센서 기반 IoT 환경에서 자원 효율성을 고려한 경량화 인증 기법

이재승*, 전문석*, 강정호*
*숭실대학교 컴퓨터학과
e-mail : ljs0322@ssu.ac.kr

Lightweight Authentication Method Considering Resource Efficiency in Sensor Based IoT Environment

Jaeseung Lee*, Moon-Soeg Jun*, Jungho Kang*
*Dept of Computer Science & Engineering, Soongsil University

요 약

최근 무선 통신 기술과 센서 디바이스들의 발달로 센서 기반 IoT 환경이 다양한 분야에 활용되고 있다. 하지만, 센서 네트워크 환경을 구성하는 센서 노드는 대부분 소형 하드웨어로 구성되어 있어 메모리, 처리능력, 에너지 등에서 많은 제약사항을 가지고 있다. 또한, 이기종 센서간의 통신 절차도 필요하다. 따라서, 본 논문에서는 DisTance-Bounding 프로토콜과 해시 함수를 이용하여 센서 노드간 인증 및 키 교환을 경량화 기법을 제안한다. 제안하는 시스템은 숲이나 군사지역 등 사람이 접근하기 어려운 곳에 활용되는 센서 노드들의 배터리 수명을 향상시켜 효율적이고 지속적인 데이터 수집이 가능할 것으로 기대된다.

1. 서론

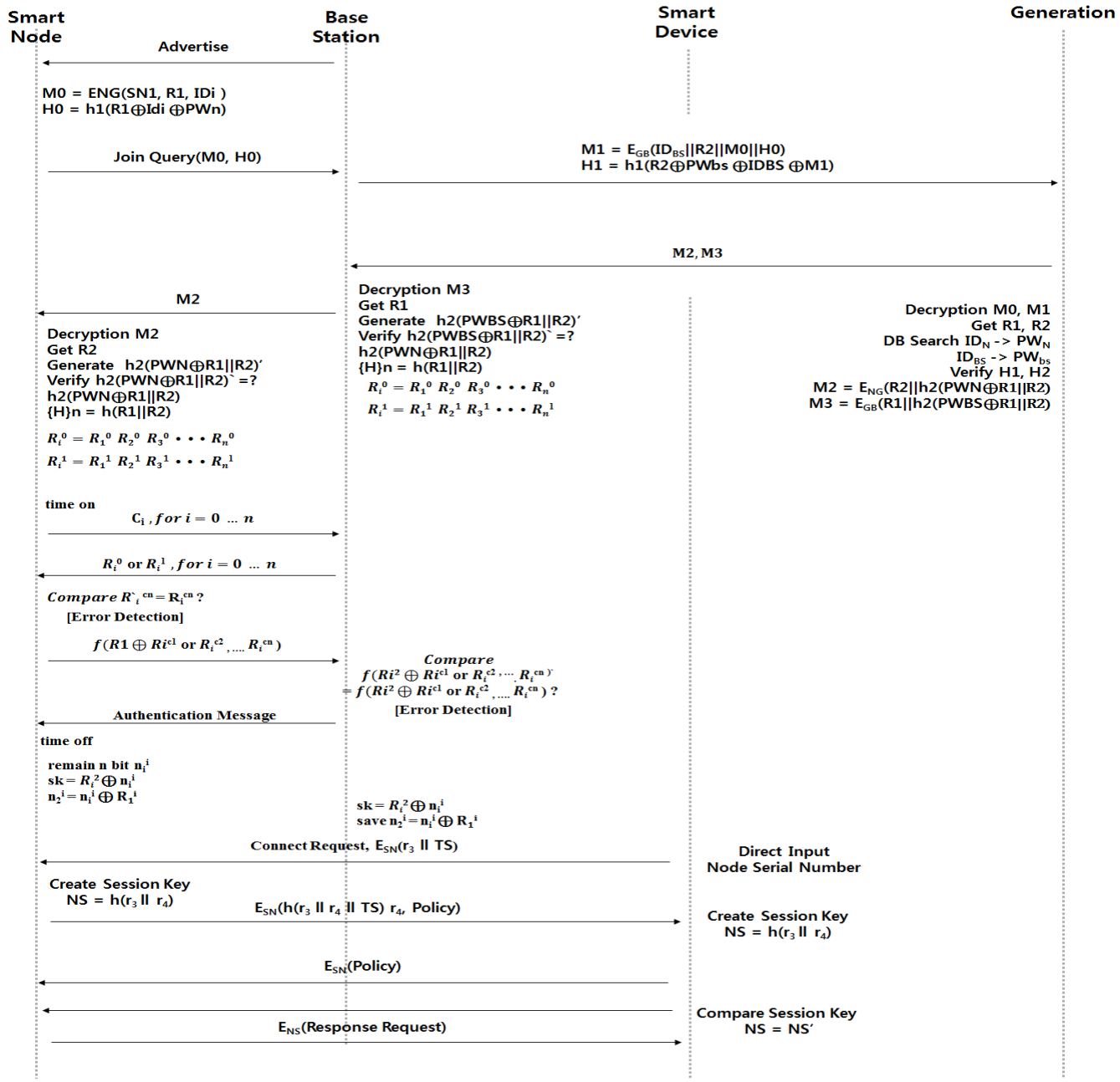
사물인터넷(Internet of Things)은 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 말한다. IoT환경에서는 지능형 서비스를 위해 다양(variety)하고 방대한 양(volume)의 디바이스 정보를 수집하며, 사용자를 정보를 기반으로 서비스를 제공받고 디바이스를 제어한다. 최근에는 무선 통신 기술과 센서 디바이스들의 발달로 무선 센서 네트워크(wireless sensor networks)기술에 기반한 IoT(Internet of Thing) 환경이 의학, 군사, 상업 등 다양한 분야에서 활용 되고 있다. 특히, 소형의 센서, 스마트 더스트를 활용하여 사람들 쉽게 접근하기 어려운 숲이나 군사 지역 등에 스마트 더스트를 뿌려놓고 해당 지역의 데이터를 수집하는 센서 기술이 미래 IT 기술로서 각광받고 있다. 이러한 스마트 더스트를 활용한 IoT 환경은 무선 센서를 이용해 데이터를 감지하고 이 정보를 베이스 스테이션이나 중간노드 들로 전송하는 센서 노드들로 구성 되어 있다. 이때, 이러한 환경에서 활용되는 센서 들은 소형 하드웨어로 구성되어 있어 한정된 메모리, 처리능력, 에너지 등에 제약의 한계를 가지고 있고, 이로 인해 제한된 자원을 최대한 활용할 수 있는 다양한 연구가 진행되고 있다.

따라서, 본 논문에서는 제한된 자원을 최대한 활용할 수 있도록 에너지 효율성을 고려하여, 연산량, 속도, 저장 공간 등에 크게 제약이 없는 해시함수에 기반한 경량화된 상호 인증 및 키 교환 방법을 제안한다.

2. 사물인터넷

인터넷을 기반으로 한 사물 지능통신 기술인 IoT(Internet of Things)는 소형 센서를 포함한 이기종 스마트 기기 간의 상호 접속 네트워크를 제공 하는 기술이다. 따라서 IoT 환경에는 센서 및 컴퓨터의 파워, 메모리의 저장공간, 배터리 량, 통신 대역폭 등 다양한 환경적 특수성을 고려해야 한다. 이에 IETF 표준화 기구의 LWIG(Light-Weight Implementation Guidance)에서는 IoT 환경을 구성 하는 장치들을 자원의 제한적인 정도에 따라 클래스 0부터 클래스 2까지 구분하고 있다. 특히 Class 0에는 메모리가 10KiB 이 하이고, 최대 적재 가능한 코드 크기가 100KiB 이하의 초경량화 장치들이 포함된다. 따라서, LWIG에서 지정하는 Class 0의 장치들은 비용이나 효율성을 고려하여 LLN (Low Power Lossy Network)으로 분류되는 IEEE 802.15.4나 저전력(Low Power) 통신 등의 접속 기술을 사용해야 한다.

서로 다른 성능을 가진 센서나 스마트 디바이스 등 이기종의 장치들은 네트워크 통신을 통해 빌딩 자동화, 환경 모니터링, 에너지 관리, 군사 목적 등 다양한 영역에 활용되고 있으며 이러한 기술들은 IoT 환경을 구성하고 있는 장치 간 상호 인증, 메시지 송신 인증 및 정보의 기밀성 등이 필수 적으로 제공되어야 한다. 현재 IETF CORE 그



(그림 1) 제안 프로토콜

룹에서는 IoT 환경을 위해 CoAP(Constrained Application Protocol)을 표준화 하고 있다. 특히 안전한 서비스 제공을 위해 기존 인터넷 환경에서 사용하던 보안 프로토콜인 DTLS(Datagram Transport Layer Security), HIP등을 자원 제한적인 환경에 맞게 경량화 하여 적용하려 하고 있다. 하지만, DTLS의 경우 전송되어야 하는 총 6번의 메시지 패킷은 fate-sharing 특성을 가지므로, 한 패킷이라도 손실 될 경우 전체 메시지를 다시 전송해야 한다. 메시지 패킷의 재전송은 전송량을 증가시켜 네트워크에 부담을 주고, 소형 센서 디바이스와 같은 제한 적인 장치의 성능이 저하되는 결과를 가져온다. 이 외에도 다양한 환경에서 IoT 환경을 위한 보안 표준화를 진행하고 있지만, 이들이 제안하는 보안프로토콜의 경량화 방안들은 이기종 IoT 환경에서 암호화 모듈을 탑재하지 못하는 초경량 장치들을 모두 수용하는데 무리가 있다.

3. 제안 프로토콜

특정 지역 홈 네트워크를 관할하는 게이트웨이는 지속적으로 광고메시지를 전송한다. 새롭게 네트워크 시스템에 등록되는 스마트 노드는 수신된 광고 메시지에 대한 응답으로 조인 메시지를 전송하며, 게이트웨이는 CA를 통해 스마트 노드를 검증한다. 스마트 노드에 대한 인증이 완료되면, 스마트 디바이스는 원격을 원하는 스마트 노드 인증을 위해 게이트 웨이를 통해 스마트 노드와 상호 인증 및 키 교환을 진행한다. 자세한 인증 및 키 교환 과정은 다음과 같다.

Step 1. 광고 메시지를 수신한 스마트 노드는 본인 인증을 위해 M0, H0를 생성하여 게이트웨이에게 전송한다.

Step 2. M0과 H0을 수신한 게이트웨이는 M1과 H1을 생성하여 제조사 CA에게 전송한다.

Step 3. 게이트웨이로부터 정보를 수신한 CA는 복호화를 통해 두 개의 난수를 획득하며, 검색된 PW를 통해 H0과 H1을 검증한다. 이후, M2와 M3를 생성하여 게이트웨이에게 전송한다.

Step 4. M2, M3를 수신한 게이트웨이는 M3 복호화를 통해 R1을 획득하며, 해시 함수를 통해 수신된 값의 오류가 있는지 검증한다. 검증이 완료되면 Distance-Bounding을 이용한 검증을 위해 두 개의 난수로 생성한 3*n비트의 정보를 저장한다. 이후 스마트 노드에게 M2를 전송한다.

Step 5. M2를 수신한 스마트 노드는 R2를 획득하게 되며, 해시 함수를 통해 전송된 값을 검증한다. 검증이 완료되면, 위의 과정과 같은 방식으로 3*n비트의 정보를 저장한다.

Step 6. 스마트 노드는 인증 절차를 수행하기 위해 랜덤한 수 c_i를 생성하여, 한 비트씩 전송한다. 이때, Relay Attack 방지를 위한 시간 체크를 위해 'Time on' 상태가 된다.

Step 7. 스마트 노드로 부터 비트를 수신한 게이트웨이는 이에 대한 응답으로 c_i 가 0일 경우 R^c의 i번째 비트를, 1일 경우 R^1의 i번째 비트를 스마트노드에게 전송 한다.

Step 8. 스마트 노드는 게이트웨이에게 전송한 c를 기반으로 R_i^{cn}을 생성하며, 클러스터 헤드의 응답 값을 취합한 R_i^{cn}값과 비교하여 올바른 노드로부터 데이터가 전송 되었는지 확인 한다. 또한, Time off 이후 시간 측정을 통해 거리를 유추하여 특정 이상의 시간이 걸렸을 경우 통신을 중단 한다.

Step 9. 게이트웨이를 인증한 스마트 노드는 수신한 R_i^{cn}값들을 f()함수를 이용하여 생성된 값을 게이트웨이에게 전송 한다.

Step 10. 게이트웨이로부터 인증값을 수신한 스마트노드는 동일한 방법으로 인증 값을 생성하여 클러스터 헤드로부터 받은 값과 비교함으로서 스마트노드를 검증하게 된다.

Step 11. 스마트 노드와 게이트웨이는 2*n bit에서 사용하고 남은 n비트를와 랜덤 수를 활용하여 세션 키를 생성 후 인증을 종료 한다.

4. 성능평가

4.1 상호 인증

본 논문에서는 비트를 교환할 때, 각각 게이트 웨이와 스마트 노드가 생성한 난수를 이용하여 R_i^0, R_i^1를 생성하며, 랜덤 값 c에 대한 응답 값으로 약속된 R_i^0, R_i^1를 이용하기 때문에 상호 인증이 가능 하다. 또한 스마트 디바이스 등록의 경우 인증된 게이트 웨이를 활용함으로서 인증이 가능하다.

4.2 Replay 및 Replay Attack

인가되지 않은 공격자가 각 노드 간 전송되어 지는 메시지를 탈취하여 재사용하는 방식의 공격으로, 메시지 재사용 공격 시 메시지를 탈취할 당시의 세션키가 아닌 새롭게 생성한 세션키 $sk = R_1^0 \oplus n_1$와 $f(R_{s1}, R_{s2})$를 사용하기 때문에 이전 메시지의 재사용으로 인한 공격에 대하여 안전하다. 또한, 각 메시지의 경우 타임스탬프 사용을 기본적으로 적용하여, 이후 사용되는 메시지의 시간 만료를 통해 확인이 가능하다. Relay Attack의 경우 비트 교환과정을 통해 각 노드가 물리적으로 근거리에 있는지 판단하여 Relay attack에 안전하다.

4.3 메시지 위변조 공격

인가되지 않은 공격자가 각 노드 간 전송되어 지는 메시지를 탈취하여 공격자가 원하는 목적으로 메시지를 위·변조하는 메시지를 전송하는 방식의 공격으로, 이 또한 마찬가지로 메시지를 탈취한 당시의 세션키가 아닌 새롭게 생성한 세션키 $sk = R_i^0 \oplus n_1$와 를 $f(R_{s1}, R_{s2})$사용하기 때문에 메시지의 위·변조로 인한 공격에 대하여 안전하다.

4.4 에너지 효율성

제안하는 스킴의 경우 디바이스에서 수행되는 연산은 단순 해쉬 연산과 사칙연산에 의존하여 수행함으로써, 타 인증기술에 비해 연산 소모시간이 적다.

5. 결론

본 논문에서는 숲, 산 등이나 군사 지역과 같이 사람이 쉽게 접근 하지 못하는 지역을 위한 센서 기반 IoT 환경에서 센서들의 에너지 효율성을 높이기 위한 경량화된 인증 및 키 교환 방법을 제안하였다. 본 논문은 비트 단위의 인증 방법인 Distance-Bounding 프로토콜과 해시 및 XoR 등을 활용하여, 기존 인증 기법에 비해 에너지 효율성을 높였으며, 보안성 평가를 통해 안전함을 증명하였다. 따라서, 센서 노드를 위한 경량화 및 IoT환경에서 발생할 수 있는 다양한 보안 위협에 대응 가능할 것으로 기대된다..

참고문헌

[1] JUN, Zhang, et al. The internet of things. IEEE Commun. Mag, 2011, 49.11: 30-31.

[2] QIAN, Zhihong; WANG, Yijun. IoT technology and application. Acta Electronica Sinica, 2012, 40.5: 1023-1028.