IoT 환경에서 그룹 기반 통신을 위한 그룹 인증 및 키 교환 기법 설계+

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

Design of group authentication and key exchange scheme for group-based communication in IoT environment

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

요 약

IoT 환경에서는 다양한 센서 디바이스들이 각 디바이스들의 역할과 위치에 따라서 그룹 형태를 이루어 통신을 하게 된다. 그룹 형태의 센서 디바이스들이 통신하는 그룹 기반 통신에서는 수집된 정보를 게이트웨이와 같은 상위 디바이스에게 안전하게 전송해야 한다. 이 때 센서 디바이스들은 게이트웨이와의 인증 과정이 필요하며, 인증 후에 세션키를 분배하여 안전한 통신을 수행할 할 수 있다. 하지만, 일반적인 환경에서는 센서 디바이스의 수가 많아질수록 게이트웨이가 인증을 수행하고 키를 분배하기까지는 매우 큰 오버헤드가 발생하게 된다. 따라서 본 논문에서는 IoT 환경에서 그룹 기반 통신에 대한 보안 요구사항을 분석하고, 그룹 환경에서 사용될 수 있는 그룹 인증 기법에 대해 설계한다.

1. 서론

IoT(Internet of Things) 환경에서는 수많은 센서 디바이스가 서로 연결되어 데이터를 공유한다. IoT 환경에서는 데이터를 실질적으로 수집하여 상위 디바이스에게 전송하는 센서 디바이스들을 연계하여 하나의 소규모 디바이스 그룹을 형성하게 된다. 이러한 소규모 그룹은 상위 디바이스인 그룹 리더(게이트웨이)를 통해 서비스 제공자와 통신하여 사용자 맞춤형 서비스를 제공받거나, 다른 디바이스 그룹과도 통신할 수 있다. 이처럼 센서 디바이스들은 그룹 기반의 통신 형태를 취하게 되며, 안전한 데이터 전송을 위해 그룹 리더와 인증 절차를 거친 후 키를 수신하여 데이터를 안전하게 전송할 수 있다.

하지만, IoT 환경에서는 많은 디바이스가 참여할 수 있으므로, 그룹의 규모가 매우 커질 수 있는데, 그룹에 참여한 센서 디바이스들의 수가 많아지면 그룹 리더는 일일이 센서 디바이스들을 인증하고 키를 분배하는 것이 매우 복잡해질 수 있다. 그룹 간 통신을 수행할 때 하나의 그룹에 참여하고 있는 디바이스의 수가 많아지거나, 여러 디바이스가 동시에 통신을 수행해야 한다면, 안전한 통신을 위해서는 각 디바이스간 세션의 수만큼 인증을 수행한 후 키 교환 과정을 거쳐 통신해야 한다. 이 때 사용될 수 있는 기술은 그룹 인증 기술이다. 그룹 인증 기술은 그룹 기반의 통신에서 매우 효율적인 인증 방법을 제공한다[1].

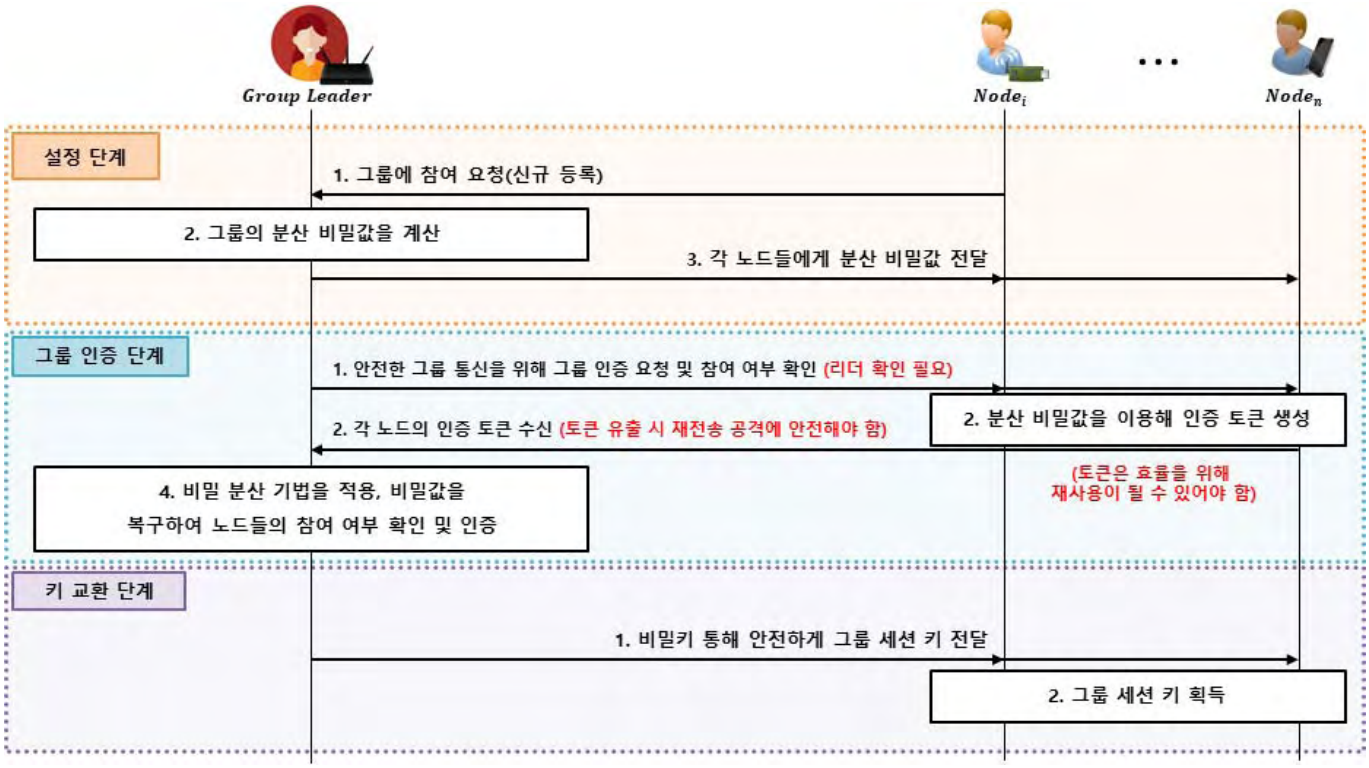
본 논문에서는 IoT 환경에서 그룹 기반 통신에 대한 보안 요구사항을 분석하고, 그룹 환경의 경량 디바이스에서 효율적으로 동작할 수 있는 그룹 인증 기법을 설계한다. 그룹에 참여하고 있는 노드의 수가 많아질수록 그룹 리더에서 발생하는 연산 오버헤드는 매우 커지므로, 그룹 리더에서 인증을 수행할 때 효율적인 방법으로 연산에 대한 오버헤드를 줄이는 과정을 제안하고자 한다. 이를 통해 그룹화된 IoT 환경에서 1:1의 인증이 아닌 동시에 1:N의 인증이 가능하도록 설계한다.

2. 보안 요구사항

본 논문에서 제안하는 그룹 기반 통신에 대한 보안 요구사항은 다음과 같다.

- 인증 : 센서 디바이스인 그룹 참여자는 그룹 리더를 통해 그룹에 참여하고 있는지에 대한 여부와 정당한 사용자인지를 인증해야 한다.
- 재전송 공격 방지 : 인증과 키 교환에 사용되는 중간 값이 공격자에게 노출되어도 공격자는 값을 그룹 리더에게 재전송하여 정당한 사용자로 인증받을 수 없어야 한다.
- 효율성 : 그룹의 규모가 커질수록 그룹 리더에 대한 연산 오버헤드가 커진다. 따라서, 그룹 인증 및 키 교환

+ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)



(그림 1) 제안 방식 시나리오

과정에 있어서 그룹 리더 측면에서의 효율성을 제공해야 한다.

3. 제안 방식 설계

본 논문에서는 2013년 Harn이 제안한 그룹 인증 방식[2]과 2017년 Chien이 제안한 그룹 인증 방식[3]에서 나타나는 취약점을 분석하고, 이에 대해 그룹 리더가 고정되어 있는 환경에 적합한 방식을 설계한다.

Harn은 Shamir의 (t,n)-Threshold 기법을 이용한 기본적인 그룹 인증 기법을 제안하였으며, 이를 응용한 Asynchronous 그룹 인증 기법, Asynchronous 그룹 인증 기법에서 비밀 조각을 여러 번 사용하기 위한 Asynchronous Multiple 기법을 추가로 제안하였다. Asynchronous Multiple 기법이 가장 개선된 방식이지만, 통신상에서 전송되는 분산 비밀 조각을 수집하여 비밀 값을 복구할 수 있는 문제가 있어, 외부의 공격자가 이를 활용하여 그룹 인증에 참여할 수 있게 된다.

Chien은 Harn의 기법을 개선한 그룹 인증 기법을 제안하였는데, 타원곡선 이산대수 문제를 이용하여 통신상에서 전송되는 비밀 조각을 공격자가 수집하여도 비밀 값을 복구할 수 없기 때문에 기존의 문제를 해결하였다. 하지만, Chien 방식에서는 타원곡선 이산대수 문제에 사용되는 타원곡선상의 임의의 점 리스트를 사전에 안전하게 분배해서 사용하게 된다. 이는 사전에 분배된 점 리스트를 모두 사용하면 재분배가 필요하게 되는 문제가 있다.

(그림 1)은 위 두 방식을 분석하고 설계한 IoT 환경의 그룹 기반 통신에 적합한 시나리오이다. 그룹 인증 단계에서 그룹의 참여하고 있는 센서 디바이스(노드)들에게 그룹 인증 요청을 할 때, 악의적인 리더에 대해 확인하는 방안이 필요하다. 또한, 분산 비밀 조각을 이용해 토큰을 생성하여 그룹 리더에게 전송하는데, 토큰은 재사용이 될 수 있어야 한다. 토큰이 그룹 리더에게 전송될 때, 공격자에게 토큰이 유출되어도 공격자는 토큰을 이용해 비밀 값을 계산할 수 없어야 한다.

4. 결론

본 논문에서는 IoT 환경에서 효율적으로 수행될 수 있는 그룹 인증 및 키 교환 기법을 설계하였다. 그룹 인증은 IoT 환경의 발달로 최근 많은 연구가 진행되고 있는 분야로, 좀 더 다양한 환경에 맞도록 지속적인 연구가 진행되어야 한다. 또한, 이후에는 그룹 리더의 메모리에 대한 오버헤드를 줄이고, 동시에 디바이스 측면에서의 연산량을 줄이는 방향으로 연구가 필요할 것으로 판단된다.

참고문헌

[1] W. T. Su, W. M. Wong, and W. C. Chen, "A survey of performance improvement by group-based authentication in IoT," Applied System Innovation (ICASI) 2016 International Conference on. IEEE, pp. 1-4, 2016.

[2] L. Harn, "Group authentication," IEEE Transactions on computers, Vol. 62, No. 9, pp. 1893-1898, 2013.

[3] H. Y. Chien, "Group Authentication with Multiple Trials and Multiple Authentications," Security and Communication Networks 2017, 2017.