ABSTRACT

Constraint device is a device that supports the development of IoT devices and communicating with each other. The communication process of the device is the activity that occurs in IoT. This communication process is carried out with a communication protocol. One of the communication protocols used is the MQ Telemetry Transport (MQTT) protocol, communication protocol that is lightweight, fast, and can be applied to constraints device. The MQTT protocol uses a broker as a server. However, the MQTT protocol does not have a security mechanism in the default settings, causing device authentication problems. Authentication problems in the MQTT protocol start with packet sniffing to obtain sensitive information on the communication packet over the network. This problem causes the registration and publishes phases of the MQTT protocol to be prone to non-authentic devices. The security mechanism in the MQTT protocol has been made previously using Transport Layer Security (TLS). However, TLS consumes more than 100 KB of memory and is not suitable for the constraints device. Therefore, this study proposes an authentication mechanism that is suitable for the constraint device to improve security in the MQTT protocol. This study proposes an authentication mechanism consisting of dynamic and event-based pillars for the MQTT protocol. The dynamic pillars aim to provide different authentication properties for each session to increase authentication security. The event-based pillars are used for scheduling and potentially reducing the computational burden on the constraint device. From the evaluation conducted, the proposed protocol can provide an authentication mechanism on the MQTT protocol. The results of validation using TAMARIN PROVER show that the proposed protocol is valid for packet sniffing threats. The proposed protocol can be implemented on the constraint device and brokers to perform authentication mechanisms.

Keywords: IoT, Authentication, MQTT, Constraint Device, Dynamic, Event-Based, TAMARIN PROVER