情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

무선 센서 네트워크를 이용한 무인 경비 시스템에서의 정보보호 기술

이 성 재*, 김 대 경*, 이 재 근*, 염 흥 열*

요 약

USN은 모든 사물에 컴퓨팅과 통신기능 및 센싱 기능을 부여하여 언제, 어디서나, 통신이 가능한 환경을 구축하는 네트워크로서, 향후에는 다양한 센싱 기능이 추가되어 이들 간의 네트워크가 구축되는 형태로 발전할 것이다. 따라서 본 논문에서는 무선 센서 네트워크를 무인 경비 시스템에 적용할 경우 나타날 수 있는 정보 보안상의 취약점을 도출하고 현재 발표되어있는 정보보호 프로토콜 중에서 적합한 기법을 제안하고자 한다.

Ⅰ. 서 론

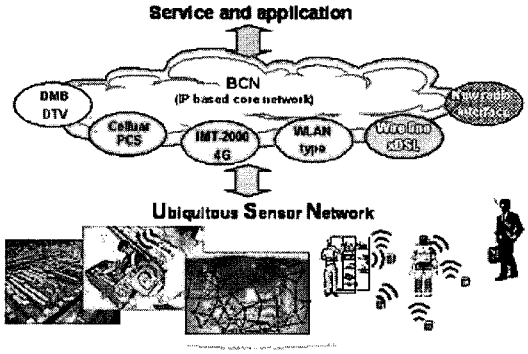
유비쿼터스 컴퓨팅 (Ubiquitous Computing)은 새로운 개념의 IT 패러다임으로, 1988년 미국 제록스 팰로앨토 연구소의 마크 와이저(Mark Weiser)[1]에 의하여 제안된 개념이다. 이는 일상생활과 컴퓨팅을 접목하여 지능화된 환경을 통해 접속되고, 이를 통하여 다양한 IT 서비스를 제공함을 목표로 하고 있다. USN(Ubiquitous Sensor Network)이란 "필요한 모든 사물에 전자식별 태그를 부착하고 이를 통하여 사물의 인식 정보를 기본으로 주변의 환경정보(온도, 습도, 압력, 오염, 균열 등)까지를 탐지하여 이를 실시간으로 네트워크에 연결하고, 관련 정보를 관리하는 것"을 말하는 것으로, 궁극적으로 모든 사물에 컴퓨팅 및 통신 기능을 부여하여 언제 어디서나 무엇과도 (Anytime, Anywhere, Anything) 통신이 가능한 환경을 구현하기 위한 것이다. USN은 전자태그에 센싱 기능과 통신 기능이 추가된 센서노드를 구성하고, 이들 노드 간에 네트워크를 통하여 연결되는 형태로 발전할 것으로 예측되고 있다.[2] 센서 네트워크의 활용사례는 다음과 같으며, 적용 범위는 점차적으로 확대될 것으로 예측된다.[3-5,8]

- ○ 텔레메틱 분야 : 타이어의 공기압, 교통 상황의 실시간 수집 등을 통해 최적화된 실시간 교통 통제를 할 수 있게 한다.
- ○ 홈네트워크 분야 : 가정에서 가전제품에 대한 원격 관리를 통해 생활의 편리성을 제고 시킬 수 있다.
- ○ 의료 모니터링 분야 : 사람의 신체 상태(혈압, 맥박, 체온 등)를 센서 네트워크를 통해 원격으로 모니터링을 할 수 있어서, 의료 응급 서비스 체계를 구축할 수 있다.
- ○ 군수 물류, 재고 관리 분야 : 물류에 대한 신속하고 정확한 정보를 파악하여, 생산품과 재고품과의 관계 등을 예측할 수 있다.
- ○ 비상대응 정보 분야 : 센서 네트워크는 건물에 대한 침입상태와 사람 및 차량에 대한 경로 정보 등을 수집하여, 신속히 비상대응 체계를 구축할 수 있게 해준다.

본고에서는 무선 센서 네트워크를 이용하여 무인 경비 시스템을 구축할 경우의 네트워크 구성방법과 보안 취약성을 도출하고, 현재 까지 발표된 정보보호 프로토콜 중에서 적합한 기법을 제안하고자 한다.

먼저 2장에서는 무선 센서를 이용한 무인 경비 시스템 구성방안을 기술하고, 3장에서는 무선 센서 네트워크 환경에서의 보안 취약성을 도출하며, 4장에서는 센서 네트워크에서 실현 가능한 보안 프로토콜을 기술하고, 끝으로 5장에서는 결론과 향후 연구과제 순으로 기술하겠다.

* 순천향대학교 정보보호학과 (auditor@ktlinkus.com, morlake@hanmail.net, jglee@nca.or.kr, hyyoum@sch.ac.kr)



〔그림 1〕 USN 개요

II. 무선 센서를 이용한 무인경비시스템

기존의 무인 경비 시스템은 보안이 취약한 지역에 여러 개의 센서를 설치하고, 센서에서 수집된 경보 정보를 사용자단말기에서 취합한 후, 전기적 신호로 변환한 뒤, 원격지에 떨어져 있는 관제실로 전달하고, 관제실에서는 경비요원에게 출동 지시하여 침입자를 검거 또는 퇴치하는 형식이다.

그러나 센서와 사용자 단말기간은 유선을 이용하기 때문에 케이블 포설이 어렵고 미관상도 좋지 않아 이를 무선센서 네트워크로 대체 할 수 있으며, 그 배치도는 각각 그림 2, 3과 같다.

따라서 무인 경비 서비스를 위한 통신망은 사용자 측의 단말 장치, 무선 센서 네트워크, 전송로(IP기반망, 이동통신망, 유선통신망, 전용회선 등) 및 서비스 제공자의 각종 응용서비스 시스템으로 구성되는데, 본 논문에서는 무선 센서 네트워크에 한해서 기술하기로 한다.

분산된 센서 네트워크는 대개 계산 능력이 강력한 기지국(Base Station)과, 센서라고 불리 우는 많은 수의 낮은 용량의 노드(Node)들로 구성 된다.

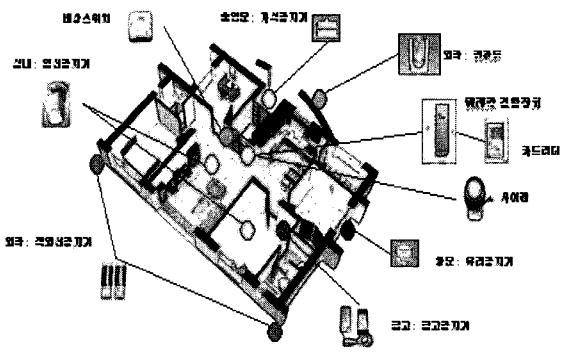
분산된 센서 네트워크에 있는 노드들은 제한된 대역폭의 무선방식을 이용하여 통신을 한다. 센서 노드에서 기지국으로 감지 내용을 전송하는 경우에는 송수신자가 비교적 명확하기 때문에 유니캐스트(Unicast) 통신 방식을 이용할 수 있으나, 센서 네트워크가 향후 USN으로 발전될 경우에는 멀티캐스트(Multicast) 통신 방식을 사용할 수도 있다.

전쟁터, 반테러 환경 등 적대적인 환경에서는 기지국으로부터 수신된 방송 메시지가 정당한 송신자로부터 수신되었는지, 또 그 메시지가 전송 중에 변경되지 않았는지를 확인하는 인증, 무결성 그리고 기밀성 등의 보안서비스를 제공할 수 있는 능력이 센서노드에 있어야 하나, 센서 노드는 소형이기 때문에 배터리의 사용기간이 매우 짧고, 또 계산 능력도 부득이 제한될 수밖에 없는 상황이다. 따라서 극심하게 자원이 제한되어 있는 무선 센서 노드를 이용하여 무인 경비 서비스를 제공하는 것이 본 논문의 주된 목표가 된다.

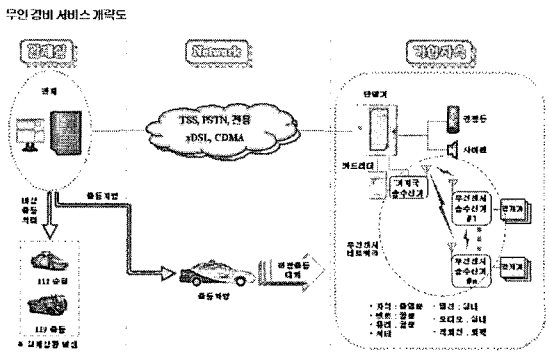
2.1 센서 네트워크 전제조건

본 논문에서 고려하는 무인 경비 서비스를 위한 센서 네트워크의 센서 노드 장치로는 미국 버클리 대학교에서 수행한 Smart Dust 프로그램에서 사용된 8비트, 4Mhz의 CPU와 저장 공간으로 8Kbytes 플래시메모리 및 512 bytes의 RAM, 그리고 OS로는 4,500 바이트의 코드 공간을 갖는 Tiny OS와 10Kbps의 무선통신 대역폭을 갖는 센서 노드 장치로 가정했다.[6-8]

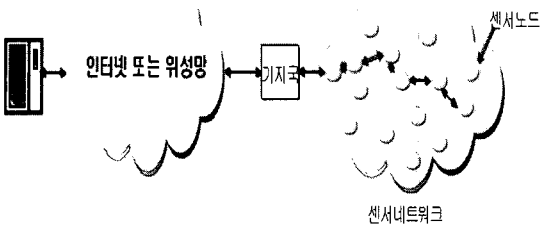
센서 네트워크의 통신 구간은 기지국 → 노드, 노드 → 기지국, 노드 → 노드구간 등 세부분으로 구분할



〔그림 2〕 센서노드 및 기지국 배치도



〔그림 3〕 무인 경비 서비스 개략도



〔그림 4〕 센서 네트워크 정보 전달 구조

수 있는데, 본 논문에서는 편의상 기지국 → 노드간의 인증과 암호화 과정에 대해 논의하고 나중에 노드 → 기지국, 노드→노드 구간에 대해서도 간단히 언급하기로 한다.

Ⅲ. 무선센서 네트워크에서의 보안 취약성

무인 경비 시스템에서의 무선 센서 네트워크는 그림 4와 같이 여러 개의 센서노드들로 구성되며, 통신 인프라와 연결하기 위한 하나의 기지국(Base Station)이 존재한다. 통신과 센싱 기능을 갖는 센서를 이용하므로, 기본적으로 전파식별에서 발생하는 모든 위협에 더하여 다음과 같은 위협들이 추가로 발생하게 된다.

- ○ 센서 노드 장치의 도난 및 분실 : 공격자가 장치를 탈취 당하게 되면, 장치에 저장되어있는 다양한 암호학적 정보가 누설될 가능성이 커서, 해당 노드를 통과하는 모든 정보를 공격자가 알 수 있게 된다.
- ○ 노드간의 통신 정보 노출 : 무선 센서 네트워크 환경에서 노드 간의 통신되는 통신 메시지가 평문 형태로 전달되면, 메시지의 위조와 변조가 가능하게 되어, 경비 대상에 대한 다양한 공격이 가능하게 된다. 특히 도처에 존재하는 센서 노드 장치간의 정보 누출은 노드의 ID 및 위치 정보의 노출을 가능케 하여 또 다른 심각한 문제를 야기 할 수 있다.
- ○ 불법 기지국 설치 : 만약 불법의 기지국이 설치된다면, 이 기지국을 통하여 전송되는 모든 정보가 노출되거나, 위장 침투의 위협이 따를 수 있어, 인증 등이 필요하다.
- ○ 센서노드에 의한 위조 정보 전송 : 무선 통신을 이용하여 센서와 기지국 또는 센서 노드 간에 있는 어떤 노드도 무선 접속이 가능하게 될 가능성이 있다. 따라서 불법 센서 노드가 정보를 위조하여 기지국으로 정보를 송신 한다면, 관제실에서는 가짜 정보를 갖고 출동하거나, 안전한 메시지라고 인정 하고 출동을 하지 않는 경우가 발생할 수 있으므로, 센서가 송신한 위조된 정보를 인증하고 검출 할 수 있는 기법이 강구되어야 한다.
- ○ 서비스 거부 공격(Denial of Service : DoS) : 서비스 거부 공격은 가용성을 침해하는 공격 방법으로, 공격대상은 센서 노드나 기지국이 될 수 있으나, 주로 정보의 집중점이나 제어의 중심점에 대한 공격을 수행하여 센서 네트워크의 정상적인 동작을 방해하는 것이다. 만약 센서 노드중 하나가 서비스 거부 공격을 받게 되면, 그 노드는 정상적인 동작을 할 수 없게 되는 공격이다.
- ○ 배터리 소진 공격 : 센서 노드는 일반적으로 배터리로 동작한다. 따라서 배터리가 소진 하게 되면, 다시 재충전하기 전에는 정상적인 동작이 불가능하다. 이러한 특성을 이용하는 것이 배터리 소진 공격이다. 공격자는 계속적으로 공격 대상 장치에게 데이터 전송요청이나 연결 요청을 보내면, 결국 센서 노드에 있는 배터리가 모두 소진하게 되어 무인 경비 시스템을 무력화 시킬 수 있다.
- ○ IP스푸핑(Spoofing) : IP 스푸핑은 기밀성에 대한 위협이다. 무선 신호는 벽을 통과 할 수 있기 때문에 건물 외부로부터 전달 될 수 도 있고, 적어도 무선 신호가 존재하는 어느 누구나 무선 접속이 가능하기 때문에 전송되는 정보가 암호화되어 있지 않을 경우 공격자가 중요한 정보를 도청할 위험이 항상 존재한다. 특히 아파트와 같은 지역에 무선 센서가 설치된 다면, 옆집으로부터의 센서 정보가 벽을 통해 자기 집으로 올 수도 있고, 또 자기 집 정보가 옆집으로도 전달될 수 있기 때문에 이를 해소하기 위한 대책으로 노드와 기지국간 인증 기능이 필요하다.
- ○ 트로이 목마, 웜 바이러스 등 : 트로이 목마, 웜 바이러스 등은 역시 무선 센서 노드 장치에 위협을 가할 수 있다. 이들은 가용성에 영향을 미칠 수 있고, 기밀성과 무결성에도 침해를 가할 수 있다.
- ○ 신호방해 공격 : 신호 방해 공격은 가용성을 침해한다. 무선 시스템에 대한 고전적인 공격은 통신 채널을 혼선 시키는 것이다. 이러한 통신

채널의 혼선이 존재한다면 무선 센서 네트워크를 이용한 무인 경비 시스템은 정상적인 서비스를 제공 할 수 없을 것이다. 그러나 이와 같은 공격은 주파수 호핑(Hopping) 이나, 스프레드 스펙트럼 방법 등을 사용하면 방지할 수 있으나, 본고에서는 설명을 생략한다.

이러한 위협을 효율적으로 막기 위해 요구되는 보안 서비스는 기밀성, 멀티캐스트 인증을 포함하는 인증 및 무결성, 그리고 신선성(Freshness) 서비스 등이다.

- ○ 데이터 기밀성(Confidentiality) : 센서 네트워크 환경의 많은 응용에서는 민감한 데이터 교류가 노드(Node)간에 빈번하게 이루어진다. 따라서 권한이 있는 노드 이외에 민감한 정보를 볼 수 없도록 해야 하며, 또 비밀키로 데이터를 암호화한 상태에서 데이터 교환이 이루어지도록 하여야 한다.
- ○ 데이터 인증(Authentication) 및 무결성(Integrity) : 메시지 인증은 센서노드에서 메시지가 전송되었다는 것을 입증하는 것이고, 무결성은 전송도중에 메시지가 변경되지 않았다는 것을 입증하는 것이다. 공격자는 쉽게 메시지를 위조하여 삽입할 수 있기 때문에, 수신자는 데이터가 원래 작성자인 노드로부터 송신 된 것인지를 확인해야 한다. 공개 키 방식은 실제적인 컴퓨팅 파워나 자원 소요가 크므로, 지연된 키 노출과 단 방향 함수 키체인(Key Chain)을 이용하는 멀티캐스트 인증방식(μTESLA)이 제안되고 있다.
- ○ 데이터 신선성(Freshness) : 데이터 신선성은 예전에 전송 되었던 데이터가 재전송되는 것을 막기 위한 기술로서, 예전에 보낸 데이터가 아니라 현재의 통신 상대가 보낸 데이터임을 보장하는 보안 서비스이다. 일반적으로 카운터 값을 이용한 약한 신선성과 임의의 난수를 이용하여 도전-응답을 통해 강한 신선성을 제공하는 두 종류가 있다.

Ⅳ. 센서 네트워크 보안프로토콜(SPINS: Security Protocol for Sensor Network)

센서 네트워크의 보안 요구사항을 만족하기 위한 기밀성, 인증 및 무결성과 신선성 등의 보안 서비스를 제공하는 프로토콜로 SPINS가 있다.[8] 이 프로토콜은 대칭형 암호 방식만을 사용하며, 무선 센서 네트워크와 같은 자원이 제한된 환경에서 보안 프로토콜을 제공할 때 자원의 오버헤드를 최소화하는 것을 목표로 한다.

SPINS는 데이터 기밀성, 양단간 데이터 인증, 무결성 그리고 신선성을 제공하는 SNEP(Secure Network Encryption Protocol)와 데이터 멀티캐스트 인증을 제공하는 μTESLA(Micro Timed Efficient Stream Loss-tolerant Authentication)로 구성되어 있다.

4.1 유니캐스트 통신 방식

센서 노드에서 기지국으로의 통신과 같은 유니캐스트 통신에서는 송수신자가 비교적 명확하기 때문에 두 통신 당사자가 서로 비밀을 공유하고, 각 패킷에 공유된 키로 계산한 메시지 인증 코드(Message Authentication Code : MAC)를 덧붙임으로써 비교적 충분한 보안을 제공할 수 있는데, 이와 같은 목적으로 사용되는 프로토콜이 SNEP이다.

4.1.1 SNEP : 데이터 기밀성, 인증, 무결성 및 신선성

SNEP 프로토콜은 다음과 같은 보안 서비스를 제공한다.

- ○ 데이터 기밀성 : 데이터 교환시 암호화를 통하여 데이터 기밀성을 제공한다.
- ○ 확고한 보안성 : 동일한 평문을 여러 개의 암호 방식으로 암호화 한 것을 공격자가 도청을 하더라도, 그 암호문으로부터 평문 정보를 알아내지 못하게 보장하는 확고한 보안성을 제공한다. 공격자가 같은 키로 암호화된 평문-암호문 쌍을 알고 있다 하더라도 암호화된 메시지의 평문을 추출해 낼 수 없도록 한다.
- ○ 양단간 데이터인증과 무결성 : MAC(메시지 인증코드)을 사용하여 양단간 데이터 인증과 무결성을 제공한다.
- ○ 재사용 방지 : MAC에 카운터(Counter) 값을 포함하여 공격자에 의한 재사용 공격을 방지한다.
- ○ 데이터 신선성 : 해당 데이터가 가장 최근의 버전임을 검증하기 위한 기능을 제공한다.
- ○ 낮은 통신 부하 : 통신 쌍방은 카운터를 나누어 갖고, 각 블록이 끝난 후 카운트를 하나씩 증가시키며, 카운터를 메시지에 포함하여 송신하지 않으므로, 낮은 통신 부하 및 기밀성을 제공한다.

4.1.1.1 SNEP의 키 설정, 암호화 및 MAC 생성

SNEP는 일반적인 구현에서 RC5[14] 대칭 키 암호화 알고리즘을 이용하여 그림 5-1과 같이 다양한 목적의 키 값을 유도한다. 마스터키(Master Key)는 기지국과 센서 노드 간 사전에 나누어 갖으며, 마스터키를 기반으로 암호화를 위한 암호화 키, MAC 값 생성을 위한 키값, 랜덤 키값 등을 생성한다.

암호화는 그림 5-2와 같이 전 단계에서 생성한 암호키를 카운터 모드(Counter Mode)로 암호화하여 Chain으로 연결하는 구조이다. E(En_Key, Counter){P} = C를 이용해 암호화 루틴을 반복 수행하여 암호화 및 복호화를 수행한다.

그리고 메시지인증코드(MAC) 생성키를 이용하여 그림 5-3과 같이 CBC 모드로 암호화된 메시지에 대한 메시지인증코드를 생성한다.

4.1.1.2 데이터 인증 및 기밀성

데이터 인증만 보장하는 경우 노드 A에서 기지국 B로 데이터 D와 메시지인증코드인 MAC (K_{MAC}, C)을 송신하며(단, D는 데이터, K_{MAC}키는 마스터키에서 추출), 데이터 인증과 기밀성을 보장하는 경우에는 노드 A에서 기지국 B로 암호화된 데이터 E = {D}(K_{encr}, c)와 이에 대한 메시지인증코드로 MAC (K_{MAC},C|E)을 송신하여 데이터 인증 및 기밀성을 제공한다(단, D는 데이터, K_{encr}는 암호 키, 카운터 C는 초기 백터 값(Initial Vector), K_{encr}키와 K_{MAC} 키는 마스터비밀키 K로부터 추출). 따라서 노드 A가 기지국 B로 보내는 완전한 메시지는 다음과 같다.

$$A \rightarrow B : \{D\}(K_{encr},c), MAC(K_{MAC},C|\{D\}(K_{encr},c))$$

4.1.1.3 Nonce를 사용한 강한 신선성

노드 A가 난수와 함께 Request 한 것에 대한 응답으로, 노드 B가 Response하여, 강한 신선성을 제공하는 SNEP의 전체 프로토콜은 다음과 같다.

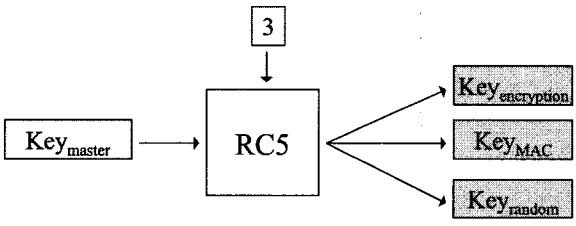
$$A \rightarrow B : N_a, R_a$$
$$B \rightarrow A : \{R_b\}(K_{encr},c), MAC(K_{MAC},N_b|C|\{R_b\}(K_{encr},c))$$

단, N_a는 A의 난수로 랜덤 하게 생성되며, R_a는 A의 Request, R_b는 B의 Response이다.

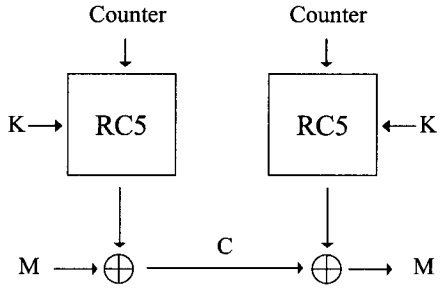
만약 MAC이 정확하게 검증된다면 노드A는 자기가 Request를 송신하고 난 후에, 노드B가 이에 대한 Response를 생산한 것이라고 인정하여, 강한 신선성이 보장된다.(그림 5-4 참조)

4.2 멀티캐스트 통신방식

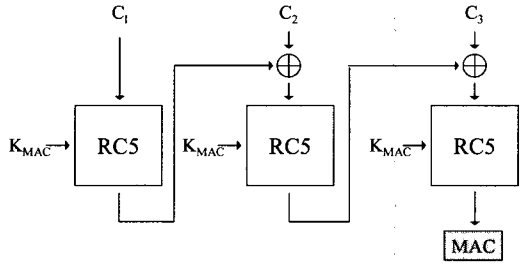
향후 무선 센서 네트워크는 홈네트워킹 서비스와 연계하여 가전제품이나, 센서 등 다양한 종류의 노드



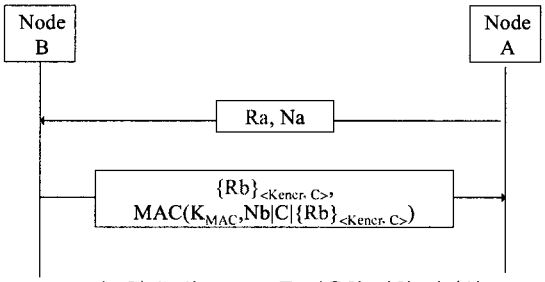
〔그림 5-1〕 키 생성 메커니즘



〔그림 5-2〕 SNEP의 암호화 과정



〔그림 5-3〕 SNEP의 MAC 생성메커니즘



〔그림 5-4〕 nonce를 사용한 강한 신선성

들과도 필요한 정보를 상호 교류하는 USN(Ubiquitous Sensor Network)으로 발전되어야 하기 때문에, 향후 USN으로 발전되더라도 센서노드를 최대한 재활용할 수 있게 하기 위하여, USN에서의 보안문제를 좀더 상세히 다루기로 한다. 멀티캐스트 통신방식에서는 송신자가 보낸 데이터 패킷이 다수의 수신자들에게 동시에 전달 되도록 그룹주소를 이용하므로, 그룹에 가입한 악의의 수신자가 송신자로 위장하여 패킷을 전송할 경우 서비스 거부 공격을 당하기 쉽고, 인터넷과 같은 공공 망을 이용 할 때에도 공격을 받을 가능성이 매우 높다.

따라서 다양한 공격으로부터 안전하게 멀티캐스트 서비스를 제공하기 위하여 소스인증, 기밀성, 무결성과 같은 보안 문제가 적합하게 고려되어야 한다.

4.2.1 μTESLA

μTESLA는 소스인증을 제공하는데 유효한 TESLA를 센서 네트워크 환경에 적합하도록 설계한 것이다.

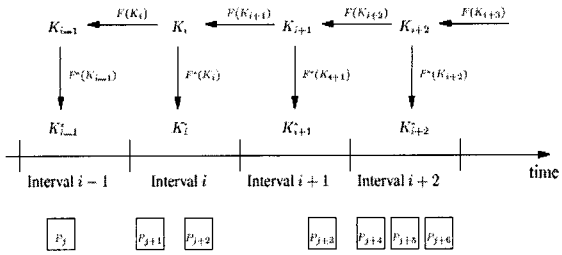
4.2.1.1 TESLA

TESLA는 멀티케스트 환경에서 소스인증을 제공하는데 유효한 프로토콜로,[3,12] 센서 네트워크의 멀티캐스트 인증에서부터 Ad-hoc네트워크 라우팅 프로토콜의 메시지 인증에 까지 여러 가지 다양한 애플리케이션에 폭 넓게 사용된다.[10]

TESLA의 주된 아이디어는 수신자가 송신자와 시간을 동기화 시키고, 송신자는 키체인을 생성하여 형성된 키체인의 키를 순차적으로 이용하며, 송신자 자신만이 알고 있는 키 K로 메시지인증코드를 계산해서 매 패킷에 첨부하면, 수신자는 패킷을 인증하지 못하는 상태에서 수신된 패킷을 저장하고, 잠시 후 송신자는 이때 사용하였던 키 K를 일정시간이 경과 한 후 노출하면, 수신자가 노출된 키를 이용하여 패킷을 인증하게 하는 것이다. 그 결과 패킷 당 한 개의 싱글 MAC만 있으면 멀티캐스트의 소스 인증을 제공할 수 있다.(그림 6 참조)

그러나 TESLA는 비대칭 암호 메커니즘인 디지털 서명(예,RSA)을 사용하여 최초 패킷을 인증하는데, 비대칭암호 메커니즘은 고도의 계산량과 통신량 그리고 저장용량을 요구한다.

또한 표준 TESLA는 패킷 당 약 24바이트의 오버헤드를 가지고 있으나, 센서노드는 약 30바이트 정도 길이의 매우 적은 메시지를 송신하기 때문에 모든 패킷에 TESLA의 키를 노출시키는 것은 실용적이지 못하며, 단방향(One-way) 키체인을 센서노드의 메모리에 넣는 것도 적당하지 않는 문제가 있어, 센서 네트워크에서 TESLA를 바로 사용하기에는 어려움이 있다.[9,16-17]



〔그림 6〕 TESLA 키체인 생성 및 MAC 키 구축방법

4.2.1.2 μTESLA 개요

μTESLA는 TESLA의 일부분을 변경하여, 센서 네트워크에 적당하도록 변형 시킨 것으로, 대칭형 메커니즘만으로 인증 서비스를 구현하였으며, 주기 당 1회씩만 키를 노출하여 적은 에너지를 소모하도록 하였고, 인증된 송신자의 수를 제한함으로써 센서 노드에서의 단 방향 키 체인을 저장하는 비용을 줄이도록 설계된 것이다.[8]

μTESLA의 대칭키 시간 지연 메커니즘은 대칭키의 노출시간을 지연시켜서 비대칭 메커니즘과 같이 동작하게 함으로서 유효한 멀티캐스트 인증을 제공한다.[8]

μTESLA의 동작 순서는 아래와 같이 살펴볼 수 있다.

송신자 셋업

단방향 키체인을 생성하기 위하여 송신자는 체인으로부터 마지막 키인 K_n을 랜덤 하게 선택한 후, 그밖에 다른 모든 키를 계산하기 위하여의사 랜덤 함수(Pseudo Random Function)F를 반복적으로 적용한다. ($K_i=F(K_{i+1})$)

인증된 패킷의 방송

시간을 타임 인터벌로 나누고, 송신자는 단방향 키체인의 각키를 일회 인터벌과 매핑(Mapping) 시킨다. 그리고 타임 인터벌 i일 때, 송신자는 현재 인터벌의 키 Ki를 사용해서 그 인터벌에서의 메시지인증코드(MAC)를 계산한다. 이때 MAC키는 공개적으로 알려진 단 방향 함수 F'에 의해서 생성된 키이다. ($K'_i=F'(K_i)$)

수신자 초기화

수신자가 체인의 인증된 키를 한번 갖게 되면, 체인의 나머지 키 들은 자동으로 인증(Self-authenticated)된다. 즉, 수신자가 키체인의 인증된 값 K_i를 갖고 있다면, 수신자는 $K_i = F(K_{i+1})$공식을 사용하여 K_{i+1}을 쉽게 인증 할 수 있다. 그러므로 μTESLA를 초기화하기 위하여, 각 수신자는 단 방향 키체인 중 신뢰성이 있는 키 하나를 전체 체인의 위임(Commitment)으로 소유할 필요가 있다.

μTESLA의 또 다른 요구사항은 송, 수신자는 상호 소결합 시간 동기(Loosely Time Synchronization)가 되어야 하고, 수신자는 단 방향 키체인의 키 노출 스케줄을 알고 있어야 한다. 인증된 키 위임과 마찬가지로 소결합 시간 동기도 양쪽 모두 강한 신선성과 점 대점 인증을 제공하는 메커니즘으로 운용될 수 있다.

수신자는 송신자에게 Request 메시지에 난수를 포함해서 송신한다. 송신자는 다음의 항목을 메시지에 포함시켜서 응답을 한다.

- T_s : 송신자 S의 현재시간(타임 동기용)
- K_i : 인터벌i에 사용했던 단방향 키체인의 키
- T_i : 인터벌 i의 출발시작시간
- T_{int} : 타임 인터벌의 지속시간
- δ : 노출지연시간(세 항목 T_i, T_{int}, δ은 키 노출 스케줄을 나타냄)

$M \rightarrow S : N_m$

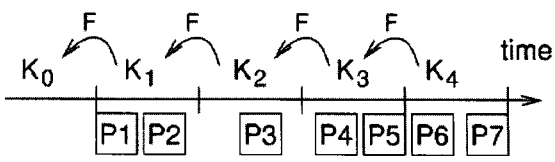
$S \rightarrow M : T_s|K_i|T_i|T_{int}|\delta MAC(K_{ms}, N_m|\ T_s|K_i|T_i|T_{int}|\delta)$

μTESLA에서 송신자는 데이터를 암호화할 필요는 없다. 메시지인증코드는 데이터를 인증하기 위하여 노드와 기지국이 나누어 갖고 있는 비밀키를 사용하며 난수 N_m은 노드가 신선성을 검증하는데 사용한다. 그리고 TESLA에서처럼 디지털 서명을 사용하는 대신에, μTESLA에서는 인증된 방송을 초기화하기 위하여 노드-to-기지국간 인증된 채널을 사용한다.

방송 패킷 인증

수신자가 메시지인증코드를 포함한 패킷을 수신하면, 공격자에 의해 패킷이 변조되지 않았는지 검사 할 필요가 있다. 만약, 입력되는 패킷이 보안조건을 만족하면, 수신자는 패킷을 저장한다.

그러나 패킷이 보통보다 더 길게 지연되는 등 보안



〔그림 7〕 키체인을 이용한 소스인증

조건을 위반하면, 그 패킷은 공격자에 의해 변조된 것이기 때문에 수신자는 패킷을 삭제한다. 왜냐하면, 공격자는 이미 타임 인터벌에 노출된 키와 메시지인증코드에 사용되었던 키를 알고 있기 때문에, 공격자가 패킷을 가짜로 만들 수 있는 위협이 있기 때문이다. 그러므로 송, 수신자는 서로 소결합 시간 동기가 되어야 할 필요가 있고, 수신자는 키 노출 스케줄을 알고 있을 필요가 있다.

센서노드는 전번 타임 인터벌의 키 K_j를 수신 하자마자, 센서노드는 키를 검사해서 인증을 한다. 검사방법은 센서노드가 이미 알고 있는 최근의 인증키 K_i와 단방향 함수 F를 이용해서 $F^{j-i}(K_j)$를 일치시켜본다.($K_i = F^{j-i}(K_j)$)

만약 검사가 성공하면, 새로운 키 K_j는 진실한 것이므로, 수신자는 MAC키를 계산하고, MAC을 검사하여, 타임 인터벌 i에서 j까지 기간 중에 보내졌던 모든 패킷을 인증 할 수 있다.

그림 7은 μTESLA의 키 인증 예를 보인 것으로, 타임 인터벌에 해당하는 키체인의 키와 한 개의 타임 인터벌에 송신된 모든 패킷들은 모두 동일한 키로 인증된다.

예를 들어 키들이 노출될 때까지의 타임인터벌을 2개의 타임인터벌이라 가정하고, 패킷을 인증하는 방법을 알아보자. 이때 수신자 노드가 소결합 시간 동기가 되고, 법적으로 인증된 방법으로 K_0을 안다고 가정한다.

인터벌 1에 송신된 패킷 P1과 P2는 키 K_1을 사용하는 한 개의 MAC을 갖고 있다. 패킷 P3은 K_2를 사용하는 MAC을 갖는다. 수신자는 그때까지 어떠한 패킷도 아직 인증할 수 없다. 여기서 패킷 P4, P5 그리고 P6을 모두 잃어 버렸다고 가정하자. 마찬가지로 키 K_1을 노출하는 패킷도 잃어 버렸다고 가정 한다면, 수신자는 P1을 아직 인증 할 수 없다. 인터벌 4에서 기지국은 키 K_2를 방송한다. 노드는 $K_0 = F(F(K_2))$를 검증함으로서 K_2를 인증한다. 그 결과로서 $K_1 = F(K_2)$도 알게 되어서, K_1을 갖는 패킷 P1, P2와 K_2를 갖는 P3를 인증 할 수 있다. 매 데이터 패킷에 노출키를 매번 첨가시키는 대신에, 키 노출은 패킷을 방

송하는 것과는 독립적으로 노출된다. 그리고 이 키 노출은 타임 인터벌에 연결이 된다. μTESLA환경 하에서는 송신자가 특별 패킷 내에 현재의 키를 포함하여 정기적으로 방송한다.

4.2.1.3 노드에서 인증된 데이터 방송

노드가 인증된 데이터를 방송한다고 가정하면, 노드의 메모리가 매우 제한 되어있어서 단 방향 키체인의 키를 저장 할 수 가 없고, 더 나아가서 최초로 생성된 키 K_n으로부터 각 키를 재계산해 내려면 계산적인 부담이 요구되며, 그밖에도 노드는 각 수신자와 키를 나누어 가질 수 없으므로 그 결과 키체인으로 인증된 Commitment를 송신해 내는 것은 노드-to-노드 키 협약에 큰 부담을 주게 된다.

또한 모든 수신자에게로 노출된 키를 방송하는 것은 노드에 부담을 주어 귀중한 배터리 에너지를 소진시킬수 있다.

이러한 문제의 해결을 위해 노드가 데이터를 방송하되, 기지국은 단 방향키체인을 유지하고, 필요시 키를 방송노드에게로 전송한다. 또한 방송노드의 에너지를 절감하기 위하여 기지국이 노출된 키를 방송하고, 새로운 수신자를 위한 최초 방송 절차를 기지국이 수행하는 방법이 있다.

4.2.1.4 노드와 노드간의 키 협약

초기화를 안전하게 하는 방법은 대칭키 셋업용으로 공개키 암호 프로토콜을 사용하는 것이다.[11-12] 그러나 센서 노드는 자원이 제한되어 있어서 공개키 암호를 사용해서 계산하려 해도 비용문제로 인해서 실행할 수가 없다. 그러므로 대칭키 알고리즘으로 프로토콜을 구축할 필요가 있다.

먼저, 키 셋업을 하는 과정에서 기지국을 신뢰하는 대리기관으로 사용하는 대칭키 프로토콜을 설계하도록 한다. 노드A가 노드B와 비밀 세션키 SK_{ab}를 나누어 갖기를 원한다고가정하자. A와 B는 어떤 비밀도 갖고 있지 않았기 때문에 S를 제3신뢰기관으로 사용할 필요가 있다. 기지국이 이러한 신뢰기관이 될 수 있다. 신뢰 셋업에서 A와 B 모두는 기지국과 비밀키 K_{as}와 K_{bs}를 각각 나누어 갖는다.

다음의 프로토콜들은 강한 키 신선성을 갖는 안전한 키 협약을 한다.

$A \rightarrow B : N_a, A$

$B \rightarrow S : N_a, N_b, A, B, MAC(K_{bs}, N_a|N_b|A|B)$

$S \rightarrow A : \{SK_{ab}\}K_{as}, MAC(K_{as}, N_a|B|\{SK_{ab}\}K_{as})$

$S \rightarrow B : \{SK_{ab}\}K_{bs}, MAC(K_{bs}, N_b|A|\{SK_{ab}\}K_{bs})$

프로토콜은 강한 신선성을 갖는 SNEP프로토콜을 사용 하며, 난수 N_a와 N_b는 A와 B양쪽에 강한 신선성을 보장한다.

SNEP프로토콜은 달성된 세션키 SK_{ab}의 기밀성을 보장해야 하며, 그리고 키가 진정으로 기지국에서 생산 된 것임을 확신하기 위하여 메시지 인증도 마찬가지로 보장해야 할 책임이 있다.

두 번째, 프로토콜 메시지 안에 있는 MAC은 서비스 거부 공격으로부터 기지국을 방어하는 것을 돕는다. 그래서 만약 노드들 중 하나로부터 적법한 Request를 수신하면, 기지국만이 A와 B로 두개의 메시지를 송신한다. 위 프로토콜의 장점은 기지국이 대부분의 전송업무를 모두 수행 한다는 것이다.

4.3 μTESLA에서의 효율적인 키체인 위임 배분

이 절에서는 키 체인 위임 (Commitment)을 효율적으로 배분하는 방법에 대해서 상세히 알아보도록 한다.TESLA는 최초의 파라미터를 배분하는 방법으로 방송을 사용한다. 이들 파라미터들은 송신자에 의해 생성된 디지털 서명에 의해서 신빙성이 보장이 된다. 그러나 각 센서 노드의 계산 능력과 대역폭이 작게 제한된 관계로, μTESLA는 이들 최초의 파라미터를 배분할 때, 공개키 암호방식을 사용할 수 없으므로, 그 대신, 유니캐스트통신을 하여, 기지국에서 센서 노드로 최초의 파라미터를 보내야 한다. 이러한 특성으로 인해서 μTESLA를 규모가 큰 센서 네트워크에서 사용하기가 어려워진다.

예를 들면 μTESLA는 10kbps의 대역폭과 30bytes의 메시지를 지원할 때, 기지국이 2,000개인 노드를 초기화 시키려면, 최초의 파라미터를 배분하기 위하여 최소한 4,000개의 패킷을 송, 수신 하여야 하기 때문에 채널이 완벽하게 동작한다 하더라도 최소한 $4,000 \times 30 \times 8 / 10,240 = 93.75$초가 소요되어, 이러한 방법으로는 수천 개의 노드를 갖고 있는 매우 규모가 큰 센서 네트워크로 확대 할 수 가 없다. 따라서 위와 같은 제약사항을 다루기 위하여 μTESLA를 확대한 개념이 제안되었다.[8]

기본적인 아이디어는 μTESLA에서 요구되는 최초의 파라미터를 유니캐스트에 기초를 하여 메시지를 전

송하는 대신, 파라미터를 미리 결정하고, 방송 하도록 하는 것이다. 가장 단순한 형태는, 센서 노드들을 초기화하는 도중에 μTESLA 파라미터를 배부하는 것이다.(각 센서와 기지국간 마스터키를 나누어 갖는 과정 중)

그러나 이 키체인은 길이가 고정된 기간에만 적용이 가능하고, 노드가 초기화 될 때 키체인의 시작시간을 예측하기가 힘들다는 문제점이 있어 실용적이지 못하다. 따라서 유연성을 더 제공하기 위하여, 매우 긴 키체인을 요구하지도 않고, μTESLA의 생명주기 기간을 특별히 연장할 수 있는, 다중 레벨 키체인 기법이 발표되었다. 이 기법에서는 낮은 레벨 키체인의 위임을 인증하기 위하여 높은 레벨 키체인을 사용한다.

그리고 메시지 손실과 서비스 거부 공격에 강력하게 대처하여 생존성을 더 개선할 수 있도록, 키체인 위임 메시지를 배분하는 방법을 제안 했는데, 그것은 주기적인 위임배분메시지 전송방식과 랜덤 선택방식을 이중(Redundant)으로 사용하는 기법이다.

이 기법을 사용하면, μTESLA의 좋은 특성 인 메시지 손실의 허용성, 재사용 방지 및 서비스 거부공격에 대한 저항성은 유지하면서, 기지국과 센서 노드 간 유니캐스트로 초기화를 하여야 하는 요구사항은 제거해 준다.[18]

앞으로 이 논문에서는 위임 K_0를 갖는 키체인을 〈K_0〉 로 표기한다.

4.3.1 이중 레벨 키체인[8]

이중 레벨 키체인은 높은 레벨 키체인(High-level)과 다중의 낮은 레벨(Low-level) 키체인들로 구성이 된다.

낮은 레벨 키체인들은 방송 메시지들을 인증하기 위하여 사용되는, 반면에 높은 레벨의 키체인은 낮은 레벨의 키체인 위임을 인증하고, 배분하는 데 사용된다.

높은 레벨 키체인은 센서 네트워크가 많은 키를 갖지 않고도, 수명기간을 오래 커버할 수 있게 하기 위해서, 타임 라인을 충분히 긴 인터벌로 나누어 사용한다. 낮은 레벨 키체인은 방송 메시지의 수신시간과 메시지의 검증 시간간의 지연을 충분히 허용 할 수 있는 짧은 인터벌을 사용한다.

4.3.1.1 초기화

초기화 과정 중에 모든 센서 노드들은 기지국과 그들의 클럭(Clock)을 동기 시킨다. (기지국과 모든 센서 노드는 타임 서비스로 그들의 클럭을 동기 시킬 수도 있다) 기지국은 다음의 파라미터를 추가로 생산한다.

먼저, 높은 레벨 키체인용 초기 랜덤 키 K_n을 선택한다.

그 다음에, 높은 레벨 키체인에서 센서 네트워크의 생명주기는 지속 시간이 $\triangle_0$인 n개의 긴 인터벌로 나누어서 $I_1, I_2, \ldots, I_n$로 나타낸다. 높은 레벨 키체인은 n+1개의 키 요소인 $K_0, K_1, K_2, \ldots, K_n$을 갖는데, 이 키 들은 랜덤 하게 선택한 K_n으로부터 생성된다. 그리고 i가 i=0, 1, 2, ..., n-1인 K_i를 구하려면 $K_i = F_0(K_{i+1})$로 계산한다. 여기서, F_0는 의사랜덤 함수이며, 키 K_i는 각 타임 인터벌 I_i와연관이 된다.

우리는 I_i의 시작시간을 T_i로 표기한다. 그래서 높은 레벨 키체인의 시작시간은 T_i가 된다. 높은 레벨 타임 인터벌의 지속시간은 네트워크 지연시간과 클럭 편차에 비해서 매우 길기 때문에, 다음번 타임 인터벌 I_{i+1}안에서 I_i의 높은 레벨 키 K_i를 노출하도록 선택한다. 그 결과, 우리는 센서노드가 t시간에 K_i로 인증되는 메시지를 수신하면 기지국이 키 K_i를 노출했는지, 노출하지 않았는지를 체크하기 위하여 다음 보안 조건을 점검한다. 즉, $t+\delta max < Ti+1$ 단, δmax는 기지국과 센서 노드간의 최대 클럭 편차이다.

센서 노드가 초기화되면, 클럭들은 기지국과 동기가 된다. 추가적으로, 시작시간 T_1, 높은 레벨 키체인의 위임 K_0, 각 높은 레벨 타임 인터벌의 $\triangle_0$지속시간, 각 낮은 레벨 타임 인터벌의 지속시간 $\triangle_1$, 낮은 레벨 키체인을 위한 노출 지연시간 d, 그리고 기지국과 센서 노드 사이의 최대 클럭 편차 δmax는 센서 네트워크의 생명주기 기간 동안 줄곧 센서들에게로 배분 된다.

4.3.1.2 위임배분메시지(CDM)방송

기지국이 센서로 인증된 메시지를 방송할 필요가 있을 때, TESLA와 μTESLA와 같은 방법으로 각 낮은 레벨 키체인용 파라미터들을 생산한다. 기지국이 개개의 작은 인터벌로 각 타임 인터벌 Ii를 나눈 것을 $I_{i,1}, I_{i,2}, \cdots, I_{i,m}$이라한다. 기지국은 $K_{i,m} = F_0(K_{i+1})$ 그리고 $K_{i,j} = F_1(K_{i,j+1})$을 계산해서 낮은 레벨 키체인을 생산한다. 단, j=0, 1, 2, ⋯, n-1그리고 F_1은 의사랜덤함수이다.

키 $K_{i,j}$는 타임 인터벌 $I_{i,j}$기간 동안에 방송된 메시지를 인증하기 위하여 사용 되는 키이다. 키체인 〈$K_{i,0}$〉 의 시작시간은T_i로 미리 결정된다. 그러므로 기지국은 낮은 레벨 키체인 〈$K_{i,0}$〉 을 갖는다.

타임 인터벌 I_i동안에 낮은 레벨 키체인 〈$K_{i,0}$〉 를 센서 노드가 사용하기 위해서는, 노드가 위임 $K_{i,0}$을 인증 하지 않으면 안 된다.

이러한 목적을 달성하기 위하여 TESLA를 확장한 즉시 인증방법을 사용한다. 특히 기지국은 각 타임 인터벌 I_i기간동안에, CDM_i라 표기하는 위임분배메시지(Commitment Distribution Message : CDM)를 방송한다.

이 메시지에는 낮은 레벨 키체인 $\langle K_{i+1,0}\rangle$ 의 위임 $K_{i+1,0}$와 위임 $K_{i+2,0}$의 이미지 $H(K_{i+2,0})$ 그리고 높은 레벨 키체인 안에 있는 키 K_i-1로 구성된다. 단 H는 의사랜덤함수이다.

기지국→센서 : $CDM_i = i \mid K_{i+1,0} \mid H(K_{i+2,0}) \mid MAC_{Ki'}(i \mid K_{i+1,0} \mid H(K_{i+2,0})) \mid K_{i-1}$

(단, "|"는 메시지의 연쇄연결을 나타내며, K_i'은 F_0, F_1과는 다른 의사랜덤함수를 갖는 K_i로부터 추출된다.)

그 결과 I_i기간 동안 낮은 레벨 키체인 $\langle K_{i,0}\rangle$ 을 사용하기 위하여, 기지국은 I_{i-2} 기간 동안에 키체인을 생산하고, CDM_{i-2} 안에 $H(K_{i,0})$을 배분한다. 그리고 CDM_{i-1} 안에는 위임$K_{i,0}$을 더 배분한다.

그리고 위임배분메시지의 손실 문제를 완화하기 위해서, 기지국은 매 타임 인터벌 I_i 동안 $F\times\triangle_0$점들을 랜덤 하게 선택하고, 이들 타임 점에서 CDM_i를 방송한다. (4.3.1.3.1 참조) 선택적으로 기지국은 타임 인터벌 I_1기간에 센서가 낮은 레벨 키체인 $\langle K_{1,0}\rangle$ 을 사용하고, CDM_1을 수신 할 때 $K_{2,0}$을 인증 할 수 있도록 하기 위해서 초기화 과정 중에 센서로 $K_{1,0}$와 $H(K_{2,0})$를 배분할 수 도 있다.

4.3.1.3 위임배분메시지 (CDM)인증

K_i는 인터벌 I_{i+1}기간 동안에 CDM_{i+1}안에서 노출되기 때문에, 각 센서는 CDM_{i+1}를 수신 할 때 까지 CDM_i를 저장할 필요가 있다. 각 센서는 키 K_j를 역시 저장하는데, K_j는 처음에 K_0로 시작 한다. CDM_i 내에서 키 K_{i-1}을 수신하고 나면, 센서는 이 키를 인증하는데, 검증방법은 $F_1^{i-1-j}(K_{i-1}) = K_j$ 이다. 그 후 센서는 현재의 K_j를 K_{i-1}로 바꾼다. 하나의 센서는 위임배분메시지들을 모두 수신 할 수 있다고 가정한다. 센서가 CDM_{i-1}를 한번 수신하면 I_{i-1}기간 동안에 위임 $K_{i,0}$을 인증할 수 있다. 센서가 CDM_{i-2}를 수신 했다고 가정하자. CDM_{i-1}을 수신하자마자, CDM_{i-1}에 노출되어있는 키 K_{i-2}로 CDM_{i-2}를 인증 할 수 있다. 그 후에 센서는 CDM_{i-1}에 있는 $K_{i,0}$에 H를 적용해서 CDM_{i-2}에 포함되어 있는 $H(K_{i,0})$과 동일한 결과가 얻어지면, $K_{i,0}$을 즉시 인증할 수 있다.

결과적으로 센서는 타임 인터벌 I_i기간 동안에 μTESLA 키체인 $\langle K_{i,0}\rangle$ 을 사용해서 기지국에서 송신된 방송메시지를 인증할 수 있다.

4.3.1.3.1 주기적인 위임배분메시지 전송방식[8]

μTESLA와 TESLA도 마찬가지지만 전송 중에 정상적인 메시지와 위임배분메시지가 손실되면, 복원 할 수 없는 문제점이 있다. 이 문제를 해결하기 위한 방법으로, 낮은 레벨의 키체인을 높은 레벨 키체인과 연결하는 방법과 위임배분메시지를 주기적으로 방송하는 방법이 있다.

먼저, 낮은 레벨 키체인을 높은 레벨 키체인으로 좀 더 연결하여, 전송 중 손실된 메시지를 복원 시킬 수 있다. 각 $K_{i,m}$은 또 다른 의사랜덤함수 F_{01}을 통해서 높은 레벨의 키 K_{i+1}로부터 각 키 $K_{i,m}$을 추출하도록 한다.

이 키 K_{i+1}은 다음 번 높은 레벨 타임 인터벌에 서 사용되는 것이다. 즉, $K_{i,m} = F_{01}(K_{i+1})$이다. 결과적으로, 비록 센서가 어떤 늦은 레벨의 키 $K_{i,j}'$(단, $j'\rangle=j$)를 수신 못한다 하더라도, $i'\rangle=i+1$인 K_i'를 노출하는 위임배분 메시지를 수신하는 한 센서는 어떠한 인증키 $K_{i,j}$도 복구 할 수 가 있다. 그림 8은 이 아이디어를 나타낸 것이다.

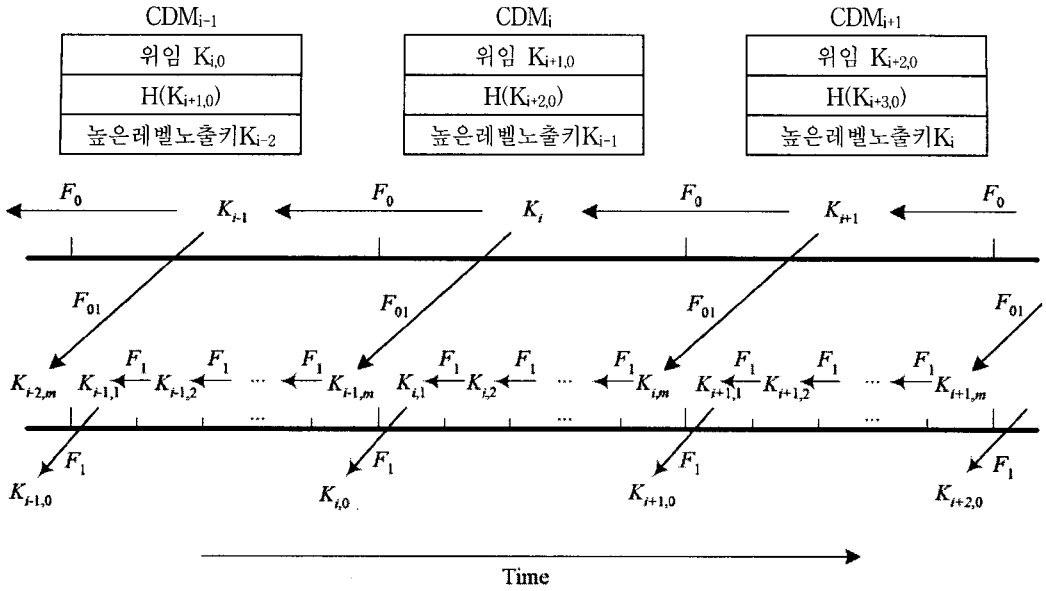
그러나 임시적인 통신장애가 발생되는 경우라면, 표준 고장 허용 방법을 사용하여 그 효과를 줄일 수 있다.

두 번째 위임배분메시지 손실 문제점을 완화하기 위한 방법은 기지국이 매 타임 인터벌 동안에 위임배분메시지를 주기적으로 방송하면 된다.

이 방송의 빈도를 F라 가정 하면, 각 위임 배분메시지는 $F\times\triangle_0$번 방송이 된다. 분석을 단순화하기 위해서, 센서가 위임배분메시지의 방송을 수신 못할 확률은 Pf라 가정한다. 그 결과 센서가 위임배분메시지의 어떤 복사본도 수신 못할 확률은 $Pf^{F\times\triangle 0}$로 줄어든다. 타임 인터벌 I_i 기간 중에 위임배분메시지를 갖고 있지 않지만, I_{i+1} 기간동안 방송 메시지를 얻기만 할 수 있으면, 센서는 먼젓번 타임 인터벌 기간 내의 모든 낮은 레벨 키들을 추출할 수 있다. 낮은 레벨 키체인의 유용성은 상응하는 위임배분메시지에 포함되어 있는 키체인의 위임을 인증하는 데에 있다.

센서는 CDM_{j-1}로 배부된 $K_{j,0}$ (단 $j\geq i$)를 인증하기 전에는 인증용의 낮은 레벨 키체인 $\langle K_{i,0}\rangle$ 을 사용할 수 없다.

이것은, 위임배분메시지가 공격자에게 매력적인 공



〔그림 8〕 이중 레벨 키체인

격 목표가 되게 하는 빌미가 되기도 한다. 공격자는 위임배분메시지의 배부를 중단 시킬 수 도 있고, 위임배분메시지가 송신되고 있을 때 에만 통신 채널을 마비시킬 수도 있다.

따라서 기지국은 랜덤 하게 나오는 숫자를 모르는 공격자라면 예측을 할 수 없도록 의사랜덤 방식이나, 랜덤 방식을 이용하여 위임배분메시지들을 송신할 필요가 있다.

공격자는 센서들이 혼돈하게 하기 위하여 위임배분메시지를 위조 할 수 도 있다.

만약 센서가 현행 CDM_i의 복사본을 갖고 있지 않다면, 정확한 $K_{i+1,0}$을 얻을 수 없을 것이다. 그리고 타임 인터벌 I_{i+1}기간 동안에 낮은 레벨의 키체인 $\langle K_{i+1,0} \rangle$ 을 사용할 수 없다.

TESLA를 즉시 인증 방식으로 확장한 방식이 서비스 거부 공격과 같은 공격에 강하게 설계 되었다 하더라도, 이 방식으로는 위의 공격을 완벽하게 방지할 수는 없다.

위임배분메시지 $CDM_i = i \mid K_{i+1,0} \mid H(K_{i+2,0}) \mid MAC_{Ki'}(i \mid K_{i+1,0} \mid H(K_{i+2,0})) \mid K_{i-1}$ 에서 공격자는 K_{i-1}와 $K_{i+1,0}$을 알 수 있으며, $H(K_{i+2,0})$을 $H(K_{i'+2,0})$로 대치해서 또 다른 메시지로 위조 할 수 있다. 즉, $CDM_{i'} = i \mid K_{i+1,0} \mid H(K_{i'+2,0}) \mid MAC_{Ki'}(i|K_{i+1,0}|H(K_{i+2,0}))|K_{i-1}$ 센서가 진짜 CDM_{i-1}의 복사본을 갖고 있다고 가정하면, K_{i-2}와 $H(K_{i+1,0})$는 모두 CDM_{i-1}속에 포함되어 있기 때문에 센서 노드는 K_{i-2}와 $H(K_{i+1,0})$를 갖고 K_{i-1}과 $K_{i+1,0}$을 각각 검증할 수 있다.

그렇지만 센서 노드는 $H(K_{i'+2,0})$의 신빙성을 검증할 방법이 없으므로, 만약 센서가 정확한 $H(K_{i+2,0})$을 포함한 CDM_i의 진짜 복사본을 저장하지 않는다면, 센서는 타임 인터벌 I_{i+1}기간 중에 CDM_{i+1}안에 있는 $K_{i+2,0}$을 인증할 수 가 없다.

만약 센서노드가 진짜 $K_{i+2,0}$을 포함하고 있는 CDM_{i+1}의 복사본을 얻을 기회를 잃는다면, 센서는 인터벌 I_{i+2}기간 중에 키체인 $\langle K_{i+2,0} \rangle$ 을 사용할 수 없게 된다.

그러나 이와 같은 문제점을 해결할 수 있는 한 가지 대응책은 I_{i-1}보다 좀 더 빠른 시간 인터벌 기간 내에 각 $K_{i,0}$을 배분 하도록 하면 된다.

이렇게 하면, 타임 인터벌 I_i전에, 상응하는 위임배분메시지를 수신 했던 센서가 비록 $H(K_{i,0})$을 갖고 있지 않다 하더라도 $K_{i,0}$을 인증 할 수 있는 이점이 있다. 그렇지만 이것이 모든 문제를 해결할 수 있는 것은 아니다. 만약 센서가 위임배분메시지의 진짜 복사본을 갖고 있지 않는다면, 센서는 결코 정확한 $K_{i,0}$을 얻을 수 없다. 이러한 맹점을 이용해서, 공격자는 먼저 언급 했던 것과 같이 단순하게 위임배분메시지를 위조할 수 있는 것이다.

4.3.1.3.2 다중 버퍼 랜덤 선택 방식

다중 버퍼 랜덤 선택 방식은 위임배분메시지들을

신뢰성 있게 방송 할 수 있도록 개선하는 방법으로 랜덤 선택 방식을 사용한다.

각 타임 인터벌 I_i 기간 중에 CDM_i메시지를 수신하면, 각 센서는 가능한 한 많은 수의 위조된 메시지를 폐기 처분하려고 시도한다.

센서가 I_i 기간 중에 위조된 CDM_i 메시지를 식별해 내는 방법은 두 가지 방법이 있다. 먼저, 센서는 만약 $F_0^{i-1-j}(K_{i-1})=K_j$이면 인증 할 수 있다. 단, K_{i-1}은 CDM_i내에 노출된 높은 레벨의 키이고, K_j는 먼저 번에 노출된 높은 레벨의 키이다. 이 시험에 불합격된 메시지는 확실하게 위조 된 것으로 폐기되어져야 한다.

두 번째로, 만약 CDM_i가 첫 번째 시험을 통과했다면, 센서는 I_{i-1} 기간 중에 수신했던 CDM_{i-1}을 인증하기 위하여 CDM_i 내에 노출된 키 K_{i-1}을 사용한다. 만약 센서가 CDM_{i-1}을 인증 할 수 있으면, CDM_{i-1} 안에 포함된 $H(K_{i+1,0})$로CDM_i내에 있는 $K_{i+1,0}$을 더 인증할 수 있다. 센서는 이 두 번째 시험에 불합격하면 CDM_i 메시지를 폐기할 수 있다.

이들 두개의 시험을 실시하면, 위조된 메시지들을 대충 걸러낼 수 있다. 하지만 이들 메시지들은 앞서 말한 것과 같이 위조된 메시지들을 모두 제외시킬 수는 없다.

센서가 진짜 CDM_i메시지를 갖게 할 가능성을 좀 더 높이기 위하여 기지국은 위의 두 가지 시험을 통과한 CDM_i메시지를 저장 시키는 방법으로 랜덤 선택 방법을 사용한다.

우리의 목표는 서비스 거부공격이 어렵게 만드는 것이다.

일부 전략들은 확장된 TESLA와 TESLA 프로토콜뿐만 아니라 낮은 레벨의 키체인에도 적용할 수 있다. 일반성을 잃지 않게 하기 위해서, 우리는 앞서 언급한 두 가지 시험을 실시해서 CDM_i의 각 복사본들은 타임 인터벌 I_i기간 중에 약하게 인증된 것이라고 가정한다.

센서 노드가 각 타임 인터벌에 방송되는 위임배분 메시지용으로 오직 한 개의 버퍼만을 갖고 있는데, 센서 노드가 n개의 CDM_i의 복사본을 수신한다면, 모든 복사본들이 버퍼에 저장될 확률은 1/n의 같은 확률을 갖는다. 여기서 CDM_i의 모든 복사본이 선택될 확률이 모두 같게 만들지 않으면, 프로토콜을 아는 공격자가 위조된 위임배분메시지가 선택되도록 만들 수 있는 위협이 있다. 센서 노드가 진짜 CDM_i의 복사본을 가질 확률은$P(CDM_i)=1-P$ 단, P=(위조된 복사본의 수/총복사본의 수)이다.

그러나 여기서 m개의 버퍼가 있다고 가정하자. 각 타임 인터벌 Ii기간 중에 센서 노드는 m개의 CDM_i 복사본 중 처음 m개의 복사본을 저장할 수 있다. k > m인 k번째 복사본을 생각하면, 센서노드는 확률 m/k로 이 복사본을 저장할 수 있다. 만약, 한 개의 복사본이 저장되어야 한다면, 센서노드는 m개의 버퍼들 중 한 개의 버퍼를 랜덤 하게 선택하고, 상응하는 복사본을 대치한다. 만약 센서 노드가 n개의 CDM_i 복사본을 수신 한다면, 모든 복사본들이 m개의 버퍼들 중에서 한 개의 버퍼에 저장될 확률은 똑같이 m/n이 된다는 것을 쉽게 알 수 있다.

만약, 타임 인터벌 I_{i+1} 기간 동안에, 센서 노드가 CDM_{i+1}의 복사본을 수신해서, 약하게 인증한다면, 센서노드는 CDM_i의 진짜 복사본을 쉽게 검증할 수 있다. 특히, 센서 노드는 저장되어 있는 CDM_i 복사본들의 MAC을 검증하기 위하여 CDM_{i+1}에 노출되어 있는 키 K_i를 사용한다.

센서 노드가 진짜 복사본을 한번 찾으면, 그 밖의 다른 모든 버퍼들을 폐기할 수 있다.

만약 이러한 일이 일어난다면, 센서노드는 CDM_{i+1}의 내용을 즉시 인증할 수 있다.

만약 센서노드가 위의 검증을 실시하고 난 후에도 CDM_i의 진짜 복사본을 찾을 수 없다면, 센서노드는 저장되어있는 모든 CDM_i의 복사본들은 위조 된 것이라고 간주하고 이 모든 것들을 폐기할 수 있다.

그 후, 센서 노드는 CDM_{i+1}의 복사본들에 대해서도 랜덤 선택 프로세스를 계속 반복할 필요가 있다.

이러한 전략을 수행하기 위해서, 센서 노드는 많아야 m+1개의 위임 배분메시지용 버퍼가 필요하다. 즉, CDM_i의 복사본들 용으로 m개의 버퍼와, CDM_{i+1} 중 첫 번째로 약하게 인증된 복사본용으로 한 개의 버퍼가 필요하다.

m개의 버퍼를 갖는 랜덤 선택 방식에서 센서 노드가 한 개의 CDM_i 진짜 복사본을 가질 확률은 $P(CDM_i)=1-P^m$ 단, P = 위조된 복사본의 수 / 총 복사본의 수로 추상 할 수 있다.

따라서 주기적인 위임배분메시지 전송 방식과 다중 버퍼 랜덤 방식을 전부 사용한 위임배분메시지 인증 방식은 다음과 같다.

센서 노드 S는 위임배분메시지용 버퍼를 m+1개 갖는다고 가정한다. 센서 노드 S가 타임 인터벌 Ii 기간 중의 타임 ti일 때 CDM_i의 한 개의 복사본을 수신하면, 센서노드는 다음과 같이 메시지를 진행시킨다.

1) 센서 노드S는 CDM_i의 보안조건을 점검한다. 즉, $t_1+\delta max < T_{i+1}$인지 확인하고, S는 보안조건이 맞지 않으면 패킷을 폐기하고, 정지한다.
2) 만약 S가 인증된 CDM_{i-1}의 복사본을 갖고 있다면, S는 CDM_i의 선행 복사본을 수신 하고, K_{i-1}과 $H(K_{i+2,0})$을 저장시키지 않으면 안 된다. 현재 CDM_i내에 있는 K_{i-1}과 $H(K_{i+2,0})$가 저장되어 있는 선행 복사본들과 같은가 점검한다. 만약 같다면 6번 단계를 진행한다. 그렇지 않으면 S는 메시지들을 폐기하고, 정지한다.
3) S는 먼저 노출된 키 K_j에 대응해서 K_{i-1}을 인증한다. 이것은 $K_{i-1}=F_1^{i-1-j}(K_j)$를 검증하므로 서 인증 할 수 있다. (K_0는 초기화 기간 중 각 센서노드로 배분되었기 때문에 K_j는 항상 존재한다는 것을 유념 할 것)
4) CDM_{i-1}의 각 복사본 C의 경우, S는 CDM_i에서 노출된 키 K_{i-1}로 그 자체의 MAC을 검증함으로써 C를 인증한다. 만약 이 검증이 실패하면, S는 C를 폐기하고, 계속해서 다음번 CDM_{i-1}의 복사본을 검증한다. 검증이 성공되면, S는 CDM_{i-1}의 모든 다른 복사본을 폐기하고 C가 CDM_{i-1}의 인증된 복사본이라고 만든다.
5) 만약 S가 CDM_{i-1}의 인증된 복사본을 갖는다면, S는 CDM_i에 동봉된 $K_{i+1,0}$을 인증한다. 이때 검증방법은 H를 $K_{i+1,0}$에 적용해서 얻은 결과식이 CDM_{i-1}에 포함되어있는 $H(K_{i+1,0})$과 같으면 된다. 만약 이것이 실패하면, S는 CDM_i 의 복사본을 단순히 폐기하고 ,정지한다. 그러나 성공하면, S는 $H(K_{i+1,0})$을 저장한다.
6) S는 CDM_i의 현재 복사본을 저장할 것인지 아닌지를 결정하기 위하여 랜덤 선택 방식을 사용한다. (만약 현재 단계가 처리되고 있다면, CDM_{i-1}의 모든 복사본은 폐기 되어져야 한다는 것을 유념 할 것)

더 나아가 CDM_i의 현재 복사본은 j차 복사본이라 가정하고, 만약 $j < m$이면, S는 저장할 버퍼공간이 있는 것이므로, S는 비어있는 버퍼 중 한 개에 현재 복사본을 저장한다. 그렇지 않으면 S는 확률 m/j로 이 복사본을 유지해서, m개의 예약된 버퍼 중에서 랜덤하게 선택된 버퍼 안에 현재 복사본을 저장 시킨다.

CDM_i안에 있는 $K_{i+1,0}$를 즉시 인증한 것은 CDM_i 그 자체를 인증 했다는 의미가 아니라는 것에 유념할 것. 공격자는 CDM_i내에 있는 $H(K_{i+2,0})$을 대치할 수 있으며, 검증을 통과하는 결과 메시지를 가질 수도 있다. 그러므로 S는 CDM_i의 복사본들을 저장하기 위해 랜덤 선택 방식을 사용하지 않으면 안 된다.

4.3.1.4 정상적인 메시지 방송 및 인증

정상적인 메시지의 방송과 인증은 확장된 TESLA[10]와 같은 방법으로 실행된다. 단, 위임배분메시지들을 배분하고 인증하는 과정에서 처리되는 키체인 위임을 배분하는 것은 예외로 한다.

4.3.2다중 레벨 키체인 기법

이중 레벨 키체인 기법은 m레벨 키체인 기법으로 쉽게 확장 될 수 있다.

m 레벨 키체인은 위에서부터 아래로 0레벨에서 m-1 레벨까지 배치될 수 있다. (m-1) 레벨 키체인 내에 있는 키들은 데이터 패킷들을 인증하는 데 사용되며, 높은 레벨 키체인은 낮은 레벨 키체인들의 위임을 즉시 배분하기 위해서 사용된다.

톱 레벨(0레벨) 키체인의 제일 마지막 키만이 랜덤하게 선택될 필요가 있다. 즉, 톱 레벨 키체인에 있는 모든 다른 키들은 이 키로부터 생산될 수 있다. 그래서 레벨i에 ($1 < I \leq m-1$)있는 모든 키체인들은 레벨i-1에 있는 키들로부터 생산된다.

같은 방법으로, 낮은 레벨 키체인들은 이중 레벨 키체인 기법에서와 같이 높은 레벨 키체인으로부터 생산된다.

높은 레벨 키체인은 낮은 레벨 키체인용 위임을 즉시 배분하기 위하여 위임 배분메시지를 방송할 책임이 있다.

보안 측면에서, 의사랜덤함수가족이 필요하다. 각 레벨과 이웃 레벨간의 의사랜덤함수는 서로 달라야 한다.

우리는 버퍼에 CDM패킷들을 저장하기 위해서 다중 버퍼 랜덤 선택 메커니즘을 역시 사용한다.

다중 레벨 키체인을 사용하는 장점은 이중 레벨 키체인 기법과 비교해서 각 키체인에 있는 키들의 수가 적거나, 비슷하게 소요되고, 또 각키체인 레벨에서의 지속시간이 짧다는 것이다.

결과적으로 긴 기간 동안으로 규모를 넓힐 수 있어, 다중레벨 키체인 기법은 서비스 거부 공격에 더 취약하지는 않다.

서비스 거부 공격을 성공시키는 요인은 센서노드 안에 있는 버퍼의 용량과 위조된 CDM메시지들의 수와의 백분율과 관계가 있다.

기지국이 일정 비율의 진짜CDM메시지를 유지하고

있는 한, 위조된 CDM메시지들의 백분율은 그리 높지 않다.

기지국은 통신비용을 줄이기 위하여, 다른 레벨 키 체인들을 위한 CDM메시지들을 피기백 방식(Piggy-back)으로 수송할 수 있다.

그럼에도 불구하고, 더 많은 레벨의 키체인을 갖는다면, 기지국과 센서 노드 양쪽에 오버헤드가 증가하게 되기 때문에, 다중 레벨 키체인용으로 더 많은 자원을 할당하면, 기지국에는 문제가 되지 않는다 하더라도, 자원이 제한된 센서 노드에서는 키체인 위임용으로 더 많은 버퍼들을 유지하지 않으면 안 된다.

추가적으로, 우리가 더 많은 레벨들을 가지면, CDM 메시지들을 송신하는 데에 더 많은 대역폭이 소요된다.

그러므로 우리는 가능한 한 센서 네트워크의 수명 기간을 맞추기 위한 최소한의 레벨들을 가지도록 하여야 한다.

V. 결론 및 향후 연구과제

이 논문에서는 무선 센서 네트워크를 이용한 무인 경비 시스템에서의 정보 보안상 취약점을 도출하고, 도출된 취약점을 해결하기 위한 방법으로 현재까지 발표된 센서 네트워크 보안 프로토콜 중에서, SPINS를 적용 할 것을 제안했다.

SPINS는 SNEP과 μTESLA로 구성되는데, SNEP은 데이터 기밀성, 양단간 데이터 인증, 무결성 그리고 신선성을 제공하고, μTESLA는 데이터 방송의 인증을 제공한다.

따라서 SNEP은 현재 유선으로 구성되어있는 센서 네트워크를 무선 센서네트워크로 즉시 대체할 수 있는 기술이고, 향후 무선 센서 네트워크가 유비쿼터스 홈 네트워크로 발전되었을 경우, μTESLA를 포함한 SPINS는 멀티캐스트 통신방식으로 사용할 수 있을 것이다.

그리고 키 체인 위임을 효율적으로 배분하는 μTESLA 다중 레벨 키 체인 기법, 주기적인 위임배분 메시지 방송방식 그리고 랜덤 선택 방식 과 같은 몇 가지 기술도 무인 방범 시스템에서 사용할 수 있을 것으로 제안 했는데, 이 기법들은 서비스 거부 공격을 퇴치하고, 생존성을 개선할 수 있는 기법들로 알려져 있다.

다만, 단점이 있다면, 타임 인터벌기간 동안 센서노드가 위임을 얻지 못하고, 센서노드가 오랜 기간 동안 기다리지 않으면 안 되는 문제, 그리고 다중의 기지국이 포함되어 있을 때의 방송인증 방법 등은 더 연구해야 할 것이다.

그리고 실제 무선 센서 네트워크를 이용해서 무인 경비 시스템에 접목했을 경우의 가능성을 실험해 보아야 할 것 이다.

참 고 문 헌

[1] Mark Weiser. The Computer for the 21 Centry. Scientific American. Vol. 256. No.3. pp. 94-104. Sep. 1991

[2] 정보통신부, "U-센서 네트워크 구축 기본계획" 2004.2.17

[3] H. Abrach, S.Bhatt, J.Charlson, H. Dui. Rose, A. Sheth, B. Shucker, J. Deng, R. Han, "MANTIS: System Support for Multimodal Network of In-Situ Sensors", In Proc. of 2nd Workshop on Wireless Sensor Networks and Applications (WSNA' 03), San Diego, CA, Sep, 2003

[4] B.j.Bonfils, P. Bonnet, "Adaptive and Decentralized Operator Placement for In-Network Query Processing", IPSN'03, April, 2003, LNCS 2634

[5] H. Han, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", Appears in IEEE Symposium on Security and Privacy 2003

[6] K. S. J. Pister, J, M Kahn, and B. E. Boser. Smart dust : Wireless networks of millimeter-scale sensor nodes, 1999

[7] http://www.citris.berkeley.edu/index.html

[8] A. Perrig, R. Szewczyk, J.D.Tygar, Victorwen D. E. Culler : SPINS : "Security Protocols for Sensor Networks, Wireless Networks" 8, 521.534, 2002

[9] Diameter CMS Security Application, draft-ietf-aaa-diameter-cms-sec-04.txt, www.ietf.org/html.charters/aaa-charter.html

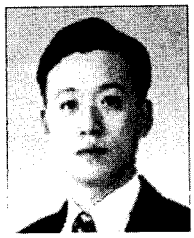
[10] Adrian Perrig, Ran Canetti, Dawn Song and Doug Tygar. "Efficient and secure source authentication for mul-

ticast. In Network and Distributed System security symposium, NDSS '01, February 2001
[11] Steven Bellovin and Michael Merrit. Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In First ACM Conference on Computer and Communications Security. CCS-1, Pages 244-250, 1993
[12] D. Harkins and D. Carrel. The internet key exchange(IKE). Request for Comments 2409, Information Sciences Institute, University of Southern California, November 1998
[13] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. Journal of Computer Security, 28:270-299,1984
[14] R.L. Rivest."The RC-5 Encryption algorithm. Proc. 1st Workshop on Fast Software Encryption, Pages 86-96,1995
[15] U.S National Institute of Standards and Technology (NIST). DES model of operation. Federal Information Processing Standards Publication 81(FIPS PUB 81)
[16] R. Gennaro and P. Rohatgi. "How to sign digital streams. In Burt Kaliski, editor, Advances in Cryptology-Crypto '97, Pages 180-197, Berlin, 1997. Springer-Verlag. Lecture Notes in Computer Science Vol. 1294
[17] Pankaj Rohatgi. A compact and fast hybrid signature scheme for multicast packet authentication. In 6th ACM Conference on Computer and Communications Security, November 1999.
[18] Donggang Liu, Peng Ning "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks" E-mail : dliu@unity.ncsu.edu
[19] A.Perrig, and J.T.D.S.R. Canetti, Briscoe. TESLA: Multicast source authentication transform. IRTF draft, draft-irtf-smug-tesla-00.txt, November 2000
[21] 조영섭, 조상래, 유인태, 진승헌, 정교일 : 유비쿼터스 컴퓨팅과 보안 요구사항 분석, 정보보호학회지, 2004. 2
[22] 주학수, 권현조, 강달천, 윤재호, 박배효, 전길수, 이재일 : RFID/USN정보보호 위협

〈著 者 紹 介〉

이 성 재 (SeongJae Lee)

1989년 8월 : 한양대학교 산업대학원 전자통신과(석사)
2000년 1월~2004년 3월 : (주)KT 임원
2004년 3월~현재 : (주)KT링커스 감사
〈관심분야〉 네트워크보안, USN보안, 공개키 기반구조, 이동통신보안



김 대 경 (DaeKyung Kim)

1995년 2월 : 경성대학교 컴퓨터공학과 졸업(학사)
2004년 2월 : 순천향대학교 산업대학원 졸업(석사)
2004년 9월~현재 : 순천향대학교 일반대학원 재학(박사)
〈관심분야〉 USN보안, 이동통신 보안, 전자투표

이 재 근(JaeGeun Lee)

1988년 3월~2002년 2월 : 고려대학교 경상대학 응용통계학과 졸업(학사)
2000년 3월~2002년 8월 : 순천향대학교 산업정보대학원 졸업(석사)
1994년 7월~1999년 7월 : 한국전산원 주임연구원
1999년 1월~2003년 4월 : 대통령비서실 총무 비서실 전산정보 담당 행정관
2003년 4월~현재 : 한국전산원 책임연구원
〈관심분야〉 네트워크보안, USN보안, 이동통신보안, 공개키기반구조PKI
E-mail : jglee@nca.or.kr

염 흥 열 (HeungYoul Youm)

1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2003년 9월~2004년 3월 ITU-T SG17/Q10, Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
〈관심분야〉 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안
E-mail : hyyoum@sch.ac.kr