SPINS 보안 프로토콜 중 SNEP의 구현

*장 범 수 (yellowcape@incheon.ac.kr), 이 기 영
인천대학교 정보통신공학과

Abstract

본 논문에서는 센서 네트워크에 SPINS 보안 프로토콜을 적용하여 그 성능을 판별하려 하였다. 센서 네트워크의 보안을 유지하기 위해 SPINS에서는 SNEP과 μTESLA로 세분화 되어 데이터 인증, 보안과 키 관리를 각각 담당하게 된다. 본 논문에서는 그 중 SNEP을 nesC를 이용하여 TinyOS기반 센서에 적용하였다.

I. 서 론

빠른 속도로 발전하는 IT분야는 이제 유비쿼터스 컴퓨팅(Ubiquitous Computing) 시대를 향해 진보하고 있다.

유비쿼터스 컴퓨팅 환경을 구축하기 위한 필수적인 기술로 센서 네트워크를 꼽을 수 있다. USN(Ubiquitous Sensor Network)은 WSN(Wireless Sensor Network)와도 유사한 의미로 통하는데, 이는 무선으로 네트워크를 구성한 센서들이 주위의 온도, 습도, 균열 정도 등을 측정하고, 측정된 데이터를 컴퓨팅하여 일상생활에 유용한 서비스를 제공할 수 있도록 하는 것이다.

그러나 센서네트워크는 센서들의 한정된 자원(Resource, Battery, etc)과 무선 링크를 사용함으로 인해 데이터가 악의를 가진 사용자에 의해 쉽게 도청, 변조될 수 있는 위험을 노출하고 있으며, 현재 사용되고 있는 유•무선 방식의 통신 보안 프로토콜을 사용하기에는 아주 작은 크기의 패킷만을 전송하는 센서네트워크에서는 오버헤드가 심해질 수 밖에 없다. 따라서 센서네트워크를 위한 다양한 보안 프로토콜들이 제안되었는데, 그 중 SPINS 프로토콜이 많은 관심을 받고 있다.

본 논문은 산업자원부, 한국산업기술평가원 지정 인천 대학교 멀티미디어 연구센터의 지원에 의한 것입니다.

본 논문에서는 센서 네트워크에 적용할 수 있도록 제안된 SPINS 프로토콜 중 SNEP을 구현하여 SNEP이 센서네트워크에 얼마나 적합한지를 알아보고자 한다.

II. 본 론

센서네트워크에 필요한 보안 요구사항은 데이터와 관련된 데이터 비밀성, 데이터 인증, 데이터 무결성, 데이터 신선성과, 노드간의 Broadcasting 통신 방식에서의 인증이다.

SPINS에서는 SNEP(Secure Network Encryption Protocol)과 μTESLA(the 'micro' version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)라는 두 가지 기술로 구분된다.

SNEP에서 제공되는 보안 기능은 다음과 같다.

① Data Confidentiality : 데이터를 비밀키로 암호화하여 수신자 이외의 제 3자는 암호 메시지에서 원래 매시지를 추론할 수 없도록 하는 보안 기능. 암호화에는 Counter Mode를 적용하여 비밀성 보장

② 양단간 데이터 인증 : 송신자 인증으로 데이터를 보낸 송신자가 정말로 해당 패킷을 전송했는지를 확인하기 위해 공유된 키로 MAC을 사용

③ 재사용 방지 : MAC에 counter값을 포함시켜서 Replay attack을 방지

④ Data freshness : 패킷이 가장 최신 패킷 임을 검증

⑤ 낮은 통신 부하 : Counter를 패킷에 담지 않고 각 end node에서 관리

실험을 하기 위해 구성한 네트워크 환경은 다음과 같다.

① 노드의 특징은 다음과 같다.

i. CPU : Atmega 128L Low power 8-bit microcontroller

ii. RF : 2.4GHz, Zigbee

iii. Bps : 250kbps

iv. Power : AAA Size 1.5V*2

v. 128MB SDRAM

② 노드의 개수는 최대 8개로 제한

③ 센서 노드와 base 노드와는 1hop 거리에서 통신

III. 구 현

각 노드는 Master key χ를 가진 채 네트워크를 구성하게 된다.

패킷 암호화에는 RC5를 적용하였으며, 노드들은 초기에 자신의 CTR을 초기화 한 후 Base노드와 CTR을 교환한 후에 패킷을 전송하게 된다.

Base노드는 패킷을 전송한 노드의 CTR와 Master key χ로 패킷을 복호화 하고 MAC과 비교함으로써 데이터 인증을 수행한다.

IV. 결론 및 향후 연구 방향

구성된 센서 네트워크에서 Base노드는 7개의 센서에서만 패킷을 받게 되고, 그로 인해 Base 노드에 부하가 가중되지 않았고 전체 네트워크에도 영향을 미치지 않았다. 또한 SNEP를 적용한 네트워크와 적용하지 않은 네트워크의 센싱 데이터 전송 및 인증 속도를 비교해 보아도 크게 차이 나지 않았다.

일차적으로 SNEP만을 구현하여 적용하였을 때 센서 네트워크의 패킷 전달 속도는 충분히 만족 할만하였다. 하지만 μTESLA를 적용하고, 네트워크가 보다 많은 센서들로 구성되어 있을 때, 라우팅 알고리즘을 적용하였을 때의 상황도 고려해 봐야 SPINS가 얼마나 센서 네트워크에 적합한 지를 결론 지을 수 있을 것이다.

참 고 문 헌

[1] Adrian Perrig, Robert Szewczyk, J.D Tygar, Victor Wen and David E. Culler, *SPINS:Security Protocol for Sensor Network*, Wireless Networks, 2002

[2] Ronald L. Rivest, *The RC5 Encryption Algorithm*, In the *Proceedings of the Second International Workshop on Fast Software Encryption (FSE)*, 1994

[3] TinyOS Tutorial, *http://www.tinyos.net/tinyos-1.x/doc/tutorial/index.html*

[4] David Gay, Philip Levis, David Culler and Eric Brewer, *nesC 1.1 Language Reference Manual*, May 2003