A Secure Secret Key-Sharing System for Resource-Constrained IoT Devices using MQTT

Taku NOGUCHI *, Masato NAKAGAWA **, Masami YOSHIDA **, Alberto Gallegos RAMONET***

**College of Information Science and Engineering,*
Ritsumeikan University, Shiga, Japan
*** Graduate School of Information Science and Engineering,*
Ritsumeikan University, Shiga, Japan
**** Graduate School of Technology, Industrial and Social Sciences Tokushima University, Tokushima, Japan*

noguchi@is.ritsumei.ac.jp, is0318kh@gmail.com, is0195hr@ed.ritsumei.ac.jp, alramonet@is.tokushima-u.ac.jp

***Abstract*— The MQTT (Message Queue Telemetry Transport) protocol has garnered significant attention as a communication protocol for a variety of IoT applications. Although it is a lightweight and energy-efficient communication protocol, it is not equipped with sufficient security mechanisms by default. Usually, secure socket layer/transport layer security (SSL/TLS) is used as a security mechanism in the MQTT protocol. However, it is not suitable for resource-constrained IoT devices because of the huge computational load involved in public key cryptography. In this paper, we propose a lightweight secure secret key-sharing system based on a secret-sharing scheme for resource-constrained IoT devices. The proposed system uses a (k, n)-threshold secret-sharing scheme to securely share a secret key for data encryption between the publisher and its subscriber hosts without compromising the lightweight nature of the MQTT protocol. A prototype of the proposed system is implemented using real IoT devices and its effectiveness and performance are evaluated. The experimental results demonstrate that the proposed system outperforms existing public key-based systems in terms of key-sharing delay.**

***Keyword*— IoT, MQTT, secret key cryptosystem, secret sharing**

Taku Noguchi He received the B.E., M.E., and Ph.D.degrees in communications engineering from Osaka University, Osaka, Japan in 2000, 2002, and 2004, respectively. He joined the College of Information Science and Engineering at Ritsumeikan University in 2004, where he is currently a professor. His research interests include performance analysis and the design of computer networks and wireless networks. He received the best tutorial paper award from IEICE ComSoc in 2012. He is a member of the IEEE, IEICE, and IPSJ.

Masato Nakagawa He received the B.E. and M.E. degrees in Information Science and Engineering from Ritsumeikan University, Shiga, Japan in 2019 and 2021, respectively. His resarch interests include IoT system, with emphasis on IoT security.

Masami Yoshida He received the B.E. and M.E. degrees in Information Science and Engineering from Ritsumeikan University, Shiga, Japan in 2016 and 2018, respectively. At present he is Ph.D. candidate at the same university. His resarch interests include mobile ad hoc networks, with emphasis on network coding. He is a student member of IEICE.

.

Alberto Gallegos Ramonet He received the B.E. degree in Computer Sscience from Guadalajara University, Jalisco, Mexico in 2005. He later received the M.S. and Ph.D. degrees in engineering from Ritsumeikan University, Shiga, Japan in 2014 and 2018, respectively. In the College of Information Science and Engineering at Ritsumeikan University, he was an Assistant Professor from 2018 to 2021. He is currently an Assistant Professor with the Graduate School of Technology, Industrial and Social Sciences, Tokushima University. His current research interests include but are not limited to wireless sensor networks, network simulations, network visualizers, routing protocols and anything related to IoT and connectivity of small devices.