홈 네트워크 보안시스템 설계

*설정환, 이기영
인천대학교 정보통신공학과
e-mail : aknari@naver.com, kylee@incheon.ac.kr

Design of Home Network Security System

*Jeong-Hwan Seol, Ki-Young Lee
School of Information and Communication Engineering
University of Incheon

Abstract

In this paper, the SPINS, a sensor network security mechanism, was researched to design a system to be applied to home network structure and check the security of which degree was ensured by a virtual network of home networking middleware. Sensor Network security mechanism SPINS provides data confidentiality and authentication by SNEP, and provides authenticated broadcast by μTESLA. We designed the system that applied SPINS to home networking middleware basic structure.

I. 서론

최근 활발히 연구되고 있는 유비쿼터스 센서 네트워크(Ubiquitious Sensor Network)는 센서 장치에 네트워크 개념을 추가해서 감지된 정보를 네트워크와 연동하여 관리, 제어하는 것을 말한다. 이와 같이, USN를 이용한 홈 네트워크 서비스는 센서 노드사이의 무선 통신을 기반으로 한다. 하지만 무선 통신은 그 특성으로 인해 보안에 큰 문제가 제기되고 있다. 게다가 홈 네트워크는 개인의 사생활을 보장해야 하는 환경이기에 보안성이 더욱 심각한 문제가 될 수 있다.

본 논문은 센서 네트워크의 보안 기술인 SPINS(Security Protocols Sensor Network)를 통해 데이터의 기밀성, 인증 및 브로드캐스트 인증을 제공하는 알고리즘에 대해 연구하였다. 또한 가상 망에서의 보안 시스템을 설계, 구현하였다.

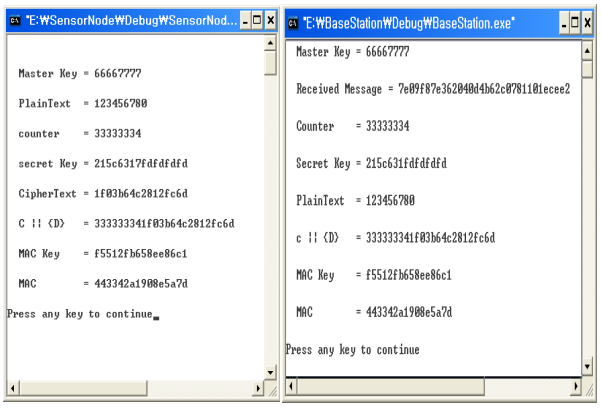
II. 본론

2.1 SPINS

센서 네트워크 보안의 대표적인 기술인 SPINS는 데이터의 기밀성과 인증을 제공하는 SNEP(Secure Network Encryption Protocol)와 브로드캐스트 인증을 제공하는 μTESLA로 구성되어있다. SNEP는 전송 시 메시지 당 8바이트의 낮은 오버헤드를 가지며 CBC(Cipher block chain) 방식을 사용하여 데이터를 암호화하며 카운터 모드(CTR)를 적용하여 데이터의 기밀성을 보장한다. 또한 MAC(Message Authentication Code)를 사용하여 데이터 인증을 제공한다. 홈 네트워크에서는 공격자가 센서 노드로 위장하여 공격하는 경우를 대비하여 BS(Base Station)와 노드간의 인증이 이루어져야 한다. μTESLA는 BS에서 센서 노드로의 브로드캐스트 인증을 제공한다. μTESLA는 기존의 TESLA 방식의 높은 연산량과 오버

헤드를 개선하여 센서 네트워크에 적합한 메커니즘이다. μTESLA는 단방향 키체인 방식을 사용하며, 이를 위해 송신자와 수신자가 서로 시간 동기화가 이루어져야한다. 또한 암 호화, 키 생성, MAC 생성 등을 위해 RC5 알고리즘을 사용한다.

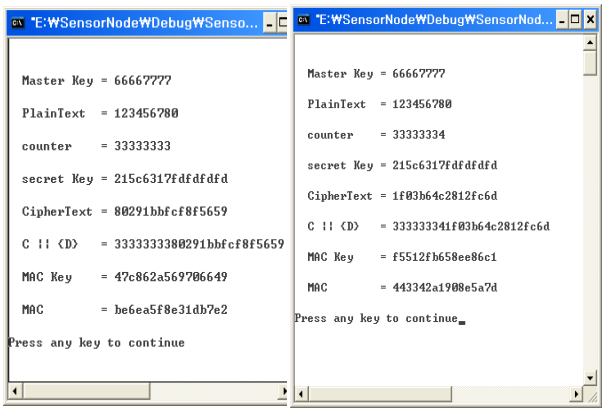
Ⅲ. 구현



(a) Mac generation of node A (b) Message encryption and authentication of node B

그림 1. MAC generation and Implementation of SNEP

그림 1.(a)는 노드 A에서 평문(plaintext)과 마스터키, 카운터가 주어졌을 때 생성된 MAC 값을 보여주고 있다. (b)는 노드 A가 메시지를 암호화하고 MAC과 함께 노드 B에게 보냈다. 노드 B는 미리 알고 있는 A의 카운터를 이용해 비밀키를 생성하고 메시지를 복호화하는 과정을 볼 수 있다. 또한 MAC키를 생성하고 MAC 을 얻어 A 노드의 MAC 값과 일치하여 정당한 송신자로부터의 메시지임을 확인할 수 있다.



(a) Initialization of counter (b) Incrementation of counter

그림 2. Comparison of ciphertext by counter increasement

그림 2은 IV로 작용하는 카운터가 증가했을 경우, 같은 내용의 평문이 전혀 다른 방향으로 암호화되는 것을 확인할 수 있다. 즉 공격자가 비밀키를 공격하여 탈취하더라도 앞으로 생성되는 메시지에 대해 원래의 평문으로 복호화할 수 없게 되는 것을 확인할 수 있다.

표 1 Measurement of SNEP computation

라운드 횟수	연산량 (k = 비례상수)
10	k • 40
20	k • 80
30	k • 120
40	k • 160
50	k • 200
60	k • 240

표 1의 결과는 SPINS 에서 사용하는 보안 알고리즘은 라운드 횟수에 따라 연산량이 산술적으로 증가하는 것을 알 수 있었다. 이는 라운드횟수가 약간의 변동이 있더라도 연산량에 미치는 영향은 상대적으로 크지 않아 센서 노드의 연산량 부담을 줄일 수 있는 요소로 볼 수 있다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 SPINS를 이용해 홈 네트워크 보안시스템을 설계, 구현해 보았다. μTESLA를 통한 브로드캐스트 인증과 SNEP을 이용한 데이터의 기밀성 및 데이터 인증이 보장되었다. 이를 통해, 센서 네트워크가 보안에 취약하다는 문제점을 해결할 수 있다. 또한 향후 센서 네트워크의 현실 적용에 대한 연구가 계속 되어야 할 것이다.

참고문헌

[1] Adrian Perrig et al, "SPINS : Security Protocols for Sensor Networks", Wireless Networks Journal, 8:521-534, 2002.
[2] William Stallings, "Cryptography and Network Security", Pearson, Education, 2003.
[3] 강주성 등, "현대 암호학", 경문사, 서울, 2002.
[4] W.Keith Edwards, "Core Jini", 영한출판사, 2002.
[5] Feng Zhao and Leonidas Guibas, "Wireless Sensor networks", Elsevier, 2005.
[6] William Stallings, "Network Security Essential", Prentice Hall, Upper Saddle River, 2005.