IoT 환경을 위한 ECQV 기반의 인증 및 키 합의 기법 설계+

이대휘, 이임영
순천향대학교 컴퓨터학과
e-mail:[leedh527, imylee]@sch.ac.kr

Design of Authentication and Key Agreement Scheme using ECQV for IoT Environments

Dae-Hwi Lee, Im-Yeong Lee
Dept of Computer Science and Engineering, Soonchunhyang University

요 약

최근 출시되는 다양한 IoT 서비스 환경에 참여하고 있는 객체들은 각자 인터넷에 연결되어 다른 객체와 통신할 수 있다. 이전에는 디바이스가 직접 인터넷에 연결될 수 있는 능력이 없었기 때문에 게이트웨이와 같은 중간 연결 매개체를 통해 인터넷에 연결되었다. 이후 IoT 디바이스의 성능이 좋아짐에 따라 디바이스가 직접 인터넷에 연결되고, 다른 디바이스들과 직접 통신할 수 있게 되었다. 디바이스는 사용자의 스마트폰이 될 수 있고, 스마트홈이나 스마트시티를 구성하는 여러 디바이스들이 될 수 있으며, 이를 확인하고 안전하게 데이터를 송수신하기 위해서는 인증 및 키 관리가 필수적이다. 객체가 인터넷에 연결될 수 있음에도 불구하고 IoT 디바이스들은 제한된 환경에서 동작하는 특성을 가지기 때문에, 기존 인증 및 키 합의 프로토콜을 그대로 적용할 수 없다. 따라서 본 논문에서는 IoT를 구성하는 객체가 인터넷에 직접 연결되고 서로 안전하게 통신하기 위해 ECQV(Elliptic Curve Qu-Vanstone) 묵시적 인증서를 통해 상호 인증 후 키를 안전하게 합의할 수 있는 인증 및 키 합의 기법에 대해 연구한다.

1. 서론

최근 IoT(Internet of Things)는 다양한 분야에 적용되고 있으며, 우리나라를 비롯한 세계 주요국과 글로벌 기업들도 적극적으로 투자하여 개발하고 있다[1]. 이러한 IoT 환경은 여러 서비스들이 출시됨에 따라 점차 거대해지고 있다. 초기의 IoT 서비스는 하나의 가정을 IoT 디바이스들과 통신 기술로 거주자에게 편의를 제공할 수 있는 스마트홈부터 시작하였다. 최근에는 더 많은 디바이스들이 인터넷에 연결된 스마트팩토리, 스마트시티와 같은 대규모 IoT 서비스들이 출시되었다. 이러한 IoT 서비스 환경에 참여하고 있는 디바이스와 같은 참여 객체들은 각자 인터넷에 연결되어 다른 객체와 통신할 수 있지만, IoT 디바이스들은 제한된 환경에서 동작하는 특성을 가지기 때문에, 기존의 키 관리 프로토콜을 그대로 적용할 수 없다.

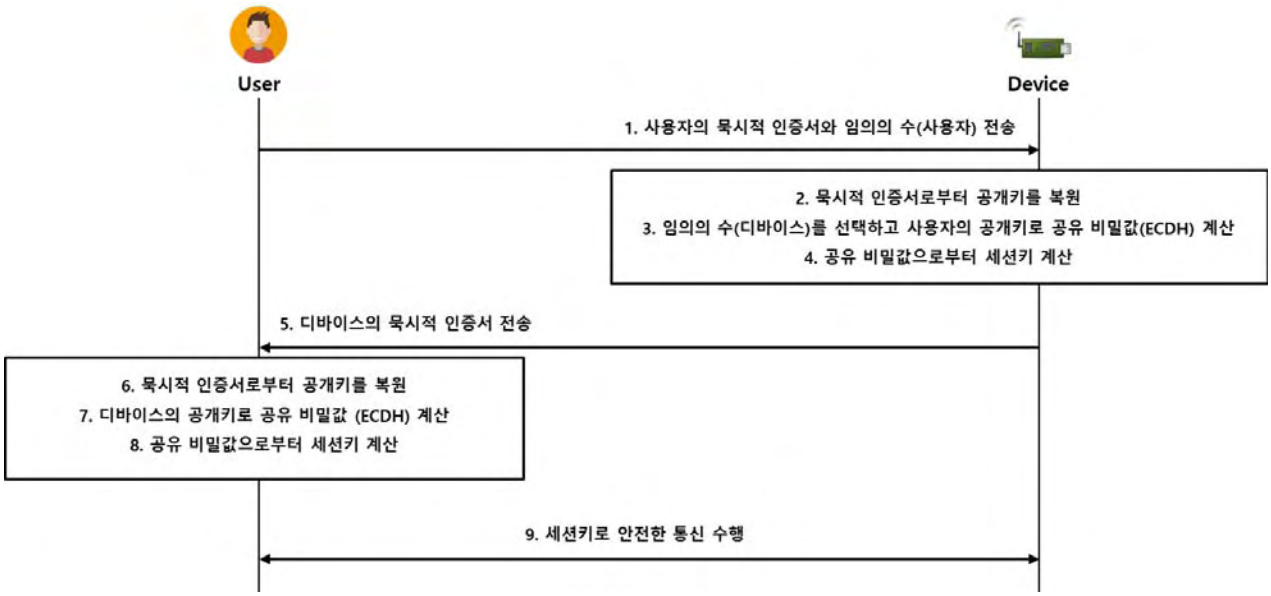
따라서 본 논문에서는 IoT를 구성하는 객체가 인터넷에 직접 연결되고 서로 안전하게 통신하기 위해 상호 인증 후 키를 안전하게 합의할 수 있는 인증 및 키 합의 기법에 대해 연구한다.

+ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2019-2015-0-00403)

2. 인증서 기반 키 관리

IoT 서비스 환경은 매우 많은 종류의 객체가 인터넷에 연결되어 통신하기 때문에 효율적이며 안전한 키 관리가 필요하며, 이 중 두 객체간 안전한 통신을 위해서는 인증과 키 합의 과정이 필요하다. 일반적으로 IoT 환경에서 키 합의를 사용하는데, 이는 두 객체간 통신에서 세션마다 비밀키를 생성할 때 비밀키 보관에 따른 노출 위험이 적어지기 때문이다. 하지만, 가장 기본적인 Diffie-Hellman 키 합의 방식에서 볼 수 있는 내용과 같이 중간자 공격이나 위장 공격 등에 취약하기 때문에, 추가적인 인증 프로세스가 필요하다. 이는 키 합의 프로토콜 자체에 객체 상호에 대한 인증 기능이 없기 때문이다. 객체가 다른 객체와 데이터를 공유하고 전달하기 위해서는 인증을 통해 객체에 대한 확인을 해야 한다. 인증 과정은 다양한 방법으로 수행 가능하며, 본 논문에서는 ECQV 묵시적 인증서 기반의 인증 방법을 설명한다.

ECQV(Elliptic Curve Qu-Vanstone)는 묵시적 인증서(Implicit certificate)라고도 불리는 인증서의 종류로 SECG SEC 4(Standard Efficient Cryptography 4)에 정의되어 있다[2]. 일반적으로 사용자에게 CA가 발급한 공개키 인증서는 식별자와 공개키, 전자서명이 포함되어 있으며, 공개키와 식별자 등을 이용해 전자서명을 검증함으로



(그림 1) 설계된 제안 방식 시나리오

써 명시적으로 사용자와 메시지를 인증할 수 있다. 묵시적 인증서에는 식별자와 공개키 복원 데이터만이 포함되어 있으며, 공개키 복원 데이터에서 식별자 등을 통해 사용자의 공개키를 계산함으로써 묵시적으로 인증서와 공개키를 검증한다. 공개키가 포함되어 있지 않기 때문에 공개키 인증서보다 크기가 작고, ECC(Elliptic Curve Cryptography)를 사용하여 다른 암호화 방식에 비해 키 길이가 짧고 속도가 빠른 장점이 있어 자원이 제한된 IoT 환경에서 사용하기에 적합하다.

3. 제안 방식 설계

본 논문에서는 IoT 환경에서의 인증 및 키 합의에 있어서 두 객체가 직접 통신할 수 있도록 ECQV를 이용한 방식을 설계한다. 기존의 ECQV 기반 키 관리 기법에서는 재전송 공격으로 인한 노드 위장이 가능한 문제점이 있었기 때문에[3,4], 이를 해결하기 위해 키 생성 과정에서 불필요한 과정을 줄이고 정당한 파라미터를 이용하는 인증 및 키 합의 기법을 설계한다. 위와 같은 문제를 해결하기 위해서는 다음의 보안 요구사항을 만족해야 하며, 사용자와 디바이스간 ECQV 기반의 인증 및 키 합의 과정은 (그림 1)과 같다.

- 상호 인증 : 여러 엔티티가 통신함에 있어서 보안을 제공하기 위해서는 상호 인증은 필수 요소이며, 인증된 엔티티간 안전한 통신을 위해서 키 합의가 필요하다.
- 키 유출 방지 : 인증을 수행하는 이유는 이후의 세션키 합의를 위해서이며, 세션키는 외부로 유출되어서는 안된다.
- 재전송/위장 공격 방지 : 공격자가 통신 메시지를 재전송하여 정당한 사용자로 위장할 수 없어야 한다. 상대방이 공격자를 정당한 사용자로 인식하게 되는 위장 공격도 방지하여 정당한 사용자에 대한 가용성을 제공해야 한다.

4. 결론

본 논문에서 설계된 방식은 ECQV 묵시적 인증서를 사용하여 두 객체에 대한 인증을 수행하고 키 합의를 진행한다. 기존 방식들에서는 특히 재전송 공격과 위장 공격 그리고 이를 통한 키 유출에 대해 문제가 있었기 때문에, 이를 해결하기 위해 전송되는 데이터를 최소화하고 통신 횟수를 줄여 속도를 높여 효율성까지 제공할 수 있다.

향후에는 1:1로 통신하는 환경이 아닌 계층적인 IoT 환경에서 사용될 수 있는 게이트웨이-객체들 간에 위와 같은 문제를 해결할 수 있는 인증 및 키 관리 기법을 연구가 필요하다.

참고문헌

[1] Karaköse, M., Yetiş, H, “A cyberphysical system based mass-customization approach with integration of Industry 4.0 and smart city,” Wireless Communications and Mobile Computing, 2017.

[2] Campagna, M, “SEC 4: Elliptic curve Qu-Vanstone implicit certificate scheme (ECQV),” Technical Report, 2013.

[3] Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., Bianchi, G, “Key management protocol with implicit certificates for IoT systems,” Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 37-42, 2015.

[4] Sciancalepore, S., Piro, G., Boggia, G., Bianchi, G, “Public key authentication and key agreement in IoT devices with minimal airtime consumption,” IEEE Embedded Systems Letters, Vol. 9, No. 1, pp. 1-4, 2017.