홈 네트워크 서비스를 위한 인증 시스템 설계 및 구현

설정환* · 이기영**

인천대학교

Design & Implementation of Authentication System for Home Network Service

Jeong-hwan Seol* · Ki-young Lee**

University of Incheon

E-mail : aknari@naver.com, kylee@incheon.ac.kr

요 약

본 논문에서는 홈 네트워크 서비스를 위한 인증 시스템을 설계하여 실제 센서 노드에 구현하였다. SPINS의 SNEP 프로토콜은 데이터 기밀성과 인증을 제공한다. SNEP을 기반으로 RC5 암호화 알고리즘을 적용하여 인증키 및 데이터의 암·복호화를 수행하였다. 또한 무선 센서 네트워크에서의 키 관리 기법인 대칭키 사전 분배 방식을 적용하여 인증키의 노출을 방지하였다. 데이터 수신을 담당하는 베이스 스테이션과 데이터 전송을 담당하는 센서 노드들로 실험 환경을 구성하였으며, 각 센서 노드는 수신된 데이터를 암호화된 인증키와 함께 베이스 스테이션으로 전송하게 된다. 실험을 통해 다른 그룹의 센서 노드와 베이스 스테이션 사이의 통신 및 악의적인 목적을 가지고 추가된 센서 노드와의 통신으로 인한 오작동을 막을 수 있음을 확인할 수 있었다.

ABSTRACT

In this paper, we designed the authentication system for home network service and applied it to actual sensor nodes. SNEP protocol of SPINS provides confidentiality of data and authentication. 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. 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

USN(Ubiquitous Sensor Network), SNEP, 키 관리, 인증

Ⅰ. 서 론

1990년대 중반 인터넷의 보급은 인간의 생활을 비약적으로 바꾸어놓는데 큰 역할을 하며 유비쿼터스 환경으로의 변화를 가속시켰다. 이러한 유비쿼터스 사회 시스템은 사회, 경제, 교육, 복지 및 인간의 일상생활에 이르기까지 다양한 서비스를 제공하게 될 것이다. 그 중 디지털 홈과 지능형 빌딩 서비스가 정점에 있게 될 것이다.

이처럼 인터넷의 발달로 다양한 IT 서비스가 새롭게 만들어지고 있고 그 중 우리의 실생활과 가장 가까운 서비스 중 하나가 홈 네트워크 서비스이다. 무선 네트워크는 홈 네트워크 장비 및 가전을 쉽게 연동할 수 있기 때문에 가장 중추적인 역할을 수행할 것이다. 그중에서도 센서 노드를 이용한 USN(Ubiquitous Sensor Network) 서비스는 홈 네트워크 서비스뿐만 아니라 홈 헬스-캐어(Home Health-Care) 서비스 및 홈 타운(Home

Town) 서비스에 이르기까지 가장 핵심적인 기술이 될 것이다. 그러나 유비쿼터스 센서 네트워크에서 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 사용으로 인해 도청, 감청, 패킷 스푸핑(packet 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 키 관리 기법, 그룹 기반 키관리, pairwise key 관리, 보안을 위한 센서 네트워크 구조 또한 같이 연구되어야 한다[1]. 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. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 유비쿼터스 홈 네트워크 환경의 보안 위협 및 요구사항에 대해 알아보고 Ⅲ장에서는 키 관리 기법, Ⅳ장에서는 SNEP 프로토콜에 대해 알아본다. Ⅴ장에서는 홈 네트워크 보안 시스템 설계와 구현 결과 및 성능 평가를, Ⅵ장에서는 논문에 대한 결론을 맺는다.

Ⅱ. 본 론

1. 홈 네트워크 환경에서의 보안 위협사항 및 요구사항

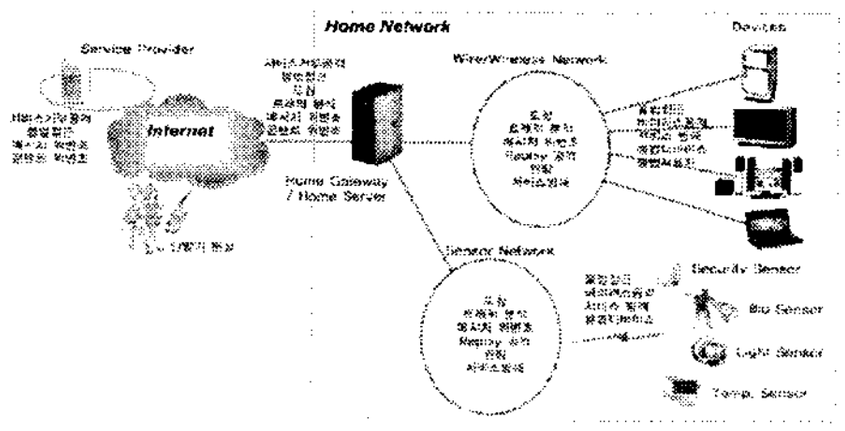


그림 1 . 홈 네트워크의 보안 취약점

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-캐어 서비스, 실버타운과 같이 생명과 직결된 바이탈 신호들과 홈-타운 전체의 안전에 영향을 주는 신호들의 사용이 증가할 것으로 예상된다. 더욱이 생체정보를 이용한 사용자 확인으로 사용자에게 최적의 자동화된 홈 서비스가 제공될 것이므로 주요 생체정보에 대한 노출이나 위변조를 통한 공격으로 인해 개인의 생명까지 위협 받을 수 있게 된다. 따라서 안전한 홈 네트워크 서비스를 위해서는 다음과 같은 보안 요소가 고려되어야 한다.

1) 데이터 기원 인증 : 메시지를 인증하기 위하여 특정한 소스로부터 왔다는 것을 확립하여야 한다. 관용 암호화와 디지털 서명 등을 이용한 공개키 방법이 적용될 수 있다.

2) 명령권한 인증 : 어떤 사용자가 어떤 일을 수행하기 위한 명령에 대해 정당한 권한이 있는지 검증하여야 한다.

3) 메시지 무결성 보호 : 입력 메시지에 대해 정당하지 않은 데이터 변경이 없음을 보증하는 기능이 필요하다.

4) 메시지 재생 방지 : 임의의 메시지를 공격자가 중간에서 가로채 나중에 재사용되는 것을 방지하여야 한다.

5) 키 분배 : 완전한 보안혜택을 위한 안전한 키 분배가 이루어져야 한다.

2. 랜덤 키 사전분배 (RKP : Random Key Pri-distribution)

Eschenauer와 Gligor는 각각의 센서 노드가 큰 키 풀로부터 랜덤하게 m개의 키를 선택하는 랜덤 키 사전-분배 스킴을 제안하였다. 두 이웃 노드가 적어도 하나의 공동 키를 공유하고 있을 경우에만 안전한 통신 확립이 가능하다. Chan et al는 Eschenauer과 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. Du et al은 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 통신 할 수 있다.[2]

3. LEAP : 로컬 암호화와 인증 프로토콜

S. Zhu, S. Setia와 S. Jajodia 는 in-network 프로세싱을 제공하는 센서 네트워크를 위환 키 관

리 프로토콜 LEAP (Localized Encryption and Authentication Protocol)을 제안했다. LEAP은 다른 안전성 요구사항을 만족시키기 위해 개인키, Pairwise 키, 클러스터 키, 그룹 키를 사용한다.[3]

4. 암호화 알고리즘

4.1 SNEP (Secure Network Encryption Protocol)

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.[4]

4.1.1 데이터 기밀성

의도된 수신자만이 데이터를 소유할 수 있도록 데이터를 비밀키로 암호화하여 제 3자가 암호 메시지에 원래 메시지를 추론할 수 없는 보안기능을 말한다. SNEP에서 암호화 방식은 CBC(Cipher block chain) 방식을 사용하여 데이터를 암호화한다. CBC 방식의 암호화 기법은 공격자에 의해 암호화키를 스푸핑(spoofing)당할 경우, 모든 메시지를 바로 복호화 할 수 있게 된다. 그래서 SNEP는 카운터 모드(CTR)를 적용하여 데이터의 기밀성을 보장한다.

4.1.2 데이터 인증

메시지 인증은 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. SNEP는 올바른 송신자가 데이터를 전송하였는지 검증하기 위해서 메시지 인증 코드MAC(Message Authentication Code)를 사용한다.

4.1.3 데이터 무결성

데이터 및 네트워크 보안에 있어서 정보가 인가된 사람에 의해서 만이 접근 또는 변경 가능하다는 확실성으로서, 2.1.2절의 데이터 인증을 통해 보장된다.

III. 암호화 알고리즘을 적용한 홈 네트워크 보안 시스템 구현

1. Jini의 기본 구조

Jini는 크게 서비스 제공자와 이 서비스를 이용하는 클라이언트, 그리고 서비스 제공자와 클라이언트를 연결해주는 역할을 하는 lookup 서버 세 부분으로 구성된다. 그림 2와 같이 각 기기는 Lookup 서버에 자신을 등록하고 Client는 Lookup 서버에 사용하고자 하는 기기를 요청한다. Lookup 서버는 요청받은 기기를 검색하여 Client에 통보해주면 Client는 요청한 기기를 사용하게 된다.

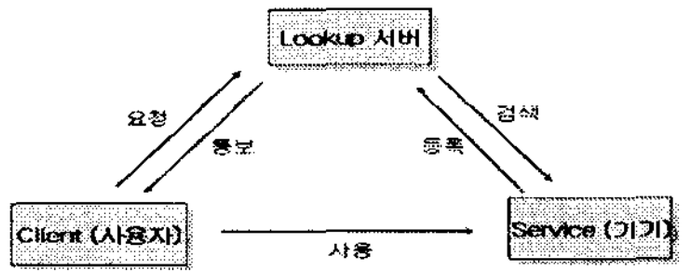


그림 3. Jini의 기본 구조

2. 암호화 알고리즘을 적용한 시스템 구조

베이스 스테이션은 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 3은 암호화 알고리즘을 적용한 보안 시스템의 구조를 보여준다.

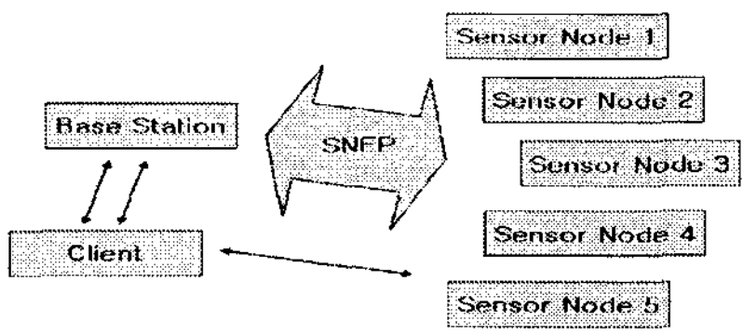
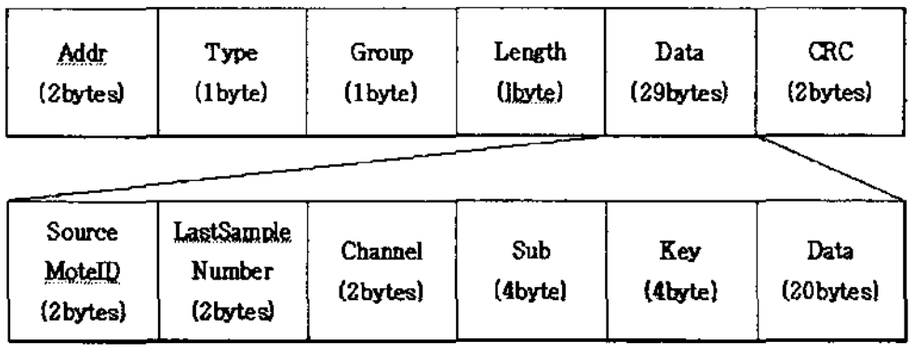


그림 4. 암호화 알고리즘을 적용한 시스템 구조

IV. 구현 결과 및 분석

센서 노드와 베이스 스테이션사이의 통신에서 사용되는 TOS_Msg 구조를 변형하였다. RC5 알고리즘을 이용하여 베이스 스테이션과 각 센서노드가 공유하는 비밀키를 암호화하고, 전송되는 데이터를 암호화함으로써 안전한 통신이 가능하도록 한다.

1. 변형된 TOS_Msg 구조



2. 실험 환경

서로 다른 그룹에 속하는 서버와 센서노드의 통신에서의 오작동과 악의적인 목적을 가지고 추가된 센서 노드와 서버사이의 오작동이 홈 네트

워크에서는 큰 위협이 될 수 있다. 이에 다음과 같은 시나리오를 구성하여 실험을 하였다.

시나리오 1. 서로 다른 그룹에 속하는 서버와 센서간의 통신

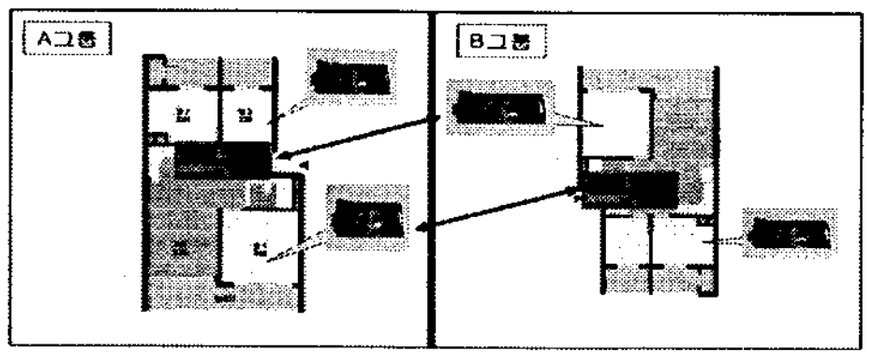


그림 5. 서로 다른 그룹간의 통신

시나리오 2. 악의적인 목적을 가지고 추가된 센서와 서버간의 통신

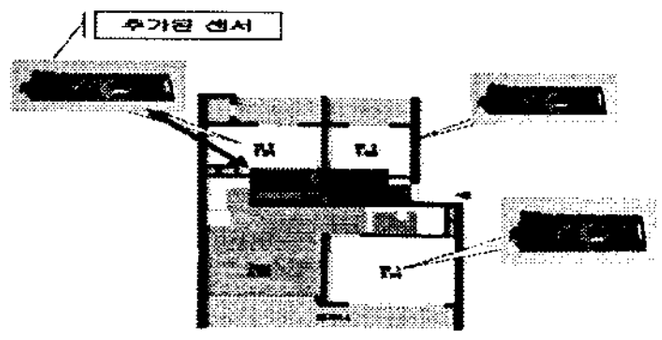


그림 6. 악의적으로 추가된 센서와 서버간의 통신

3. 실험 결과

3.1 인증 과정이 성공적으로 수행

시나리오 1, 2에서 다른 그룹간의 통신과 악의적인 목적으로 추가된 센서는 디바이스 인증 과정을 통하여 메시지가 폐기되어 Oscilloscope에는 2개 데이터가 그래프로 표현된다.

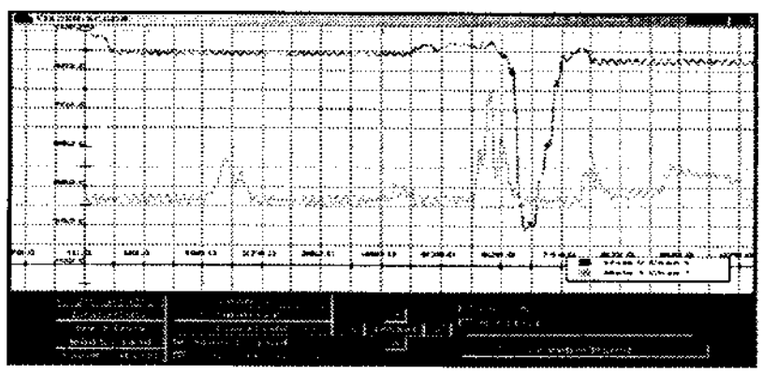


그림 7. 성공적인 인증과정 결과

3.2 인증과정을 거친 데이터 수신 모습

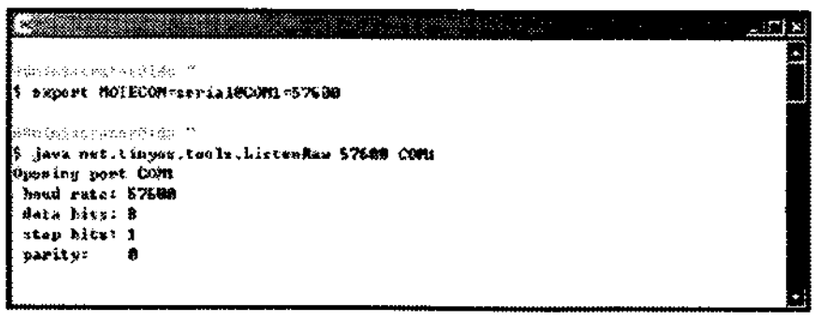


그림 8. 인증 실패 시 폐기된 데이터

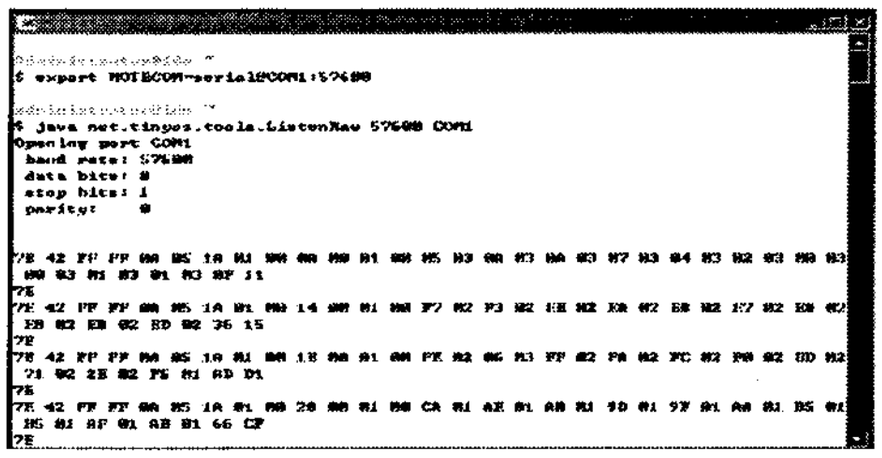


그림 9. 인증 성공 시 전송되는 데이터

인증에 실패 하여 폐기된 경우는 그림8 과 같이 수신되는 데이터가 없으며, 디바이스 인증 절차가 성공한 경우 수신되는 데이터는 그림9 와 같다.

V. 결 론

유비쿼터스 컴퓨팅 환경에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 개인생활의 위협도 증가한다. 따라서 인증, 기밀성, 무결성 등이 제공되어야 한다. 본 논문에서는 불법적인 디바이스 접속을 통해 주요한 자원에 대한 공격이나 데이터의 유출 가능성 및 디바이스의 오작동에 대한 대책으로 인증 시스템을 구현해 보았다. 인증 구현 방법으로 TOS_Msg를 변경하고 RC5 알고리즘을 이용, 비밀키를 암호화하여 센서노드와 베이스스테이션간의 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. 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 예상 된다.

참고문헌

[1] 권태경 외3명, "무선 센서 네트워크 보안", 한국통신학회지, 제23권 제9호 pp. 88~102, 9.2006

[2] W.Du 외3명, "A Pairwise Key Predistribution scheme for Wireless Sensor Network", ACM CCS, 3.2003

[3] S. Zhu 외2명, "LEAP:Efficient Security Mechanism for Large-Scale Distributed Sensor Networks", 10th ACM Conference on Com. & Comm. Security, pp. 62~72, 2003.

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