ISSN 2383-630X(Print) / ISSN 2383-6296(Online)
Journal of KIISE, Vol. 45, No. 3, pp. 195-199, 2018. 3
https://doi.org/10.5626/JOK.2018.45.3.195

속성 기반 암호화 기법을 활용한 보안 MQTT 프로토콜

(Secure MQTT Protocol based on Attribute-Based Encryption Scheme)

김 남 호 †　　홍 충 선 ††
(Nam Ho Kim)　(Choong Seon Hong)

요 약 최근 사물인터넷(IoT)의 규모가 증가함에 따라 다량의 데이터가 발생하고 있고 이런 데이터를 이용한 다양한 서비스가 등장하고 있다. 이에 따라 빅 데이터들을 효율적으로 처리/전송 할 수 있는 사물인터넷 환경에 적합한 프로토콜이 필요하다. MQTT는 사물인터넷환경을 위한 경량의 메시징 프로토콜이다. 그러나 MQTT 프로토콜은 보안성을 제공하기 위해서는 TLS를 사용할 수 있지만, TLS를 사용할 경우 Handshake 및 패킷 오버헤드가 증가하는 문제점을 갖는다. 따라서 본 논문에서는 MQTT 프로토콜에 경량화 암호화 알고리즘을 활용하여 보다 강한 보안성을 제공하는 Secure_MQTT 프로토콜을 제안한다.

키워드: 사물인터넷, 키 정책, 속성 기반 암호화, 타원곡선암호화, 보안 프로토콜

Abstract Recently, with increasing scale of internet of Things (IoT), a large amount of data are generated and various services using such data are emerging. Therefore, a protocol suitable for IoT environment that can efficiently process / transmit big data is needed. MQTT is a lightweight messaging protocol for IoT environment. Although MQTT protocol can use TLS to provide security, it has a problem in that handshake and packet overhead will increase when TLS is used. Therefore, this paper proposed as Secure_MQTT protocol. It can provide stronger security by using lightweight encryption algorithm for MQTT protocol.

Keywords: internet of things, Key-Policy, attribute-based encryption, elliptic curve encryption secure protocol

· 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2015-0-00557, IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술 연구)
· 이 논문은 제43회 동계학술발표회에서 '경량화 암호화 알고리즘 기반 보안 MQTT 프로토콜'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 경희대학교 컴퓨터공학과
knm1471@khu.ac.kr
†† 종신회원 : 경희대학교 컴퓨터공학과 교수(Kyung Hee Univ.)
cshong@khu.ac.kr
(Corresponding author임)

논문접수 : 2017년 2월 15일
(Received 15 February 2017)
논문수정 : 2017년 11월 24일
(Revised 24 November 2017)
심사완료 : 2017년 12월 5일
(Accepted 5 December 2017)

정보과학회논문지 제45권 제3호(2018. 3)

1. 서 론

최근 다양한 IoT 디바이들이 등장하고 있으며, 국내외 IoT 시장 규모가 향후 10년동안 최대 5배 이상 성장할 것으로 예상하고 있다[1]. 이렇듯 IoT 디바이스 네트워크 규모의 증가와 디바이스 종류가 다양해짐에 따라, 이와 관련한 많은 서비스들이 등장하고 있다.

그로인해 머지않아 스마트 장치들의 확산과 사물 인터넷 기술로부터 발생되는 정보의 생산은 빅데이터 환경을 발생시킬 것이고, 이렇게 모인 데이터들은 각 산업 분야에 큰 발전을 가져올 것이다. 따라서 많은 정보들을 효율적으로 처리할 수 있는, CoAP과 MQTT 같은 사물인터넷 프로토콜이 필요하다[2].

낮은 전력, 낮은 대역폭을 갖는 자원이 제한적인 환경에서도 사용할 수 있는 프로토콜로는 CoAP과 MQTT를 들 수 있다. 그러나 자원이 제한적인 네트워크에서는 보안 위협요소들에 노출될 가능성이 더 크다[3]. 또한, MQTT 3.1.1 표준을 제정한 OASIS에 따르면 MQTT는 메시지 전송에만 초점이 맞춰져 설계되어 있고, 표준 보안 기술이나 보안 정책 가이드라인이 없다고 한다[4]. 따라서 사물인터넷 환경에 MQTT를 적용할 경우 그에 따른 보안 기술이 제공되어야 한다.

따라서 본 연구에서는 사물인터넷 환경에 맞는 경량화 타원 곡선 알고리즘을 활용한 Secure MQTT를 제안한다.

본 논문의 2장에서는 MQTT와 암호화 알고리즘에 대해 간략히 언급하고, 3장에서는 Secure MQTT의 구조를 제시한다. 마지막으로 4장에서는 결론 및 향후 계획으로 논문을 마친다.

2. 관련 연구

2.1 타원 곡선 알고리즘

타원 곡선 알고리즘(Elliptic Curve Cryptography Algorithm)은 이산대수에서 사용하는 유한체의 곱센군을 타원곡선군으로 대치한 암호체계로써, 다른 암호체계에 비하여 짧은 키 사이즈로 대등한 안전도를 가지는 것이 큰 장점이다.

ECC 알고리즘을 이용한 암호 시스템은 난수와 결합한 공개키를 각 단말에 공유하여 공격자가 유추할 수 없는 비밀키로 동기화하고, 암호화하는 순서로 진행된다. 이와 같은 암호 시스템을 구현하기 위해서는 키 분배 알고리즘과 메시지 암호 알고리즘이 구성되어야 하며, ECC 기반의 키 분배 방식은 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘이 대표적이다. EC-ElGamal 알고리즘은 ECDH 알고리즘을 바탕으로 메시지를 암호화하는 방법이며, 현재 ECC 알고리즘 기반으로 암호기법 중 가장 많이 사용하는 암호 알고리즘이다. 메시지 암호화는 비밀키 계산 이후 단말이 메시지와 비밀키를 연산하여 서버 송신 과정과 서버가 비밀키를 이용하여 암호화 된 메시지를 연산하는 과정으로 진행된다[5].

2.2 속성기반 암호화(Attribute-Based Encryption)

속성 기반 암호화는 암호화된 데이터에 맞는 속성값을 가지는 사용자만이 데이터를 복호화할 수 있는 암호화 기법이다. 속성 기반 암호화는 크게 Key-Policy기반 암호화, Cypertext-Policy기반 암호화로 구분할 수 있다.

Key-Policy 속성기반 암호화에 따르면, 암호화된 데이터와 속성의 집합으로 암호문을 구성하고, 각 사용자들은 사용자의 속성에 대해 Access Tree 구조로 개인키를 보유한다. 만약 사용자의 Access Tree 구조가 암호문의 속성의 집합을 만족하는 경우 사용자가 암호문을 복호화할 수 있다. 그림 1은 한 예시를 보여준다.

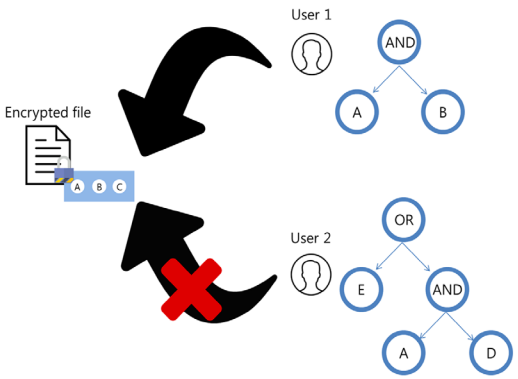

그림 1 KP-ABE 접근 관리
Fig. 1 KP-ABE Access Control

그림 1에서 나타난 바와 같이 각 사용자들은 각각의 Access Tree를 보유한다. 암호화된 파일은 속성 집합 {A, B, C}를 활용하여 암호화 되어 있다. 각각의 사용자들이 암호화된 파일의 복호화를 시도할 경우, 사용자 1은 {A&B}의 Access Tree를 보유하고 있고, 이는 암호화에 사용되었던 속성 집합 {A, B, C}를 만족하므로 암호문을 복호화할 수 있다. 그러나 사용자 2의 경우 Access Tree가 암호문 속성 집합을 만족하지 않으므로 복호화된 평문에 접근할 수 없다.

2.3 MQTT

MQTT는 경량의 Publish/Subscribe 메시징 프로토콜로써 사물인터넷에서의 사용을 목적으로 만들어졌다. TCP 기반으로 만들어 졌고, QoS를 제공한다.

MQTT는 Publisher, Subscriber, Broker 이렇게 세 요소로 구성되어있다. Publisher와 Subscriber는 모두 Broker에 대한 클라이언트로 작동한다. Publisher는 토픽을 발행하기 위한 목적으로 Subscriber는 토픽을 구

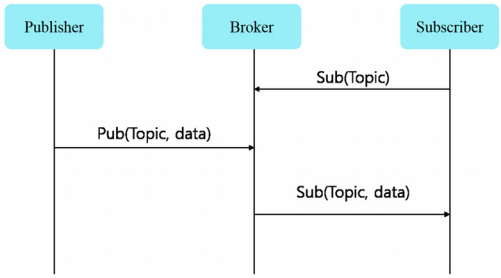

그림 2 MQTT 프로토콜 메시지 전송
Fig. 2 MQTT Protocol Message Transport

독하기 위한 목적으로 Broker 서버에 연결한다. 하나 이상의 Publisher와 Subscriber가 브로커에 연결해서 토픽을 발행하거나 구독할 수 있다. MQTT 프로토콜의 메시지 전송 Flow는 그림 2와 같다. Subscriber는 특정 Topic에 대한 데이터를 Broker에게 요청한다. Publisher는 자신의 데이터를 Topic과 함께 발행한다. Broker는 해당 Topic을 요청했던 Subscriber에게 Topic과 데이터 정보를 전달한다.

MQTT 프로토콜을 제안한 OASIS에 의하면 기존의 MQTT 프로토콜은 보안성을 제공하기 위한 메커니즘이 없어 TLS를 활용하기를 권장하고 있다.

3. 제안 사항

본 연구에서는 기존의 MQTT 프로토콜을 사물인터넷 환경에 적합한 보안성이 강화된 MQTT 프로토콜을 제안한다.

앞서 언급했듯이, OASIS는 MQTT를 활용한 보안 통신을 위해 TLS를 활용하기를 권장하고 있다. 그러나 TLS를 활용할 경우 사물인터넷 환경의 다양한 기기들에 대해서는 적합하지 않다. TLS는 OpenSSL을 활용하는데, 이는 CPU 성능이 낮고 네트워크 대역폭이 낮은 기기들은 사용할 수 없으며, 발생하는 오버헤드의 근본적 해결 방법은 없다[4]. 따라서 Lightweight하고 Robust한 암호화 메커니즘이 필요하다.

본 논문에서 제안하는 시스템 모델은 다음과 같다.

본 논문에서는 그림 3과 같은 사물인터넷 네트워크 구조를 고려한다. 하나의 신뢰할 수 있는 노드인 Broker와 소수의 자원 제약이 없는 노드들 그리고 다수의 자원 제약이 심한 노드들로 구성되어있다. 각각의 자원 제약이 심한 노드들은 자원 제약이 없는 노드들과 연결되어있다. 각각의 자원 제약이 심한 노드들은 자원 제약이 없는 노드들과 사전에 키를 공유하고 있다고 가정한다.

제안하는 보안 메커니즘은 크게 두 단계로 구성된다. 3.1장에서는 보안 통신을 위한 키 교환 및 Access Tree 구성을 위한 Set-up phase를, 3.2장에서는 Secure MQTT

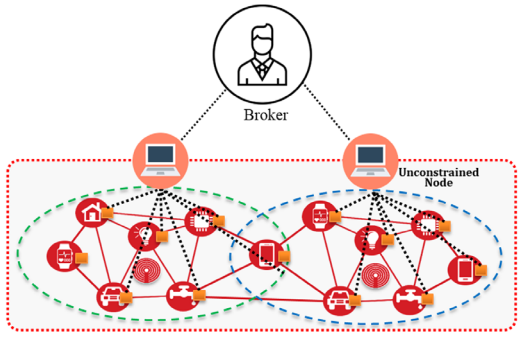

그림 3 시스템 모델
Fig. 3 System Model

표 1 표기법
Table 1 Notation

Notation	Description
x	Random Number for Key Generation (Node side)
y	Random Number for Key Generation (Broker side)
G	Base Point for Key Generation
S	Node's Attribute Set
C	Ciphertext
T_s	Access Tree in Subscriber
T_P	Access Tree in Publisher
M	Plaintext (Original Data)

에서의 통신 Flow를 다룬다. 표 1은 각 장에 언급되는 기호와 설명을 나타낸다.

3.1 Set-up phase

이 단계는 모든 노드와 Broker간의 통신 이전에 일어나는 과정이다. 각 노드는 먼저 Broker를 통한 통신을 위해 Broker에게 자신을 등록한다. 등록을 마친 노드와 Broker는 ECDH(Elliptic Curve Diffie-Hellman) 키교환 알고리즘을 활용하여 대칭키를 생성한다. 노드와

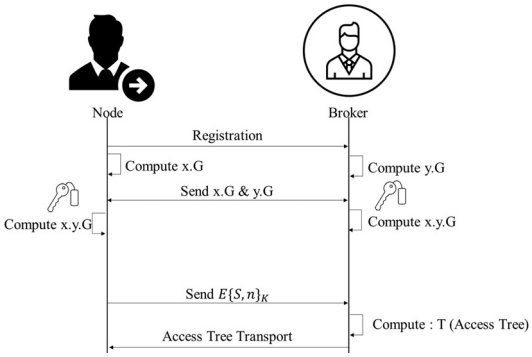

그림 4 Set-up 단계
Fig. 4 Set-up phase

Broker는 각각 랜덤 변수 'x'와 'y'를 선택한다. 상호간 서로의 비밀값인 x.G와 y.G를 전달하고, 자신의 랜덤 변수를 활용하여 대칭키를 생성한다. 노드는 Access Tree를 생성하기위해 Broker로 자신의 속성 집합 S을 대칭키로 암호화하여 전송한다. 브로커는 암호화된 메시지를 대칭키를 이용해 복호화하여 노드의 속성 집합을 확인한다. 브로커는 속성 집합을 확인하여 각 노드별 고유 Access Tree를 생성하여 전송한다.

3.2 Secure MQTT 통신 Flow

Set-up 단계에서 각각의 Node들은 Broker에 자신을 등록함으로써 자신의 Access Tree와 키를 보유한다. Set-up 단계가 완료된 노드 중 특정 Topic에 대한 데이터를 요청하고, 획득하는 과정은 그림 5와 같다.

Subscriber는 Broker에게 Topic에 대한 데이터를 요청한다. 이때. Publisher가 데이터를 생성할 경우, 자신의 Access Tree인 T_P로 데이터를 암호화한다. 그러나 자원 제약이 있는 노드의 경우, Key Policy 속성 기반 암호화를 활용해 데이터를 암호화하려면 큰 오버헤드가 발생한다. Key Policy 속성 기반 암호화에는 자신의 $|Access\ Tree|+1$ 의 지수연산이 요구되기 때문이다. 따라서 암호화 연산을 자원 제약이 심한 노드가 아닌 주변의 제약이 없는 노드에서 이루어져야한다. 따라서 다음과 같은 방식으로 데이터를 암호화한다.

자원 제약이 심한 노드인 Publisher는 데이터와 속성 집합을 공유키로 암호화하여 모든 자원 제약이 없는 노드에게 전달한다. 자원 제약 없는 노드는 Publisher의 Access Tree를 활용하여 데이터를 암호화 하고 Publisher에게 전달한다. 모든 자원 제약이 없는 노드들로부터 암호화된 데이터를 전달받으면 각각의 암호화된 데이터를 Broker에게 Publish한다. Broker는 각각의 암호화된 데이터들을 전달받으면 하나의 암호화된 데이터로 재조립한다.

이와 같이 Broker가 암호화된 데이터를 전달 받으면 Topic에 대한 데이터를 요청한 Subscriber와의 대칭키를

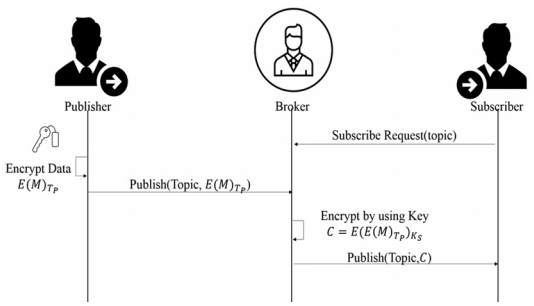

그림 5 Secure MQTT 통신 Flow
Fig. 5 Secure MQTT Communication Flow

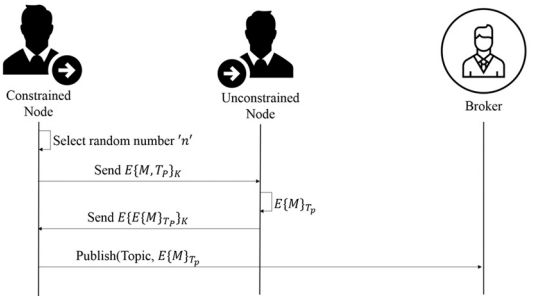

그림 6 암호화 구조
Fig. 6 Encryption Scheme

활용하여 Ciphertext를 생성한다. Broker는 Subscriber에게 Topic과 Ciphertext를 전달한다. Subscriber는 자신의 K_S로 Ciphertext를 복호화하고, 자신의 Access Tree로 암호화된 데이터를 복호화 함으로써 평문의 데이터를 획득할 수 있다.

4. 보안성 검토 및 성능 평가

4.1 보안성 검토

만약 임의의 노드가 암호화된 데이터를 복호화하는 것을 시도하는 경우, Publisher의 Key-Policy를 알거나, Subscriber와 Broker의 대칭키 정보를 활용해야 한다.

제안하는 MQTT 프로토콜에서는 Broker가 각각의 Publisher와 Subscriber로부터 고유 식별 값을 받아 Key-Policy를 생성하고 전달한다. 이 때, 수많은 사물인터넷 기기들이 존재하므로 Access Tree 형태의 Key-Policy의 높이와 너비가 충분히 넓다. 따라서 임의의 공격자 노드는 Key-Policy를 모르기 때문에 복호화를 할 수 없다.

또한 공격자가 Man-in-the-middle 공격을 시도한다고 하더라도 Key-Polciy 속성과 대칭키의 정보를 공격자는 알지 못하므로 데이터 복호화는 불가능하다. 또한 대칭키는 Elliptic Curve Diffie-Hellman 키 교환 방법을 사용하므로 공격자가 대칭키 획득을 시도한다면 Diffie-Hellman 문제를 갖게 된다.

4.2 성능 평가

기존의 MQTT와 TLS를 활용하여 통신하는 경우, TLS Handshake와 추가적인 패킷의 전송 등으로 사물인터넷 환경에 적용하기에는 오버헤드가 크다. 그러나 제안하는 Secure MQTT의 경우, 기존의 MQTT 상에 속성기반 암호화 알고리즘과 대칭키 암호화 알고리즘을 활용하여 보안 통신을 제공한다. 따라서 보안 통신을 위해 추가적인 HandShake나 패킷 헤더의 추가 없이 통신이 가능하므로 효율적이다.

본 논문에서는 Key-Policy 속성 기반 암호화와 대칭키를 활용하여 보다 보안성이 보장된 MQTT 프로토콜

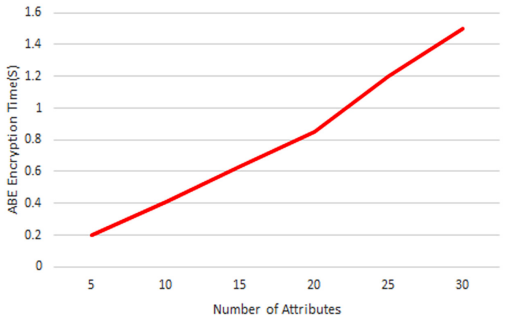

그림 7 항목에 따른 연산 시간
Fig. 7 Encryption Time per number of attributes

을 제안했다.

Key-Policy 속성 기반 암호화는 다른 암호화 기법과는 달리 사물인터넷 기기들이 보유하고 있는 속성들을 이용해 Broker가 Key-Policy를 생성/전달하기 때문에 각각의 기기들이 처리해야할 연산이 매우 적어 낮은 전력, 한정된 자원을 가진 기기들에서도 에너지 소모가 적다.

또한 ECDH 키교환 알고리즘을 통해 대칭키를 생성하고 Broker가 Subscriber로의 데이터 전송 시 대칭키를 활용하여 해당 대칭키를 보유한 기기만 복호화를 할 수 있게끔 구성하였다. 이와 같은 방법은 기존의 Key-Policy 속성 기반 암호화의 문제점인 암호문에 대한 사용자의 접근 제어를 보완 할 수 있다. 또한 ECC알고리즘은 RSA에 비해 길이가 짧은 키를 활용하여 같은 수준의 보안성을 보장하기 때문에 사물인터넷 환경에 적용하기에 적합하다.

5. 결론 및 향후 연구

본 논문은 사물인터넷 환경에 적합한 보안성을 보장하는 MQTT 프로토콜을 제안한다. 본 논문에서 제안하는 프로토콜은 Key-Policy 속성 기반 암호화 알고리즘과 ECDH(Elliptic Curve Diffie-Hellman) 키 교환 알고리즘을 통해 보안 통신을 제공한다.

사물인터넷 기기들마다 가질 수 있는 속성을 기반으로 Broker는 Key-Policy 속성을 생성하고 속성 기반으로 암호화를 함으로써 기존의 MQTT 프로토콜에 보안성을 강화하였다. 또한, 새로운 메시지 타입을 정의하여 Subscriber와 Broker 간 대칭키를 생성함으로써 기존에 존재하였던 Man-in-the-middle 공격을 방지할 수 있도록 하였다. 이와 같은 방법은 기존의 MQTT 프로토콜에 보안성을 강화할 뿐만 아니라, 각각의 사물인터넷 기기들이 암호화 연산으로 인한 자원 및 에너지 소모량이 적어 사물인터넷 환경에 적용하기 적합하다고 볼 수 있다.

그러나 현재 제안된 Secure MQTT에서 Publisher는 자원이 제한적이지 않은 노드에게 암호화 연산을 의존한다. 이러한 경우에 자원이 제한적이지 않은 노드가 해당 암호화 연산을 거부하거나 수행하지 못 할 수 있다. 따라서 이러한 문제점들을 다시 한 번 검토하여 보다 효율적이고 견고한 보안 메커니즘으로 확장할 계획이다.

References

[1] Lee Hyoeun et al., "IoT status and major issues," *Information and Communication Technology Promotion Center, IT statistical survey and trend analysis report*, 1-42, 2014 (In Korean)

[2] Sang-Hyun Kim, Young-Don Kim, Jung-Hyuck Lee, Chang-Se Oh, Min-seok Seo, Chang-Suk Lee, Hyun-Ju Park, "A Study On The Procedure That Sensor Devices Are Connected To Home Server In IoT Environment," *Korea Computer Congress*, Vol. 41, No. 1, pp. 1263-1265, 2014. (In Korean)

[3] Nam Hee Kang, "Standard Technology Trends for Internet of Things Security," *The Journal of The Korean Institute of Communication Sciences*, Vol. 31, No. 9, pp. 40-45, 2014. (In Korean)

[4] Se-Ra Oh, Young-Gab Kim, "Security Analysis of MQTT and CoAP protocols in the IoT Environment," *2016 Korea Information Processing Society Spring Conference*, Vol. 23, No. 1, pp. 297-299, 2016. (In Korean)

[5] Hyun-Soo Kim, Seok-Cheon Park, "Design and Implementation of effective ECC Encryption Algorithm for Voice Data," *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 15, No. 11, pp. 2374-2380. 2011 (In Korean)

김 남 호
2016년 경희대학교 컴퓨터공학과(공학사)
2016년 3월부터 현재까지 경희대학교 컴퓨터공학과 석사과정. 관심분야는 네트워킹, 네트워크 보안

홍 충 선
1983년 경희대학교 전자공학과(공학사)
1985년 경희대학교 전자공학과(공학석사)
1997년 Keio University, Department of Information and Computer Science (공학박사). 1988년~1999년 한국통신통신망연구소 수석연구원/네트워킹 연구실장. 1999년~현재 경희대학교 컴퓨터공학과 교수. 관심분야는 인터넷 서비스 및 망 관리구조, 미래인터넷, IP mobility, Sensor Networks, Network Security