홈 네트워크 서비스를 위한 인증시스템 구현에 관한 연구

이 기 영*

A Study on Implementation of Authentication System for Home Networking Service

Ki Young Lee*

이 논문은 인천대학교 2007년도 자체연구비 지원에 의하여 연구되었음

요 약

본 연구에서는 홈 네트워킹 서비스를 위한 인증 시스템을 설계하고 이것을 실제 센서 노드에 적용하였다. 무선 센서 네트워크의 키 관리 기법인 대칭키 사전 분배방식과 계층적인 키 구조를 적용하여 인증키의 노출을 방지하였다. 또한 SPINS를 기반으로 CBC(cipher block chain) 방식의 RC5 암호화 알고리즘을 적용하여 인증키 및 데이터의 암호화를 수행하였다. 베이스 스테이션(BS)과 센서 노드로 실험 환경을 구축하였고, 각 센서 노드들은 수신된 데이터를 암호화된 인증키와 함께 BS로 전송하게 된다. 실험은 홈 네트워크 서비스에서 발생할 수 있는 보안 위협에 대한 시나리오를 설정하여 진행하였다. 이를 위해 TinyOS의 TOS_Msg 데이터 구조를 약간 변경하여 인증을 위한 8바이트의 인증키를 저장하고 각 센서 노드의 인증 및 데이터의 암호화를 가능하게 하였다. 이를 통해 다른 그룹의 센서노드와 BS 사이의 통신 및 악의적인 목적으로 추가된 센서 노드와의 통신으로 인한 오동작을 막을 수 있었고 생체신호와 같은 중요한 데이터를 전송하는 경우 암호화를 통한 안전한 홈 네트워킹 서비스가 가능함을 확인하였다.

ABSTRACT

In this paper, we designed the authentication system for home network service and applied it to actual sensor nodes. The pair-wise pre-distribution key skim is applied for prevention of authentication key from sniffing on the wireless sensor networks. The authentication key and data are encrypted by using the CBC mode RC5 algorithm based on the SPINS. The experimental environment consists of a base station (BS) and sensor nodes and each sensor node sends both sensing data and the encrypted authentication key to the BS. For simulations we set up some what-if scenarios of security menaces in home network service. Slightly modified the TOS_Msg data arrays of TinyOS is suggested to store 8-byte authentication key which can enable data encryption and authentication at the each sensor node. As a result, malfunction caused by communication between BS and nodes of other groups of added nodes having malicious purpose can be protected. Also, we confirmed that a critical data of home networking service like vital signal can be transmitted securely through this system by encryption technique.

키워드

Home Networking, Sensor Network, Authentication, Key management

* 인천대학교 정보통신공학과

접수일자 2009. 03. 17
심사완료일자 2009. 04. 06

Ⅰ. 서 론

유비쿼터스 센서 네트워크(Ubiquitous Sensor Network, USN)는 센서 장치에 네트워크 개념을 추가해서 감지된 정보를 네트워크와 연동하여 관리, 제어하는 것을 말한다. 이와 같이, USN을 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. 향후 헬스 케어 서비스와 같이 개인의 생명과 직결된 홈서비스가 활성화 될 것이므로 재산뿐만 아니라 생명까지 위험에 처하는 경우가 늘어나게 될 것이다.

센서 네트워크의 보안 요구사항으로는 데이터 기밀성, 데이터 인증, 데이터 무결성 등이 고려되어야 하며, 각 네트워크 환경에 맞는 키 관리 기법, 그룹 기반 키 관리, 대칭키 관리, 보안을 위한 센서 네트워크 구조 등이 함께 연구되어야 할 사항이다. 이중 홈 네트워크 환경에서는 키 관리 기법과 데이터 기밀성 및 인증이 가장 중요한 보안 요소라 할 수 있다.

그러나 유비쿼터스 센서 네트워크에서 사용되는 센서 노드는 일회성, 저전력, 작은 기억공간, 제한된 계산능력 등의 특징을 갖는다. 또한 통신 수단으로는 지그비(Zigbee), 블루투스(Bluetooth) 등의 무선망을 사용하게 된다. 이러한 제약은 센서 네트워크의 보안성을 매우 취약하게 하는 요소이다. 무선망 사용으로 인해 도청, 감청, 패킷 스푸핑(spoofing) 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(data freshness) 등이 고려되어야 하며 환경에 맞는 키관리 기법, 그룹 기반 키관리, Pair-wise 키 관리, 보안을 위한 센서 네트워크 구조 또한 같이 연구되어야 한다.

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

Ⅱ. 유비쿼터스 홈 네트워크 환경의 보안 위협 및 요구사항

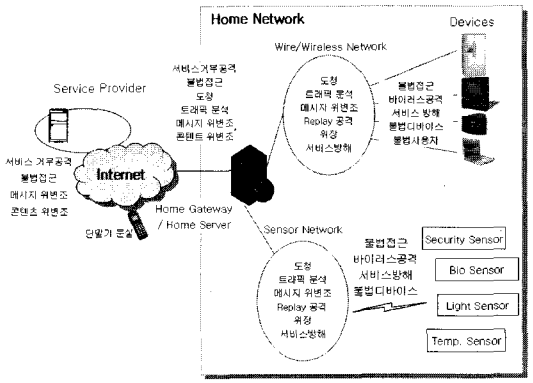

그림 1. 홈 네트워크의 취약성
Fig. 1 Weakness of home networks

그림 1은 홈 네트워크에서 발생될 수 있는 보안 취약성을 정리한 것이다. 인터넷 등에서 발생되던 취약성이 홈 네트워크 내부 망에서도 그대로 발생됨을 알 수 있다. 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. 더욱이 생체정보를 이용한 사용자 확인으로 사용자에게 최적의 자동화된 홈서비스가 제공될 것이므로 주요 생체정보에 대한 노출이나 위변조를 통한 공격으로 인해 개인의 생명까지 위협 받을 수 있게 된다. 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. 무선 센서 네트워크를 위한 키 관리 기법과 암호화 알고리즘

3.1 랜덤 키 사전분배 (RKP : Random Key Pre-distribution)

Eschenauer와 Gligor는 각각의 센서 노드가 큰 키 풀로부터 랜덤하게 m개의 키를 선택하는 랜덤 키 사전-분배 방식을 제안하였다. 두 이웃 노드가 적어도 하나의 공동키를 공유하고 있을 경우에만 안전한 통신 확립이 가능하다[2]. Chan 등은 Eschenauer와 Gligor의 기본 스킴을 안전한 연결 확립을 위해선 적어도 q(q>1)개의 키를 공유 해야만 하는 q-합성수 스킴으로 확장하였다. 이 스킴을 공격하기 위해 공격자는 더 많은 링크를 손상시켜야 한다. 하지만, 희망하는 연결성을 얻기 위해서 더 많은 수의 키를 저장할 필요가 있다는 단점이 있다[3]. Du 등은 기본 스킴과 Blom의 키 관리 스킴을 조합하여 pairwise 키 스킴을 제안했다. Du의 pairwise 키 스킴에서 각각의 센서 노드들은 ω개의 비밀 행렬로부터 랜덤하게 τ열을 선택한다. 같은 비밀 행렬로부터 열을 선택했을 경우, 두 이웃 노드는 서로 안전하게 통신할 수 있다[4].

3.2 LEAP : 로컬 암호화와 인증 프로토콜

S.Zhu, S.Setia와 S.Jajodia는 네트워크 프로세싱을 제공하는 센서 네트워크를 위환 키관리 프로토콜 LEAP (Localized Encryption and Authentication Protocol)을 제안했다[5]. LEAP은 다른 안전성 요구사항을 만족시키기 위해 4가지 형태의 키를 사용하고, 센서 네트워크의 실질적인 면을 고려했다는 점에서 의미가 있다. 네 가지 키는 개인 키, Pair-wise 키, 클러스터 키, 그룹 키이다.

3.3 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 다음 보안요소를 제공한다.[6]

3.3.1 데이터 기밀성

의도된 수신자만이 데이터를 소유할 수 있도록 데이터를 비밀키로 암호화하여 제3자가 암호 메시지로부터 원래 메시지를 추론할 수 없는 보안기능을 말한다. SNEP에서는 CBC(Cipher block chain) 방식을 사용하여 데이터를 암호화하는데 이 방식의 암호화 기법은 공격자에 의해 암호화키를 도청당할 경우, 모든 메시지를 바로 복호화 할 수 있게 된다. 그래서 SNEP은 카운터 모드(CTR)를 적용하여 데이터의 기밀성을 보장한다.

3.3.2 데이터 인증

센서 네트워크에서 매우 중요한 요소이다. 공격자의 공격 유형 중 위장(masquerade), 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(Message Authentication Code)를 사용한다[7].

3.3.3 데이터 무결성

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

3.4 RC5 알고리즘

RC5(Ron's Code 5) 암호화 알고리즘은 SPINS에서 암호화, 키 생성, MAC 생성 등에 사용되는 주요 알고리즘으로 입출력 크기, 키 크기, 라운드 수가 가변인 블록 알고리즘이다[8]. RC5의 암호화와 복호화 과정은 각각 그림 2와 3과 같다.

```
A = A + S[0]
B = B + S[1]
for i=1 to r do
    A = ((A ⊕ B) << B) + S[2 * i]
    B = ((B ⊕ A) << A) + S[2 * i + 1]
```

그림 2. RC5의 암호화 과정
Fig. 2 RC5's encryption

```
for i=r down to 1 do
    B = ((B - S[2 * i + 1]) >> A) ⊕ A
    A = ((A - S[2 * i]) >> B) ⊕ B
B = B - S[1]
A = A + S[0]
```

그림 3. RC5의 복호화 과정
Fig.3 RC5's decryption

여기서,A와 B는 w-비트 word로 구성된 입출력문 이고, r은 라운드 수 ($0 \le r \le 255$), 그리고 S는 비밀 키 K로부터 결정되는 (2r+2)개 word의 랜덤한 배열로 정의된다.

Ⅳ. 암호화 알고리즘을 적용한 홈 네트워크 인증 시스템 구현

4.1 Jini

Jini는 크게 서비스 제공자와 이 서비스를 이용하는 클라이언트, 그리고 서비스 제공자와 클라이언트를 연결해주는 역할을 하는 Lookup 서버 세부분으로 구성된다. 그림 4와 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 4는 Jini의 기본 구조를 나타낸다.[9]

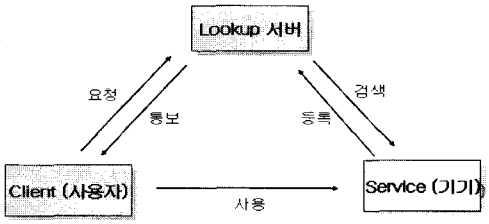

그림 4. Jini의 기본 구조
Fig.4 Jini's fundamental form

4.2 암호화 알고리즘을 적용한 시스템 구조

베이스 스테이션(BS)은 각 센서노드와 Zigbee를 이용하여 메시지를 주고받는다. 센서 노드는 측정된 데이터를 인증키와 함께 베이스 스테이션으로 보냄으로써 사용자 식별이 가능하게 된다. 또한 데이터를 암호화함으로써 기밀성을 보장한다. 그림 5는 암호화 알고리즘을 적용한 보안 시스템의 구조를 보여준다.

4.3 실험 환경 및 실험 방법

TinyOS에서 센서 노드와 BS 사이의 통신에서 사용되는 TOS_Msg 구조를 변형하였다.

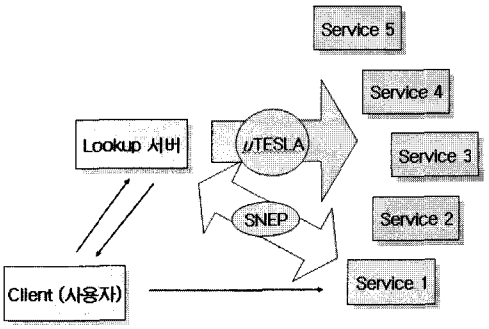

그림 5.SPINS가 적용된 Jini 구조
Fig.5 Jini applied by SPINS

TOS_Msg는 사용자에 의해 변경이 가능한 29bytes의 데이터 공간을 제공한다. 이를 수정하여 비밀 키를 할당하였다. 또한 RC5 알고리즘을 적용, 공유키를 이용하여 BS과 각 센서노드가 공유하는 비밀 키를 암호화하고, 안전한 통신을 위하여 전송되는 데이터를 암호화 하였다.

4.4 제안하는 TOS_Msg 구조

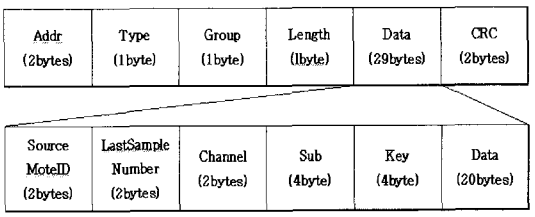

그림 6. 수정된 TOS-Msg 구조
Fig. 6 Modified TOS_Msg structure

그림 6은 제안하는 TOS_Msg 구조를 보여준다. 안전한 통신을 위해서 BS과 각 센서 노드는 생성된 공유키와 비밀 키를 사전분배 방식을 통해 저장하게 된다. 그리고 각 센서 노드는 공유키를 이용하여 비밀 키를 암호화 하게 되고 암호화 된 비밀 키를 Sub(4bytes), Key(4bytes)로 나누어서 수집된 데이터와 함께 BS으로 전송하게 된다. 따라서 암호화된 비밀 키가 노출이 되더라도 암호화에 사용된 공유키는 노출되지 않기 때문에 기밀성을 유지할 수 있다.

V. 구현 결과 및 분석

5.1 다른 그룹에 속한 노드와 BS 사이의 통신

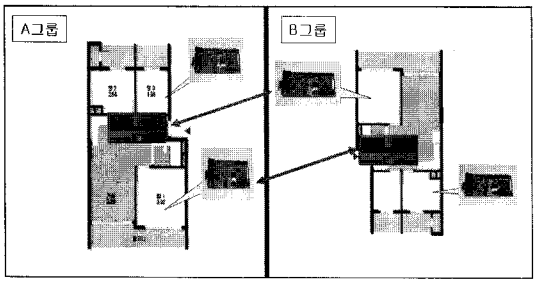

그림 7 A와 B 그룹 사이의 통신.
Fig. 7 Communication between A and B group

그림 7은 A그룹과 B그룹 사이의 통신으로 인한 보안 위협사항을 보여준다. A그룹의 BS은 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 인증하게 함으로써 무결성과 기밀성을 유지할 수 있다.

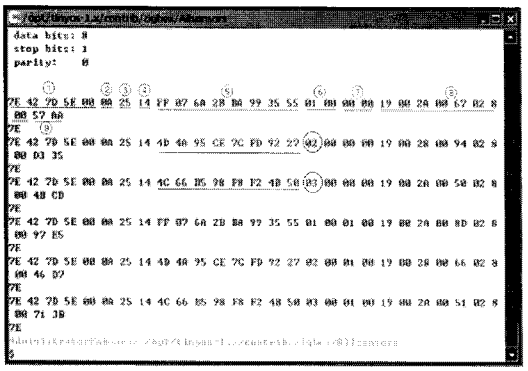

그림 8. 암호화된 비밀키의 전송
Fig. 8 Transmission with encrypted key

그림 8은 센서 노드가 암호화된 비밀 키를 수신된 데이터와 함께 보내는 것을 보여준다. 그림 9는 BS이 암호화된 비밀 키를 복호화해서 인증된 노드 여부를 확인하는 것을 보여준다.

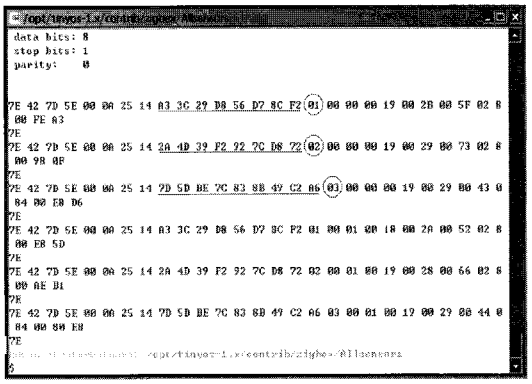

그림 9. 인증된 노드의 확인
Fig.9 Certification of authorized nodes

그림 8과 9는 Java 응용 프로그램을 통해 베이스 스테이션에 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. (그림 9에서는 탈출문자가 포함되어 9byte가 됨) ⑥은 노드 넘버, ⑦은 수신된 데이터의 샘플링 넘버를 의미한다. ⑧은 센서 노드의 센싱 데이터 값으로 실험에서는 온도, 조도, 습도 값을 나타내지만 암호화된 중요 생체정보의 전송에 응용이 가능하다. ⑨는 CRC, 마지막 7E는 데이터의 끝을 나타내는 값이다.

같은 그룹에 속한 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 10은 악의적인 목적을 가지고 공격자에 의해 추가된 센서 노드가 BS에게 공격자에 의해 만들어진 데이터를 전송함으로써 장비의 오작동을 유발시키는 위협이 발생할 수 있음을 보여준다.

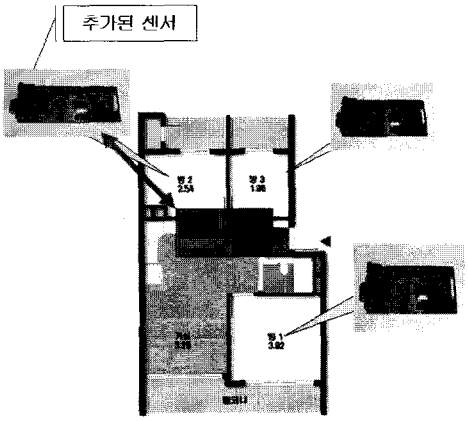

그림 10. BS와 공격노드 사이의 통신
Fig.10 Communication between BS and malicious node

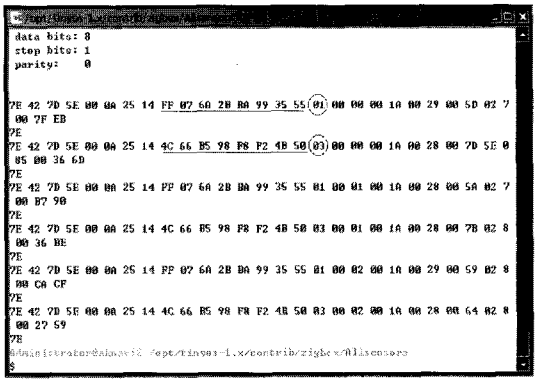

그림 11. 비인가 노드의 데이터 폐기
Fig. 11 Discarded data of unauthorized nodes

그림 11은 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. 2번 노드가 공격자에 의해 추가된 노드이기 때문에 비밀 키를 이용한 인증을 통해 2번 노드의 데이터가 수신되지 않는 것을 확인할 수 있다.

5.3 중요한 정보에 대한 위협

홈 헬스-캐어 같이 인체 정보를 전송하는 서비스의 경우 수집된 데이터는 인간의 생명에 직접적인 영향을 줄 수 있는 중요한 정보가 된다. 이러한 데이터가 무선 네트워크상에 노출될 경우 큰 위험을 초래할 수 있다. 따라서 이러한 정보들을 암호화하여 전송함으로써 안전한 통신이 가능함을 확인할 수 있다.

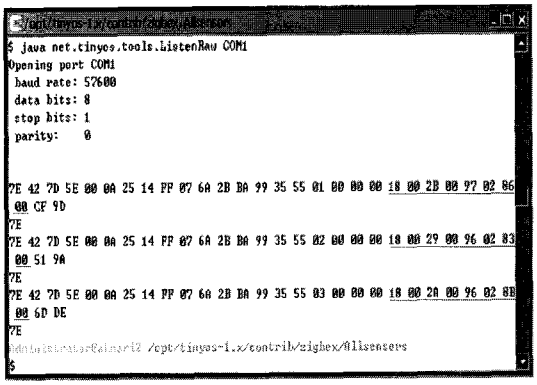

그림 12. 평문의 전송
Fig. 12 Transmission of plaintext

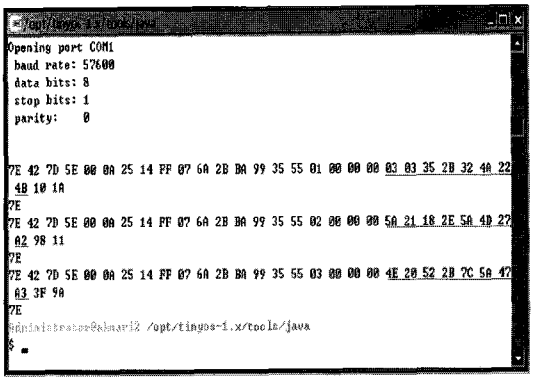

그림 13. 암호화된 데이터의 전송
Fig. 13 Transmission of encrypted data

그림 12는 암호화되지 않은 데이터가 전송됨을 보여준다. 수신된 데이터는 암호화 되지 않은 평문으로 전송되기 때문에 공격자에 의한 도청의 위험이 발생할 수 있다. 그림 13은 생체 신호와 같은 보안이 요구되는 중요한 데이터의 경우, 암호화하여 전송함으로써 데이터의 노출을 막을 수 있음을 보여준다.

5.4 공격자가 임의의 메시지를 가로채 재사용 하는 경우

메시지 재생 공격의 경우, 위의 여러 시나리오와는 다르게 동일한 데이터를 계속해서 보냄으로써 예기치 않은 결과를 초래할 수 있다. 이러한 메시지 재생 공격에 대한 피해를 막기 위해서 RC5 알고리즘에 카운터 모드를 적용하여 암호화하게 된다. 결국 BS은 이전에 수신된 센서 노드의 비밀 키가 다시 사용되더라도 그 값은 현재의 값과 다르기 때문에 공격자에 의한 데이터 여부를 결정할 수 있게 된다.

그림 14는 암호화에 카운터 모드가 적용되었음을 보여준다. 카운터 모드가 적용된 암호화의 경우 동일한 데이터인 경우에도 암호화가 수행된 후에 전혀 다른 데이터가 전송된다.

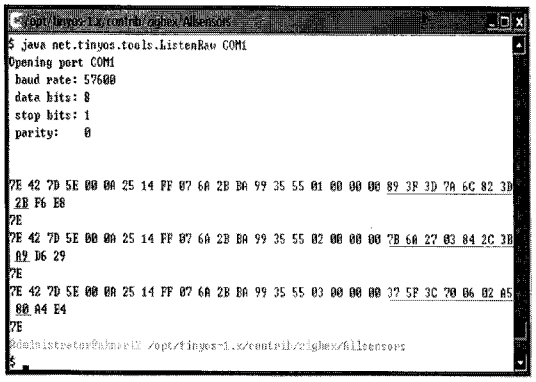

그림 14 CRT 모드가 적용된 암호화
Fig. 14 Encryption applied by counter mode

VI. 결론 및 향후 연구과제

본 논문은 기존의 홈 네트워크 미들웨어의 구조를 바탕으로 불법적인 접근을 통한 주요한 자원에 대한 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. 이러한 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 연산량을 통해 안전한 통신이 가능하도록 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 29바이트의 데이터 배열에 8바이트의 비밀 키를 저장함으로써 인증에 필요한 공유키와 비밀 키를 센서 노드에서 사용 가능하게 된다. 공유키는 각 센서 노드와 베이스 스테이션 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 베이스 스테이션간의 인증 과정을 수행하였다. 이때 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.

인증 과정을 통하여 안전성이 확보됨으로서 홈서비스에 따라 개인의 경제 손실 뿐 아니라 개인정보의 도용으로 인해 생명까지도 위협받을 수 있는 상황을 방지 할 수 있을 것으로 기대되어 홈서비스 활성화에 도움이 될 것으로 예상된다.

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.

참고문헌

[1] 한종욱 외 2인, "홈네트워크 보안 기술 동향", 한국통신학회지 제23권 9호, pp.113-124, 2006년.

[2] L. Eschenauser and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks", Proc. 9th ACM Conf. on Computer and Communication Security, pp.41~47, Nov. 2002.

[3] H. Chan, A. Perring and D. Song, "Random Key Distribution Schemes for Sensor Networks', Proc. IEEE Symposium on Security and Privacy, pp.197~213, May 2003.

[4] W.Du, et al, "A Pairwise Key Predistribution scheme for Wireless Sensor Network", Proc. 10th ACM Conf. on Computer and Communication Security, pp.42~51, Aug. 2003.

[5] S. Zhu et al, "LEAP: Efficient Security Mechanism for Large-Scale Distributed Sensor Networks", 10th ACM Conference on Com. & Comm. Security, pp. 62~72, 2003.

[6] Adrian Perrig et al, "SPINS : Security Protocols for Sensor Networks", Wireless Networks Journal, 8:521-534, 2002.

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

[8] R.L. Rivest, The RC5 encryption algorithm, in : Workshop on Fast Software Encryption. pp.86-96, 1995.

[9] 백선욱, "Jini 규격에 기반한 댁내 네트워크 시스템의 설계 및 구현", 산업과학연구 제10호, 2000년.

저자소개

이 기 영 (Ki Young Lee)

1982년 연세대학교 전기공학과
1984년 연세대학교 대학원
전기공학과 공학석사
1987년 Univ. of Colorado, ECE, M.S.
1993년 Univ. of Alabama, ECE, Ph.D.
1994년~현재: 인천대학교 정보통신공학과 교수
※관심분야: 인터넷 트래픽 제어 및 프로토콜, USN, 네트워크 보안시스템