홈 네트워크를 위한 보안 시스템 구현에 관한 연구

설정환, 김인겸, 이기영

인천대학교 정보통신공학과

A Study of Implementation for Home Networking Security System

Jeong-hwan Seol, In-Kyum Kim, and Ki-young Lee

Dept. of Information and Telecommunication Engineering, University of Incheon

E-mail : kylee@incheon.ac.kr

요 약

본 논문에서는 홈 네트워크 서비스를 위한 인증 시스템을 설계, 구현하였다. 무선 센서 네트워크에서의 키 관리 기법인 대칭키 사전 분배 방식을 적용하여 인증키의 노출을 방지하였다. 또한 TinyOS의 TOS_Msg 구조를 변형하였다. TOS_Msg는 29바이트의 데이터 배열을 사용자에 의해 변경 가능하도록 제공하고 있다. 이 데이터 배열에 8바이트의 인증키를 저장하였다. 또한 SPINS를 기반으로 RC5를 사용하여 인증키 및 데이터의 암호화 및 복호화를 수행하였다. 실험을 통해 다른 그룹의 센서 노드와 베이스 스테이션(BS) 사이의 통신 및 악의적인 목적을 가지고 추가된 센서 노드와의 통신으로 인한 오작동을 방지할 수 있음을 확인하였다.

ABSTRACT

In this paper, we design and implement the authentication system for home network service and applied it to actual sensor nodes. We achieved authentication key, encryption and decryption applied RC5 encryption algorithm of SNEP. In addition, we used pair-wise key pre-distribution for prevention of authentication sniffing in wireless sensor network. The experiment environment consists of a base station receiving data and sensor nodes sending data. Each sensor nodes sends both the data and encrypted authentication key to the base station. As a simulation environment, we assumed some what-if scenarios of security menaces in home network service. And we slightly altered the TOS_Msg construction of TinyOS. The experiences had shown that the malfunction doesn't happen in communication among other groups. And we confirmed in tests that the system is secure when a sensor having malicious propose is added.

키워드

Home Networking, SPINS, 키 관리, 인증

Ⅰ. 서 론

홈 네트워크 서비스는 다양한 유.무선 네트워킹 기술을 적용하여 댁내의 모든 가전 기기는 물론 사용자가 항상 휴대하고 다니는 핸드폰, PDA등을 하나의 네트워크로 구성하여, 가정기기를 내. 외부에서 제어할 수 있게 해준다. 뿐만 아니라 비상 상황이 발생했을 경우 사용자의 위치에 상관없이 이를 통보하고 또 이에 대한 적절한 조치를 취함으로써, 개개인의 생활을 더 편리하고 안전하며 즐겁고 윤택한 삶을 영위할 수 있게 해 주는 핵심적인 기술로 이를 통해 커다란 시장을 형성할 수 있는 미래의 신 성장 동력 산업이다. 설치가 어려운 홈 네트워크 장비 및 가전을 쉽게 연동할 수 있는 기술로서 무선 네트워크는 가장 중추적인 역할을 수행할 것 이다. 그중에서도 센서 노드를 이용한 유비쿼터스 센서 네트워크 (USN) 서비스는 홈 네트워크 서비스뿐만 아니라 홈 헬스-캐어 서비스 및 홈타운 서비스에 이르기까지 가장 핵심적인 기술이 될 것이다.

그러나 USN에서 사용되는 센서 노드는 일회성, 저전력, 작은 기억공간, 제한된 계산 능력 등의 특징을 갖는다. 또한 통신 수단으로는 Zigbee, Bluetooth 등의 무선망을 사용하게 된다. 이러한 제약은 센서 네트워크의 보안성을 매우 취약하게 하는 요소이다. 무선망 사

용으로 인해 도청, 감청, 패킷 스푸핑 등의 공격을 당하기 쉬우며 위에서 언급한 제약사항으로 인해 지금까지 연구된 강력한 보안 알고리즘을 적용시키는데 한계가 있다. 따라서 센서 네트워크에서는 데이터 기밀성, 데이터 인증, 데이터 무결성, 데이터 신선성 등이 고려되어야 하며 환경에 맞는 키관리 기법, 그룹 기반 키관리, Pair-wise 키 관리 등이 센서 네트워크 구조와 같이 연구되어야 한다.

본 연구에서는 무선 센서 네트워크를 활용한 홈 네트워크 서비스에서의 보안 위협사항 및 요구사항을 분석하고 데이터 기밀성 및 인증을 제공하는 SPINS (Security Protocols Sensor Networks)의 SNEP (Secure Network Encryption Protocol)과 안전한 키 관리 기법에 대해 연구하였다. 또한 홈 네트워크 미들웨어인 Jini의 구조를 기반으로 하여, 위의 알고리즘이 적용 가능한 보안 시스템을 설계하고 구현하였다.

Ⅱ. 홈 네트워크의 보안 위협 및 요구 사항

그림 1은 홈 네트워크에서 발생될 수 있는 보안 취약성을 정리한 것이다. 인터넷 등에서 발생되던 취약성이 홈 네트워크 내부 망에서도 그대로 발생됨을 알 수 있다.

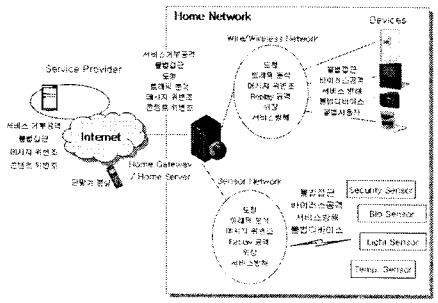

그림 1. 홈 네트워크의 보안 위협 요소

특히, 홈 네트워크를 구성하는 센서 노드 및 정보 가전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안 기능의 탑재가 어려우므로 사이버공격에 이용되거나 목표가 될 가능성이 더욱 높다. 게다가 향후 홈 네트워크 서비스에서는 헬스-케어 서비스, 실버타운과 같이 생명과 직결된 생체 신호들과 홈-타운 전체의 안전에 영향을 주는 신호들의 사용이 증가할 것으로 예상된다. 따라서 안전한 홈 네트워크 서비스를 위해서는 데이터 기원 인증, 명령권한 인증, 인증메시지 무결성 보호, 메시지 재생 방지, 키 분배의 보안 요소가 고려되어야 한다[1].

Ⅲ. 인증프로토콜과 암호화 알고리즘

3.1 LEAP:로컬 암호화와 인증 프로토콜

S. Zhu는 in-network 프로세싱을 제공하는 센서 네트워크를 위한 키 관리 프로토콜 LEAP (Localized Encryption and Authentication Protocol)을 제안했다[3]. LEAP은 다른 안전성 요구사항을 만족시키기 위해 4가지 형태의 키(개인 키, Pair-wise 키, 클러스터 키, 그룹 키)를 사용하고, 센서 네트워크의 실질적인 면을 고려했다는 점에서 의미가 있다.

3.2 SNEP

SNEP은 센서 네트워크 보안의 대표적인 기술인 SPINS에서 데이터의 기밀성과 인증을 제공하는 부분으로 전송 시 메시지 당 8바이트의 낮은 오버헤드를 발생시키며, 양단간 카운터를 이용하여 암호화시키는 장점을 가진다. SNEP는 다음의 보안요소를 제공한다.[4]

● 데이터 기밀성

SNEP에서는 CBC(Cipher block chain) 방식을 사용하여 데이터를 암호화한다. CBC 방식의 암호화 기법은 공격자에 의해 암호화키를 스푸핑 당할 경우, 모든 메시지를 바로 복호화 할 수 있게 된다. 그래서 SNEP은 카운터 모드(CTR)를 적용하여 데이터의 기밀성을 보장한다.

● 3.2.2 데이터 인증

공격자의 공격 유형 중 위장, 내용 수정, 순서 수정, 메시지의 지연과 재전송 등의 공격에 대처하기 위한 방법으로 인증이 사용된다. SNEP은 올바른 송신자가 데이터를 전송하였는지 검증하기 위해서 메시지 인증 코드 (MAC)를 사용한다[5].

● 데이터 무결성

데이터 및 네트워크 보안에 있어서 정보가 인가된 사람에 의해서 만이 접근 또는 변경 가능하다는 확실성으로서, 데이터 인증을 통해 보장된다.

3.3 RC5(Ron's Code 5) 알고리즘

RC5 암호화 알고리즘은 SPINS에서 암호화, 키 생성, MAC생성 등에 사용되는 주요 알고리즘으로 입출력 크기, 키크기, 라운드 수가 가변인 블록 알고리즘이다[6].

Ⅳ. 암호화 알고리즘을 적용한 홈 네트워크 보안 시스템 설계

4.1 Jini

Jini는 크게 서비스 제공자와 이 서비스를 이용하는 클라이언트, 그리고 서비스 제공자와 클라이언트를 연결해주는 역할을 하는 Lookup 서버 세부분으로 구성된다. 그림 2와 같이 각 기기는 Lookup 서버에 자신을 등록하고 클라이언트는 Lookup 서버에 사용하고자 하는 기기를 요청한다. Lookup 서버는 요청받은 기기를 검색하여 클라이언트에 통보해주면 클라이언트는 요청한 기기를 사용하게 된다. 그림 2는 Jini의 기본 구조를 나타낸다.[2]

4.2 암호화 알고리즘을 적용한 시스템 구현

BS는 각 센서노드와 Zigbee를 이용하여 메시지를 주고받는다. 센서 노드는 측정된 데이터를 인증키와 함

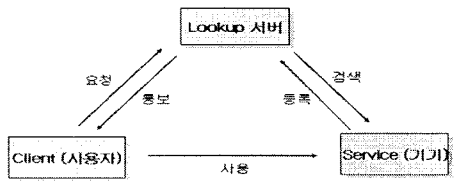

그림 2. Jini의 기본구조

께 BS로 보냄으로써 사용자 식별이 가능하게 된다. 또한 데이터를 암호화함으로써 기밀성을 보장한다. 그림 3은 암호화 알고리즘을 적용한 보안 시스템의 구조를 보여준다.

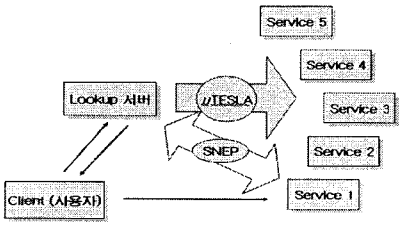

그림 3. SPINS이 적용된 시스템 구성

4.3 실험 환경 및 실험 방법

TinyOS에서 센서 노드와 BS 사이의 통신에서 사용되는 TOS_Msg 구조를 변형하였다. TOS_Msg는 사용자에 의해 변경이 가능한 29byte의 데이터 공간을 제공한다. 이를 수정하여 비밀 키를 할당하였다. 또한 RC5 알고리즘을 적용, 공유키를 이용하여 BS와 각 센서노드가 공유하는 비밀 키를 암호화하고, 전송되는 데이터를 암호화함으로써 안전한 통신이 가능케 하였다.

4.4 제안하는 TOS_Msg 구조

Addr (2bytes)	Type (1byte)	Group (1byte)	Length (1byte)	Data (29bytes)	CRC (2bytes)

Source MoteID (2bytes)	LastSample Number (2bytes)	Channel (2bytes)	Sub (4byte)	Key (4byte)	Data (20bytes)

그림 4. 제안된 TOS_Msg 구조

그림 4는 제안하는 TOS_Msg 구조를 보여준다. 안전한 통신을 위해서 BS와 각 센서 노드는 생성된 공유키와 비밀 키를 사전분배 방식을 통해 저장하게 된다. 그리고 각 센서 노드는 공유키를 이용하여 비밀 키를 암호화 하게 되고 암호화된 비밀 키를 Sub(4bytes), Key(4bytes)로 나누어서 수집된 데이터와 함께 BS로 전송하게 된다. 따라서 암호화된 비밀 키가 노출이 되더라도 암호화 공유키는 노출되지 않기 때문에 안전한 통신이 가능하다.

V. 구현 결과 및 분석

5.1 다른 그룹에 속한 노드와 BS 사이의 통신

그림 5는 A그룹과 B그룹 사이의 통신으로 인한 보안 위협사항을 보여준다. A그룹의 BS는 자신의 그룹 내에 속한 센서 노드들의 데이터만을 수신해야 하지만 B그룹의 센서 노드의 데이터를 수신함으로써 장비의 오작동을 유발할 수 있다. 이를 막기 위해, 센서 노드는 암호화된 비밀 키를 전송하여 BS이 자신의 그룹에 속한 노드임을 인증케 함으로써 안전한 통신을 할 수 있다. 그림 6은 센서 노드가 암호화된 비밀 키를 수신된 데이터와 함께 보내는 것을 보여준다. 그림 7은 BS이 암호화된 비밀 키를 복호화해서 인증된 노드 여부를 확인하는 것을 보여준다.

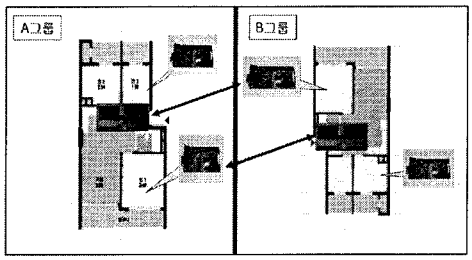

그림 5. A와 B그룹간의 통신환경 설정

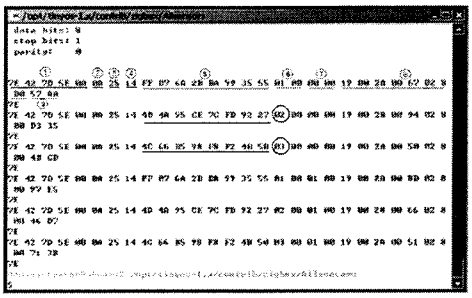

그림 6. 암호화된 비밀키 전송

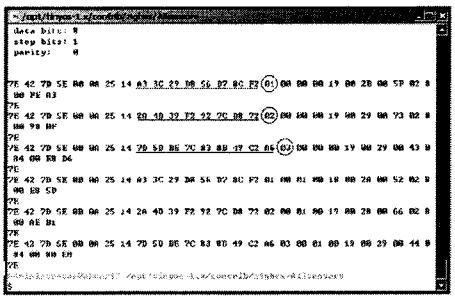

그림 7. 인증 노드의 확인

그림 6과 7는 Java 응용 프로그램을 통해 BS에 정상적으로 수신된 각 센서노드의 데이터를 16진수로 보여주고 있다. 수신된 데이터의 각 바이트는 ①~⑨로 구분된다. ①은 데이터의 시작을 알리는 (7E 42)와 센서 노드에서 사용되는 ADDR 값인 (7D 5E 00)로 구성된다. ②는 MSGTYPE, ③은 그룹 ID(GID), ④는 메시지 길이(MSGLEN), ⑤는 TOS_Msg의 Data 배열의 시작으로 비밀 키를 저장한 8bytes 값이다. ⑥은 노드 넘버, ⑦은 수신된 데이터의 샘플링 넘버를 의미한다. ⑧은 센서의 데이터 값으로 온도, 조도, 습도 값을 의미한다. ⑨는 CRC, 마지막 7E는 데이터의 끝을 나타내는 값이다. 같은 그룹의 1번, 2번, 3번 센서 노드의 데이터는 정상적으로 수신이 되고 다른 그룹에 속한 노드로부터 전송되는 데이터는 수신되지 않는 것을 확인할 수 있다.

5.2 다른 그룹에 속한 노드와 BS 사이의 통신

그림 8은 악의적인 목적을 가지고 공격자에 의해 추가된 센서 노드가 BS에게 공격자에 의해 만들어진 데이터를 전송함으로써 장비의 오작동을 유발시키는 위협이 발생할 수 있음을 보여준다.

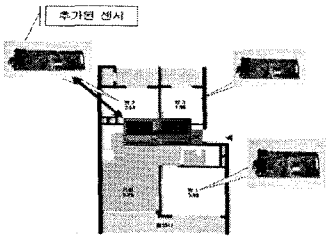

그림 8. BS와 공격 노드 사이의 통신

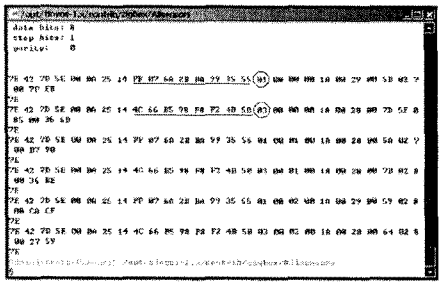

그림 9. 비인가 노드의 데이터 폐기

그리고 그림 9는 공격자로부터 전송되는 데이터를 폐기하는 것을 보여준다. 2번 센서 노드가 공격자의 의해 추가된 노드일 경우 BS에서는 각 센서 노드로부터 암호화된 비밀 키를 수신하고 이 비밀 키를 복호화 함으로써 자신의 그룹 내에 속한 노드인지 여부를 판단하게 된다. 이렇게 비밀 키를 이용한 인증을 통해 2번 노드로부터 전송되는 데이터를 폐기하게 된다.

5.3 공격자가 임의의 메시지를 재사용하는 경우

메시지 재생 공격의 경우, 위의 여러 시나리오와는 다르게 동일한 데이터를 계속해서 보냄으로써 예기치 않은 결과를 초래할 수 있다. 이러한 공격을 막기 위해서 RC5 알고리즘에 CRT 모드를 적용하여 암호화하게 된다. 결국 BS는 이전에 수신된 센서 노드의 비밀 키가 다시 사용되더라도 그 값은 현재의 값과 다르기 때문에 공격자에 의한 데이터 여부를 결정할 수 있게 된다. 그림 10은 암호화에 CRT 모드가 적용되었음을 보여준다. 이 경우 동일한 데이터인 경우에도 암호화가 수행된 후에 전혀 다른 데이터가 전송된다.

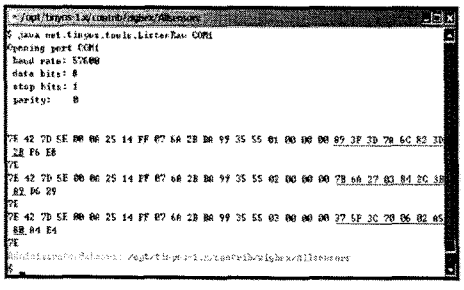

그림 10 카운터 모드가 적용된 암호화

VI. 결론 및 향후연구과제

본 논문은 기존의 홈 네트워크 미들웨어의 구조를 바탕으로 불법적인 접근을 통한 공격이나 데이터의 유출 가능성 및 디바이스의 오작동에 대한 대책으로 인증 시스템을 구현해 보았다. 안전한 키 관리를 위해 사전 키 분배 방식을 적용하여 키 노출을 방지하고 개인 키, 그룹 키, 클러스터 키와 같이 계층적인 키 구조를 적용하였다. 이런 계층적인 키 구조는 U-City와 같은 서비스 환경에도 적용 가능할 것이다. 또한 센서 네트워크 보안 메커니즘인 SPINS의 SNEP를 이용하여 비밀 키 및 수집된 데이터를 암호화함으로써 낮은 오버헤드와 적은 연산량으로 안전한 통신을 가능하게 하였다.

본 논문에서는 인증 구현 방법으로 공유키를 각 센서 노드에 사전분배 함으로써 공유키의 노출을 방지하였고, TOS_Msg를 변경하여 인증에 필요한 비밀 키를 각 센서 노드에 저장하였다. 제안하는 TOS_Msg는 29 바이트의 데이터 배열에 8바이트의 비밀 키를 저장함으로써 인증에 필요한 공유키와 비밀 키를 센서 노드에서 사용 가능하게 된다. 공유키는 각 센서 노드와 BS 사이의 통신에서 노출되지 않기 때문에 안전성이 보장된다. 비밀 키는 공유키로 암호화되어 전송되기 때문에 공격자에게 노출되더라도 기밀성을 유지할 수 있다.

RC5 알고리즘을 이용, 비밀 키를 암호화하여 센서노드와 BS 간의 인증 과정을 수행하였다. 이 때 인증과정을 통과하지 못하게 되면 데이터는 바로 폐기된다. 인증과정을 통해 통신이 원활히 이루어지는 것과 불법적인 데이터는 폐기 되는 것을 Java 응용 프로그램을 통해서 검증할 수 있었다.

향후 과제로는 홈 네트워크와 홈 네트워크를 연결하는 클러스터 단위의 네트워크에서의 인증 방법을 적용해보고 연산량, 배터리 등을 측정하여 효율적인 알고리즘으로 개선하여야 할 것이다. 또한 멀티 홉 기반의 네트워크에 대한 암호화 알고리즘의 구현에 대한 연구도 진행 되어야 할 것이다.

참고 문헌

[1] 한종욱 외2인,"홈네트워크 보안기술 동향", 한국통신학회지 제23권 9호, pp.113-124, 2006년.

[2] 김연숙 외2인, 홈네트워크에서의 미들웨어", 한국통신학회지 17권 11호, pp.90-100, 2000년.

[3] S. Zhu, et al, LEAP: Efficient Security Mechanism for Large-Scale Distributed Sensor Networks, 10th ACM Conf. on Computer and Comm. Security, pp.62-72, 2003.

[4] Adrian Perrig et al, SPINS, Wireless Networks Journal, 8: pp.521-534, 2002.

[5] William Stallings, Cryptography and Network Security, Pearson, Education, 2003.

[6] R. Rivest, The RC5 encryption algorithm, WS on Fast Software Encryption. pp.86-96, 1995.