경량화 암호화 알고리즘 기반 보안 MQTT 프로토콜

김남호○, 홍충선*
경희대학교 컴퓨터공학과
{knm1471, cshong}@khu.ac.kr

Lightweight Cryptography Algorithm based Secure MQTT Protocol

Namho Kim○, ChoongSeon Hong*
Department of Computer Science and Engineering, Kyung Hee University

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.

1. 서 론

최근 IoT 다양한 디바이스들이 등장하고 있으며, 국내외 IoT 시장 규모가 향후 10년 동안 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 빅 데이터 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 곱셈군을 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 비밀 키로 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 암호 기법 중 가장 많이 사용하는 암호 알고리즘이다. 메시지 암호화는 비밀 키 계산 이후 단말이 메시지와 비밀 키를 연산하여 서버 송신 과정과 서버가 비밀 키를 이용하여 암호화 된 메시지를 연산하는 과정으로 진행된다.[5]

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (B0190-16-2017, IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술 연구) *Dr. CS Hong is the corresponding author

2.2 Key-Policy 속성기반 암호화(KP-ABE)

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

Key-Policy 속성기반 암호화에 따르면, 암호화 된 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 복호화 할 수 있다.

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 구독하기위한 목적으로 Broker 서버에 연결한다. 하나 이상의 Publisher와 Subscriber가 브로커에 연결해서 토픽을 발행하거나 구독할 수 있다.

3. 제안 사항

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

OASIS에 의하면, 기존의 MQTT 프로토콜은 보안성을 제공하기 위한 메커니즘이 없어 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. 제안하는 Secure MQTT는 다음과 같다.

먼저 본 논문에서는 기존의 MQTT 메시지 타입에 두 종류의 메시지 타입을 추가한다. 본 논문에서는 Broker가 자체적으로 메시지를 보내는 경우를 고려하여 '0' 번과 '15'번의 메시지 타입을 새롭게 정의한다. '0'번의 메시지 타입은 Broker가 자체적으로 생성하여 Subscriber나 Publisher에게 보내는 메시지이다. '15번' 메시지는'0'번 메시지에 대한 Ack타입이다. 이러한 메시지 타입을 구성하여 제안하는 MQTT 프로토콜은 그림 1과 같은 Flow를 통해 메시지를 주고받을 수 있다.

표 1. Propose MQTT Message Type

명칭	수	설명
BROMSG	0	Broker가 생성한 메시지
CONNECT	1	Connect Request
CONNACK	2	Connect Acknowledgement
PUBLISH	3	Publish Message
PUBACK	4	Publish Acknowledgement
PUBREC	5	Publish Received
PUBREL	6	Publish Release
PUBCOMP	7	Publish Complete
SUBSCRIBE	8	Subscribe request
SUBACK	9	Subscribe Acknowledgement
UNSUBSCRIBE	10	Unsubscribe request
UNSUBACK	11	Unsubscribe Acknowledgement
PINGREQ	12	Ping Request
PINGRESP	13	Ping Response
DISCONNECT	14	Disconnect
BROMSGACK	15	BROMSG Acknowledgement

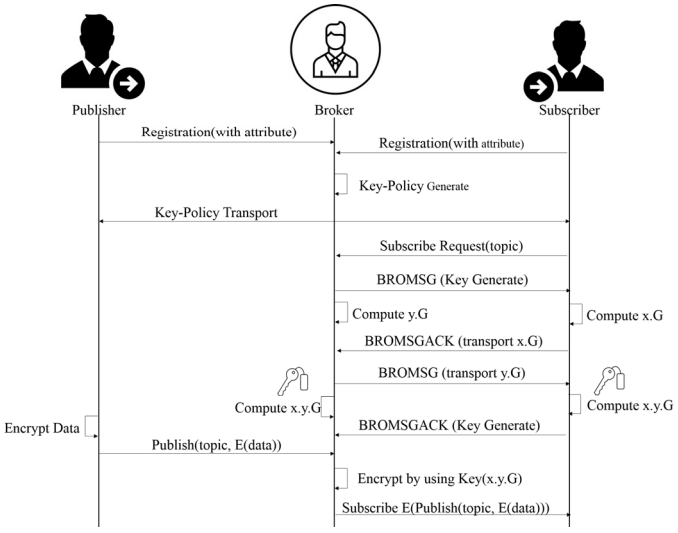

그림 1. Secure MQTT communication Flow

여기서 Broker는 신뢰할 수 있는 서버라고 가정한다. 먼저, Subscriber와 Publisher는 Broker서버로 자신의 고유 정보와 함께 자신을 등록 요청한다. 그에 따라 Broker는 고유정보를 활용하여 Key-Policy를 생성하고 전달한다. 만약 Subscriber가 특정 Topic의 정보를 요구한다면, Broker는 Subscriber에게 대칭 키 생성을 위한 요청을 보낸다. Subscriber와 Broker는 ECDH(Elliptic Curve Diffie-Hellman) 키 교환 방법을 이용하여 대칭키를 형성한다. Publisher가 데이터를 전송하는 경우에, Key Policy을 활용하여 데이터를 암호화하고 Broker로 Publish한다. Broker는 Publish된 암호문을 다시 한 번 Subscribe와 생성한 대칭키로 다시 한 번 암호화를 진행

하고 Subscriber에게 전달한다. Subscriber는 자신의 대칭키와 Key-Policy를 이용하여 복호화함으로써 데이터를 획득할 수 있다. Subscriber가 UNSUBSCRIBE 패킷을 보내면, Broker는 UNSUBACK 패킷을 보내고 동시에 기존의 대칭키를 삭제한다.

4. 성능 평가

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

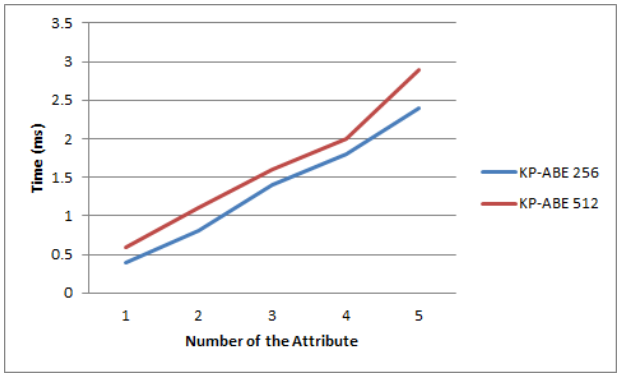

그림 2. 항목에 따른 연산 시간

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.

보안성 분석 측면에서 제안 시스템을 위협하는 공격으로는 크게 암호문 공격과 Man-in-the-middle 공격이 존재한다. 먼저 암호문 공격은 암호문을 통해 공격자가 평문을 알아내거나 암호화가 쓰인 알고리즘이나 키를 알아내는 방법이다.

그러나 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 공격자는 Key-Policy를 모르기 때문에 복호화 할 수 없으며, 임의의 Key-Policy 추측하여 복호화를 시도할 경우 시간 복잡도는 $O(K^n)$ 이 되므로 암호문 공격으로부터 제안하는 시스템은 안전하다고 할 수 있다.

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.

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.

향후 연구 방향은 본 논문에서 제안한 MQTT 프로토콜을 보다 경량화 하여 사물인터넷 환경에 최적화된 경량화 알고리즘을 고안하고 실제 자원이 제한된 사물인터넷 환경에 적용 시키는 것이다.

참 고 문 헌

[1] 이효은 외 11명,"IoT 현황 및 주요 이슈", 정보통신기술진흥센터 IT통계 조사 및 동향분석 보고서, 1-42, 2014

[2] 김상현, "사물인터넷 환경에서 센서 단말들이 홈 서버에 연결되는 절차에 관한 연구", 한국정보과학회 학술발표논문집, VOL 41, No.1, 1263-1265p, 2014

[3] 강남희, "사물인터넷 보안을 위한 표준기술 동향", 한국통신학회지(정보와통신), 31권, 9호, 40-45p, 2014

[4] 오세라, 김영갑 "IoT 환경에서의 MQTT, CoAP 보안 기술 분석", 2016년 한국정보처리학회 춘계학술발표대회, 23권, 1호, 297-299p, 2016

[5] 김현수, 박선천, "음성 데이터 보안을 위한 효율적인 ECC 암호 알고리즘 설계 및 구현", 한국정보통신학회논문지, 15권, 11호, 2374-2380p, 2011