중앙 집중식 키 관리를 통한 MQTT 프로토콜 효율성 증대 연구

원찬희 · 김기천*

건국대학교

A Study on the Enhancement of MQTT Protocol with Centralized Key Management

Chan-hee Won · keecheon Kim*

Konkuk University

E-mail : snicky87@konkuk.ac.kr · kckim@konkuk.ac.kr*

요 약

모든 사물들이 다양한 네트워크를 통해 상호 소통하는 지능형 기술 및 서비스인 사물인터넷(Internet of Things)은 최근 ICT산업의 발전으로 주목받고 있는 분야 중 하나이다. 사물인터넷에서 주로 사용되는 프로토콜 중 하나인 MQTT(Message Queue Telemetry Transport)는 메모리 및 전력 이용을 효율화시키기 위해 가벼운 패킷 구조를 채택하였으며 보안성을 제공하기 위해 TLS 방식을 사용하는 안전한 프로토콜이다. 본 논문에서는 MQTT에서 TLS을 사용할 때 Broker에서 처리되는 암복호화 과정 대신, 인증 서버 추가를 통하여 중앙 집중식 키 관리를 수행하는 효율적인 MQTT 프로토콜을 제안하고자 한다.

ABSTRACT

Internet of Things(IoT) is an intelligent technology and service in which all objects communicate with each other through various networks. Recently Internet of Things(IoT) is one of the fields that is attracting attention as the development of ICT industry. MQTT is a protocol which is safe using TLS or adopting light packet structure for effciency of memory and power using. In this paper, when TLS is used the process of encryption / decryption in the broker occurs. We propose an efficient MQTT protocol through centralized key management by adding authentication server.

키워드

IoT, MQTT, TLS, Key management

Ⅰ. 서 론

최근 ICT 산업의 발전으로 모든 사물들이 여러 네트워크를 통해 상호 소통하는 지능형 기술 및 서비스인 사물인터넷(Internet of Things)은 주목받고 있는 분야 중 하나이다. 가트너에 따르면 2017년에 전 세계에서 84억 건의 연결된 사물이 2016년에 비해 31%가 증가할 것이며, 2020년에는 204억 건에 다다를 것이라 예측하였다[1].

이처럼 사물인터넷(Internet of Things)의 빠른 속도로 발전하는 만큼 IoT 기기의 보안 문제에 대한 우려도 커져가고 있다. 현재 IoT에서 활용되는 기술은 CoAP, XMPP, MQTT 등이 있는데 이 중 MQTT(Message Queue Telemetry Transport)은 TCP/IP기반으로 저 전력, 저 사양으로 경량의 메시지를 전송하는 프로토콜이다. MQTT는 일반적으로 평문 전송이 가능하지만 보안 강화를 위해 SSL/TLS의 사용을 권장하고 있다[2]. 중개자(Broker)는 발행자(Publisher)/구독자(Subscriber)와 암호화 통신을 위해 SSL/TLS를 사용하는데 이때, Broker에서 에너지 소비를 발생 시킬 수 있으며, 통신 초기에 선택된 암호화 알고리즘은 기기의 사양(에너지, 통신 속도 등)을 고려하지 않아서 IoT 기기의 성능을 저하시킬 수 있다[3].

위 문제를 해결하기 위한 방안으로 MQTT에서 SSL/TLS을 사용할 때 Client들과 Broker 사이에서

발생하는 암복호화 과정 대신, 인증 서버를 새로 추가하여 중앙 집중식 키 관리를 통한 효율적인 MQTT 프로토콜을 제안하고자 한다.

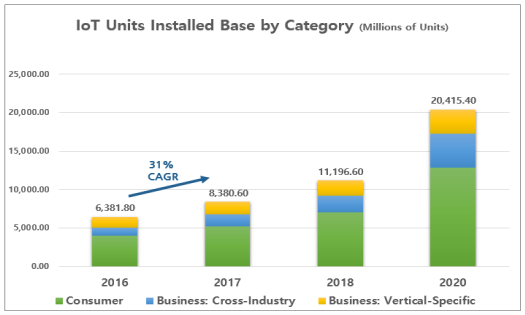

그림 1. 전 세계 설치된 IoT 기기의 수

Ⅱ. 본 론

2.1 MQTT

MQTT(Message Queue Telemetry Transport)은 publish/subscribe 방식의 메시지를 전송하는 프로토콜이다. 중개자(Broker), 발행자(Publisher) 그리고 구독자(Subscriber)로 3가지의 형태로 구성되어 있으며 가볍고 개방적이며 단순하고 쉽게 구현할 수 있도록 제작된 TCP/IP 기반의 프로토콜이다. 이러한 특성으로 M2M(Machine to Machine) 및 IoT(Internet of Things)와 같은 환경에 적합하다.

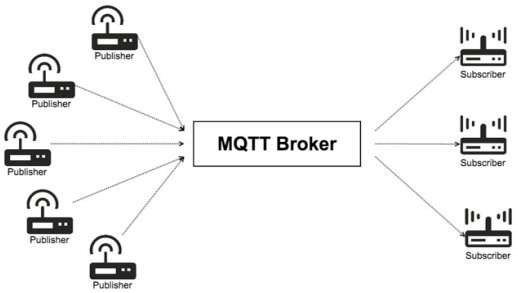

그림 2. MQTT Pub/Sub 모델

2.2 제안 연구

본 논문에서는 인증 서버를 추가하여 중앙 집중식 키 관리를 통해 MQTT 프로토콜 효율성을 향상 시키는 방법이다. 그림 3에서와 같이 중개자와 발행자, 구독자 그리고 인증 서버를 추가한 상태에서 제안한 방법이 진행된다. 제안한 방법은 SSL/TLS 통신이 아닌 일반 통신에서 진행된다. 발행자는 비밀키와 함께 암호화된 데이터를 중개자에게 전송을 하고, 암호화에 사용된 비밀키는 인증 서버에 전송을 한다. 암호화된 데이터는 메시지를 관리하는 역할인 중개자가 구독자가 요청할 때까지 저장한다. 이후 구독자가 데이터를 요청할 때, 중개자는 저장하고 있던 암호화된 데이터를 전송하고, 추가로 구독자는 인증 서버에 비밀키를 요청하여 비밀키를 받아 암호화된 데이터를 복호화하여 확인한다.

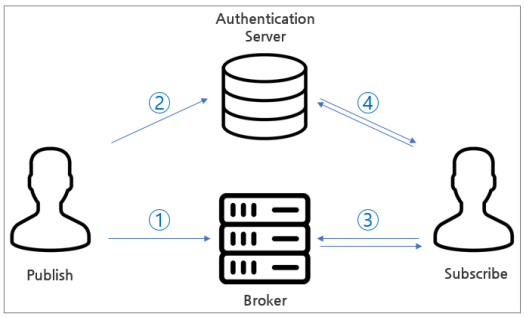

그림 3. 중앙집중식 키 관리를 통한 MQTT

Ⅲ. 결 론

본 논문은 사물인터넷 환경에 적합한 중앙 집중식 키 관리를 통한 MQTT 프로토콜의 효율성 증대 방안을 제안한다. 본 논문에서 제안하는 프로토콜은 새로운 인증 서버를 추가하여 공개키를 통한 대칭키 기반의 안전한 통신 방법을 갖게 한다. 이는 기존 TLS가 적용되는 MQTT 프로토콜에서 Client와의 통신을 통해 broker에서 발생할 수 있는 에너지 소비량에 대한 효율성 향상시킬 수 있는 방법이다.

향후에는 본 논문에서 제안한 MQTT 프로토콜의 효율성 확인을 위한 시스템을 구축하고 시뮬레이션을 통해 성능을 평가하여 사물인터넷 기기에 적용시킬 것이다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업“의 연구결과로 수행되었음(과제번호 H2101-17-1001)

참고문헌

[1] “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016”, http://www.gartner.com/newsroom/id/3598917

[2] MQTT, mqtt.org.

[3] 정진희, 조대호. "무선 환경에서 SSL/TLS를 사용하는 IoT의 에너지 효율성 향상을 위한 기법." 정보보호학회논문지, 26.3 (2016.06): 661-666.