70003/160792642026112706004

it compatible with the existing systems without disturbing their functionalities. However, the scheme in [15] lacks the differentiation of devices (clients) to allow devices with different access modes for subscribing different security-sensitive topics. [18] proposed security architecture and protocols to bootstrap MQTT security in the wireless sensor network and showed its capability to enhance MQTT security. [7] proposed making a security schema in MQTT protocol using Cryptographic Smart Cards, for the authentication schema, the trusted data confidentiality, and data integrity, because MQTT-TLS is not possible in most lightweight devices that make up the IoT ecosystem. Furthermore, a survey contribution [19] reviewed attacks against the MQTT protocol and the corresponding defense mechanisms for identifying vulnerabilities, detecting and preventing attacks.

In this paper, a novel lightweight authentication scheme is proposed for MQTT-based IoT applications based on zero knowledge algorithm. Its main difference from the mentioned algorithms is that it can not only authenticate in a single request-response cycle but also identify anonymous accesses and network anomalies. The major contributions of this paper are:

1) The proposed secure ZK-MQTT identifies the anonymous and malicious behavior of the publish-subscribe nodes of the MQTT protocol in the IoT networks.
2) Subsequently, a novel lightweight authentication scheme based on zero-knowledge algorithm is developed to allow authentication in a single request-response cycle.
3) Finally, the proposed ZK-MQTT is validated and verified under varying network scenarios.

The organization of this paper is as follows. Section 2 reviews the fundamental concepts of MQTT and ZKP. Section 3 describes the proposed algorithm, followed by the numerical results in Section 4. Section 5 concludes the paper.

2 Background

Before stepping into the proposed algorithm, we review MQTT and Zero-Knowledge Proof (ZKP) in the following.

2.1 MQTT Overview

Two MQTT standardized versions exist, namely version 3.1.1 [2] and version 5 [16]. In MQTT, the server, a.k.a. broker, is responsible for relaying messages between clients using persistent TCP-based connections. Clients connect to the broker using a CONNECT message. After connection established, clients publish or subscribe to 'topics' hosted by the broker. As the broker receives a PUBLISH message, it forwards the message to all clients subscribed to the topic. To subscribe to topics, clients send SUBSCRIBE messages containing topic information.

For the security issues, version 3.1.1 supports optional username/ password-based authentication of clients, provided in the CONNECT packet. MQTT version 5 addresses a set of limitations of version 3.1.1 and also has more support for security. Two new authentication fields are introduced in the CONNECT packet: Authentication Method and Authentication Data. With these, a client can signal to the broker which authentication method to use and can provide different types of authentication data (apart from username and password). Additionally, version 5 supports a new AUTH packet that can be used to extend the authentication phase, such as to add a challenge, or to re-authenticate.

2.2 Zero Knowledge Proof (ZKP) Overview

The Zero-Knowledge Proof is a concept used in many cryptography systems [17]. It allows a party to prove that he/she knows something (i.e. credential), without having to send over the value of the credential. ZKP has the following properties:

- Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true to an honest verifier every time.
- Soundness: if the statement is false, it is not possible (with a very small chance) to fake the result to the verifier that the statement is true.
- Zero-knowledge: if the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed.

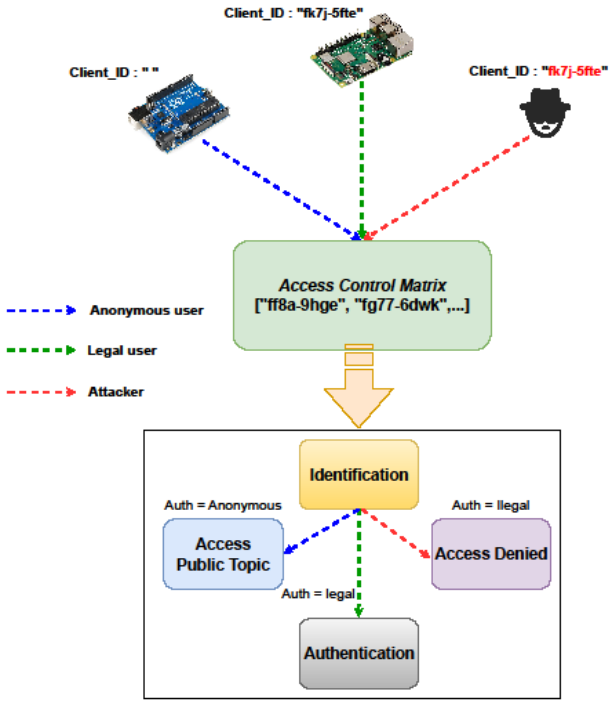

Figure 1. ZK-MQTT identification architecture

3 Proposed Algorithm

MQTT is widely used in application layer to transmit data among the devices in IoT due to its simplicity and scalability [6], wherein the publisher, subscriber,

and broker are the basic elements for accomplishing communication between the IoT devices. For example, the publisher device sends a MQTT request message, CONNECT, to connect with the broker. Then, the broker will send the acknowledgment, CONNACK, to the sending device once the request is received. Subsequently, the publisher sends the message with a particular topic to the broker, and the subscriber or receiver device subscribes to the topic and receives the messages from the broker.

The authentication procedure of the proposed ZK-MQTT is mainly divided into two parts. The first part is identification, and the second part is authentication. The so-called identification refers to determining whether the registering device is anonymous, legitimate, or illegitimate and what is the next step to take. While authentication refers to having legitimate devices authenticate after identification. The identification architecture is shown as in Figure 1. In this figure, an access control memory (ACM) is added for device identification through querying, adding a new legitimate device, and deleting an illegitimate one. In the sequel, the anonymous devices are permitted to subscribe public topics, the illegitimate is refused to subscribe to topics, while the legitimate device will go to the authentication procedure. In the following, we detail the above two procedures.

3.1 Identification

The used notations are listed in Table 1.

In our proposed ZK-MQTT, each end device has to perform the registration procedure. The device provides its device ID to the MQTT broker. Then the broker calculates the token, F as

$$F = H(H(ID) \oplus H(psk)) \tag{1}$$

where H() is the hash function of SHA256. The broker then checks whether the received ID is empty? If "yes", the broker sets the "auth" field as "anonymous" and sends it to the device; else, the broker looks for the ID in ACM to see if it already exists. If not, it will add the device ID into ACM, and set "auth" to "User" and send it with the secret token F to the device. If the device ID already appears in ACM, the broker checks whether there is a legitimate device connection to it. If "yes", it means that a duplicate device is found trying to connect, this new connection request will be regarded as a Session Hijacking attack and will be directly refused, the procedure flow chart is shown in Figure 2.

Table 1. Notations

Symbol	Description
p	prime number
q	primitive divider of p
pwd	A client's password as a combination of symbols
ID	device's ID
H()	one-way hash function
$\|\|$	concatenation operator
$\oplus$	exclusive-OR operator
mod	modulus operator
auth	identity of device
F	an unique token for a device
psk	pre-shared key
PK	server's public key
SK	server's private key
E	random large number

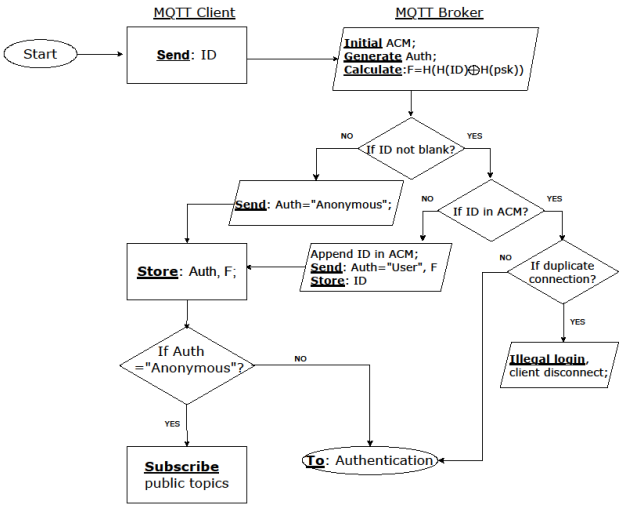

Figure 2. Identification procedure

3.2 Authentication

Here we present a two-way authentication scheme, that is, authentication at both the client side and the broker side, as shown in Figure 3. The client or device has F, Y values and public g, p, psk values. To pass the authentication procedure the client generates a large random number E[1] and calculates:

$$X = H(pwd) \tag{2}$$

$$Y = g^X \bmod p \tag{3}$$

$$M = H(pwd) \oplus H(psk) \tag{4}$$

$$N = H(F \| Y \| H(psk)) \tag{5}$$

where M and N are two session keys by using F, Y. Next, the device sends a CONNECT message with the ID value into the username field and values E, M, N into the password field. The data about the client identifier is always sent in the variable header of the CONNECT message of the MQTT protocol, thus there is no necessity in information repeating, but the presence of the hash value M, N conclusively verifies the message with the device.

After the broker receives the CONNECT message, it finds the device by username and calculates the public PK

[1] A larger E can achieve a more secure authentication, however, there is a trade-off between complexity and security.

by using the stored private key SK as:

$$A = g^K \bmod p \tag{6}$$

$$S = (K + SK \cdot E) \bmod (p-1) \tag{7}$$

$$PK = g^{SK} \bmod p. \tag{8}$$

For the client, it must identify the broker. This can be accomplished by sending a message from the broker to the client. But a CONNACK message of the MQTT protocol does not have any field to input additional data. The CONNACK message has limited size fields in the fixed and variable headers, each of them is no more than a few bits. The payload field is missing. Thus, this type of message is incompatible as a data transmitter. To accomplish the broker approval on the client, an additional header is attached to the first message from the broker to the client that contains a payload field.

After receiving the first message from the broker, the client then check the validity of values A and S according to the equation:

$$W = g^S \bmod p = (A \cdot (PK^E \bmod p)) \bmod p = T. \tag{9}$$

Subsequently, the broker authenticates the client in a similar way. It calculates the hash value based on the saved value M, N and check if R = N according to:

$$L = (M \oplus H(psk)) \bmod (p-1) \tag{10}$$

$$Z = g^L \bmod p \tag{11}$$

$$R = H\left(F \| Z \| H\left(psk\right)\right). \tag{12}$$

Comparing to the TLS protocol, the proposed authentication algorithm takes place during request-response cycles, there is no need for a third party. Comparing to the method in [15], the proposed two-way authentication scheme gets rid of time stamps, and makes it more robust to variant transmission delay. The detailed comparison between the mechanism in [15] and the proposed one is listed in Table 2.

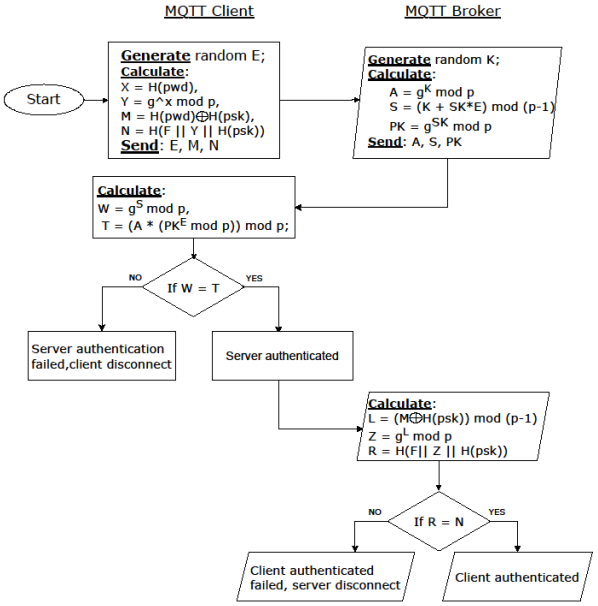

Figure 3. Authentication procedure

Table 2. Comparison of mechanisms

Mechanism	Encrypted algorithm	Computational complexity	Time synchronization	Verify invalid client ID	Prevention against MITMA
[15]	ZKP+Schnorr	O(5n + 2 log p)	yes	no	yes
Proposed	ZKP+DHKE	O(5n + 2 log p)	no	yes	yes

4 Experiment Results

In this section, the performance and time consuming are evaluated through a practical MQTT-IoT experimental network.

4.1 Experiment Network

The experiment network is shown as in Figure 4, wherein a MQTT client, a MQTT broker, and a gateway is considered. At the MQTT client, the paho-mqtt package in the Python Package Index (PyPI) is used for sending and receiving messages in MQTT communication. While at the broker, an Ubuntu virtual machine is deployed and Eclipse Mosquitto server software is used. Then the simulated data is upload to the chain by ShimmerEVM API. We also make the following assumptions in our experiments:

1) The sizes of all sensing data transmitted from the clients are the same.
2) All MQTT client devices have the same computing capabilities.
3) Data transmission is performed within the local network (except data uploading to the chain).
4) Each connection request is processed by a thread, so there is no order issue.

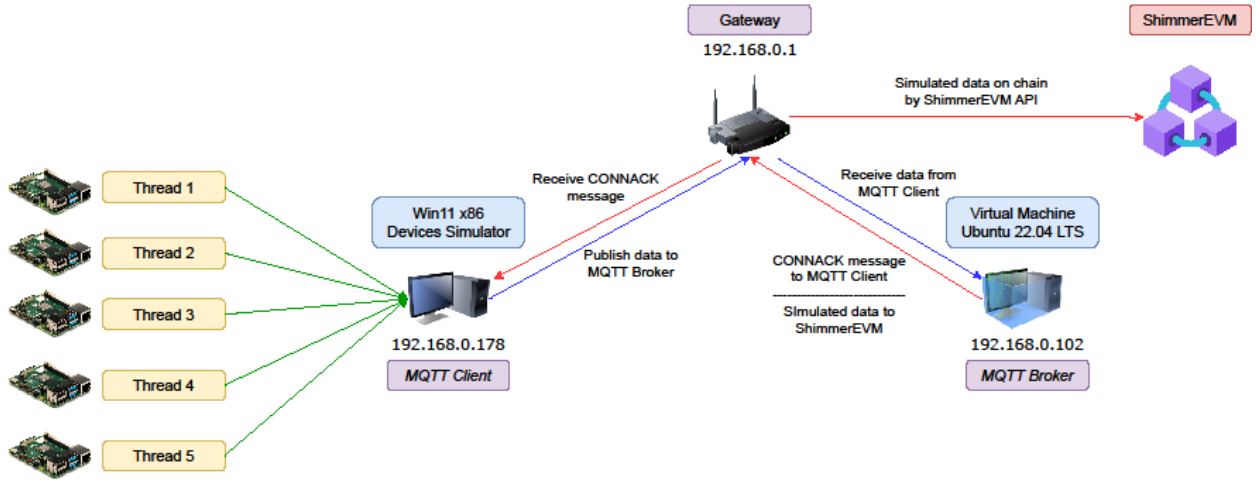

Figure 4. Experiment environment

4.2 Results and Discussion

Here we compare the authentication time and total MQTT transmission time consumption among the following four schemes: TLS encrypted MQTT over TCP, TLS encrypted MQTT over websocket, ZK-MQTT over TCP [15], and the proposed ZK-MQTT over TCP.

From Figure 5, one can find that the consumed authentication time of our proposed improved ZK-MQTT scheme and Dikkii's ZK-MQTT scheme [15] increases with the increase of the number of iterations. Although the consumed time of the proposed and Dikkii's ZK-MQTT is lower than that of the other two TLS encrypted MQTT methods, the consumed time of the latter two methods is relatively stable and not affected by the number of iterations. The main reason for this is that our method and the method in [15] both publish the authentication contents on a subscribed topic. As the number of iterations increases, the message content in the topic increases accordingly. If there is no appropriate restriction on the survival time of the Retained Message, it will lead to too much message content in the same topic, and consequently the processing speed of the MQTT broker slows down, resulting in an increase in authentication time.

In Figure 6, the transmission time of MQTT packets (messages) is compared among the four methods. It is shown that MQTT-TLS over Websocket consumes the most time due to the packets transferring to HTTP format. Comparing the consumed time of the proposed scheme with the other three methods, our proposed ZK-MQTT scheme saves about 53% to MQTT-TLS over websocket, 9% to MQTT-TLS over TCP, and 5% to Dikkii's ZK-MQTT. It is noteworthy that identification and authentication are considered in our proposed ZK-MQTT, while other functions like parameter negotiation and certificate exchange, provided by TLS, would not be addressed here.

Finally, the resource utilization comparison among these four methods is listed as in Table 3. The memory usage of the proposed method is slightly reduced by 4 MB compared to MQTT-TLS over Websocket, by 2.1 MB compared to MQTT-TLS over TCP, and by 0.2 MB compared to that of [15].

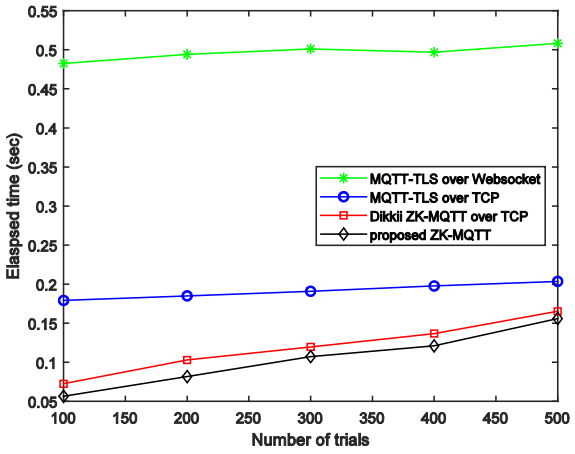

Figure 5. Authentication time comparison among 4 considered methods

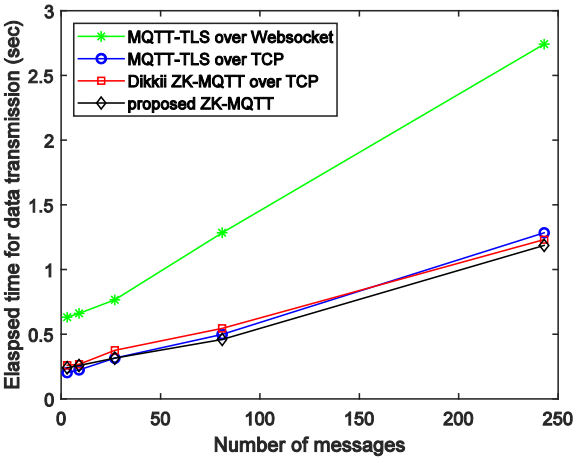

Figure 6. Comparison of transmission time

Table 3. Resource utilization comparison

Authentication methods	Normalized memory %	VIRT	RES
MQTT-TLS over Websocket	0.1	13.7 MB	23.2 MB
MQTT-TLS over TCP	0.1	11.7 MB	21.3 MB
Dikkii's ZK-MQTT over TCP	0.1	11.4 MB	19.3 MB
Proposed ZK-MQTT over TCP	0.1	11.2 MB	19.1 MB

5 Conclusion

This paper proposes an improved identification and authentication algorithm based on ZKP and DH key exchange. The consumed time for authentication and for MQTT transmission is similar to the results in [15], even slightly better than the original architecture. Under conditions similar to the above results, the proposed algorithm can additionally check whether the device ID is a valid value or an interrupt malicious connection during the identification stage, and allow anonymous devices to subscribe public or non-sensitive services. We also propose a way to upload data to ShimmerEVM with reduced verification time. The integration with emerging technologies, such as Artificial Intelligence (AI) and blockchain, would be left for our future research.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, *Computer Networks*, Vol. 54, No. 15, pp. 2787–2805, October, 2010.
https://doi.org/10.1016/j.comnet.2010.05.010

[2] A. Bank, R. Gupta, Mqtt version 3.1.1, *OASIS Standard*, October, 2014.
https://www.oasis-open.org/standard/mqttv3-1-1/

[3] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (coap), RFC 7252, June, 2014.
https://www.rfc-editor.org/info/rfc7252/

[4] H. Lampesberger, Technologies for web and cloud service interaction: a survey, *Service Oriented Computing and Applications*, Vol. 10, No. 2, pp. 71–110, June, 2016.
https://doi.org/10.1007/s11761-015-0174-1

[5] S. Vinoski, Advanced message queuing protocol, *IEEE Internet Computing*, Vol. 10, No. 6, pp. 87–89, November-December, 2006.
https://doi.org/10.1109/MIC.2006.116

[6] H. A. P., K. K., Secure-mqtt: an efficient fuzzy logic-based approach to detect dos attack in mqtt protocol for internet of things, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, Article No. 90, April, 2019.
https://doi.org/10.1186/s13638-019-1402-8

[7] E. B. Sanjuan, I. A. Cardiel, J. A. Cerrada, C. Cerrada, Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach, *IEEE Access*, Vol. 8, pp. 115051-115062, June, 2020.
https://doi.org/10.1109/ACCESS.2020.3003998

[8] P. Fremantle, B. Aziz, J. Kopecky, P. Scott, Federated identity and access management for the internet of things, *2014 International Workshop on Secure Internet of Things*, Wroclaw, Poland, 2014, pp. 10-17.
https://doi.org/10.1109/SIoT.2014.8

[9] M. Michaelides, C. Sengul, P. Patras, An experimental evaluation of mqtt authentication and authorization in iot, *15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, New Orleans, LA, USA, 2021, p. 69–76.
https://doi.org/10.1145/3477086.3480838

[10] M. Schukat, P. Flood, Zero-knowledge proofs in m2m communication, *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies* (*ISSC 2014/CIICT 2014*), Limerick, Ireland, 2014, pp. 269–273.
https://doi.org/10.1049/cp.2014.0697

[11] I.-H. Chuang, B.-J. Guo, J.-S. Tsai, Y.-H. Kuo, Multi-graph zero-knowledge-based authentication system in internet of things, *2017 IEEE International Conference on Communications (ICC)*, Paris, France, 2017, pp. 1–6.
https://doi.org/10.1109/ICC.2017.7996820

[12] M. Singh, M. A. Rajan, V. L. Shivraj, P. Balamuralidhar, Secure MQTT for Internet of Things (IoT), *5th International Conference on Communication Systems and Network Technologies*, Gwalior, India, 2015, pp. 746–751.
https://doi.org/10.1109/CSNT.2015.16

[13] K. M. Renuka, S. Kumari, D. Zhao, L. Li, Design of a secure password-based authentication scheme for m2m networks in IoT enabled cyber-physical systems, *IEEE Access*, Vol. 7, pp. 51014–51027, April, 2019.
https://doi.org/10.1109/ACCESS.2019.2908499

[14] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, J. Bastos, A lightweight authentication mechanism for m2m communications in industrial iot environment, *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp. 288–296, February, 2019.
https://doi.org/10.1109/JIOT.2017.2737630

[15] D. Dikii, Authentication Algorithm for Internet of Things Networks Based on MQTT Protocol, *Serbian Journal of Electrical Engineering*, Vol. 17, No. 3, pp. 389–403, October, 2020.
https://doi.org/10.2298/SJEE2003389D

[16] A. Banks, E. Briggs, K. Borgendale, R. Gupta, MQTT version 5.0, *OASIS Standard*, March, 2019.
https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[17] S. Goldwasser, S. Micali, C. Rackoff, The Knowledge Complexity of Interactive Proof-Systems, in *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, Providence, Rhode Island USA, 1985, pp. 291–304.
https://doi.org/10.1145/22145.22178

[18] C.-S. Park, H.-M. Nam, Security Architecture and Protocols for Secure MQTT-SN, *IEEE Access*, Vol. 8, pp. 226422-226436, December, 2020.
https://doi.org/10.1109/ACCESS.2020.3045441

[19] S. Lakshminarayana, A. Praseed, P. S. Thilagam, Securing the IoT Application Layer from an MQTT Protocol Perspective: Challenges and Research Prospects, *IEEE Communications Surveys & Tutorials*, Vol. 26, No. 4, pp. 2510-2546, 4th quarter, 2024.
https://doi.org/10.1109/COMST.2024.3372630

Biographies



Yao-Jen Liang received the Ph.D. degree in communication engineering from National Taiwan University, Taiwan, in 2010. He is currently an associate professor with the department of electronic engineering, National Ilan University. His current research interests include wireless communications and statistical signal processing.



You-Jhen Lin received the B.S. and the M.S. degrees in electronic engi-neering from National Ilan University, Taiwan, in 2021 and 2023. He is currently working as an IT engineer in the semiconductor manufacturing industry under Taiwan Semicon-ductor Manufacturing Company (TSMC) Group. His research interest focuses on network engineering and information security.



Fang-Chang Kuo received the B.S. and Ph.D. degree in electrical engineering from Tatung University in 1986, and from National Central University, Taiwan, in 1997, respectively. He is currently a professor with the department of electronic engineering, National Ilan University. His research interests are in the areas of communication networks and wireless communications.



Chih-Cheng Tseng received his Ph.D. degree from the Graduate Institute of Communications Engineering, National Taiwan University, in 2007. He is currently a professor of the department of computer science and engineering, National Taiwan Ocean University. His research interests include the design and performance evaluation of the next generation mobile communication technologies.



Tung-Tsun Lee received the B.S. and M.S. degrees in computer science and engineering from National Chiao Tung University, Taiwan, in 1983 and 1985, respectively. Since 1992, he has been a lecturer with the department of electronic engineering, National Ilan University, Taiwan. His research interests include security, image processing and computer networks.