논문 2007-02-17

유비쿼터스 홈 네트워크에서의 ZigBee End-to-End 보안 기술

(ZigBee End-to-End Security For Ubiquitous Home Network)

박 우 출*, 이 명 수, 윤 명 현, 김 성 동, 양 성 현
(W.C. Park, M.S Lee, M.H. Yoon, S.D. Kim, S.H. Yang)

Abstract : 무선 기술이 가지는 장점인 설치의 편리성, 기동성으로 인하여, ZigBee를 이용한 홈 네트워크 서비스 활용성에 대한 기술개발이 활발히 진행되고 있다. 이러한 유비쿼터스 홈 서비스의 활용성에도 불구하고 ZigBee 기반 홈 기기나 센서 정보의 도청, 비정상적인 패킷의 유통, 메시지 재사용등의 데이터 위/변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 공격등에 쉽게 노출되어 있다. 본 논문에서는 이에 대한 효과적인 대응과 관리 처리를 위하여, 유비쿼터스 홈 네트워크에서의 ZigBee 기술을 사용할 시에 발생할 수 있는 보안 문제점을 해결하기 위한 ZigBee 기반 End-to-End 보안 기술을 개발하였다.
본 기술 개발의 특징은 ZigBee Device, 코디네이터/게이트웨이 영역은 ZigBee 표준 스펙을 구현하였으며, 응용어플리케이션/서버 영역은 표준 스펙이 정의 되어 있지 않으나, 이 부분을 유비쿼터스 홈 네트워크 서비스 관점에서 설계 및 구현하였다. ZigBee 디바이스가 가지는 하드웨어 자원의 빈약성을 고려하여 최대한 보안 기능을 리소스가 풍부한 응용어플리케이션/서버의 자원 활용에 촛점을 맞췄다.

Keywords : ZigBee, End-to-End, Security, Ubiquitous, Home Network

Ⅰ. 서 론

현대의 주거문화는 유비쿼터스 홈으로 진화하면서 유무선 기반으로 가정 내의 다양한 가전기기 및 센서들이 네트워크로 상호 연결되어 다양한 서비스를 가능하게 하는 방향으로 발전하고 있는 추세이다. 다른 특징은 지식적이고, 상황적응적인 상호 연동을 통하여 사용자의 편의를 극대화시킬 수 있는 기술을 추구하고 있다. 현재 세계 각국은 핵심 기술의 선점뿐만 아니라 보다 지능화, 고도화된 유비쿼터스 홈서비스 제공을 위한 기술 개발에 집중하고 있다. 이러한 유비쿼터스 홈서비스의 활용성에도 불구하고 무선 홈 기기나 무선 센서 정보의 도청, 비정상적인 패킷의 유통, 메시지의 재사용 등의 데이터 위·변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 등의 공격에 쉽게 노출되어 있어, 이에 대한 효과적인 대응과 관리 처리 기술이 급속도로 요구되고 있다.

보안 구조가 있다[1]. 베이스스테이션과 클러스터 구조를 중심으로 aggregator를 가지는 기본 구조를 기반으로 한 그룹 키 관리 연구가 있다[2]. 센서 네트워크에서 센서 노드간 Pairwise Key 설정을 위해 제안한 프로토콜이 베이스 스테이션이 먼저 다량의 랜덤 키를 생성하여 이를 키 풀에 저장하고 키 풀에서 무작위로 임의의 키 집합을 선택하여 키 링을 생성하여 이를 각 센서 노드에게 분배한다. 센서 노드들은 자신이 갖고 있는 키 링의 키 정보를 이웃 노드들에게 브로드캐스팅 함으로써 무선 통신 반경 내에서 자신의 이웃하는 노드들과 공유키를 찾는다[3]. Brutch는 센서네트워크에서 침입 탐지 시스템에 대하여 3가지 형태를 설계하였으며, 첫째는 stand-alone 구조이며, 각 노드 각각이 독립적으로 침입 탐지 시스템이며, 각각이 침입에 대하여 책임을 진다. 두 번째 구조는 각 노드들이 분산 및 협력을 통하여 침입 탐지에 대응한다. 세 번째는 hierarchical 구조 형태이며, 다중 구조의 센서네트워크에서 클러스터 헤드 형태를 가진다[4].

* 교신저자(Corresponding Author)
논문접수 : 2007.6.15. 채택확정 : 2007. 9. 6.
박우출, 이명수, 윤명현, 김성동 : 전자부품연구원 유비쿼터스컴퓨팅연구센터
양성현 : 광운대학교 전자공학과
※ 본 논문은 산업자원부 성장동력기술개발사업의 결과물임.

1. 유비쿼터스 센서네트워크 관련 보안 취약점

ZigBee와 같은 무선 센서네트워크 관련 보안 문제점은 I/O 장치 및 무선 통신을 사용하므로 인한 공격 받기 쉬운 구조를 가지고 있으며, 높은 자원 제약성으로 인해 기존의 보안 기술 적용이 어려우며, 제작 비용등의 이유로 tamper resistance 기술을 구현하기 어렵다. 노드사이의 통신 정보를 모니터링을 통하여 정보를 쉽게 얻을 수 있다. 무선 센서네트워크가 가지는 특징인 RF가 간단한 구조로 인하여 패킷 스니핑이 가능하다. Radio Jamming 등을 사용한 DoS 공격의 용이성, 자원 고갈 공격의 용이성, 센서 노드에 대한 공격의 용이성이 있다. 또한 공격자는 여러 센서 노드로 부터 낮은 정보량의 데이터를 가공하여 주요 정보를 얻을 수 있다.

2. 유비쿼터스 센서네트워크 공격 기술

무선 센서네트워크에서의 공격은 아래 그림과 같이 수동적 공격(Passive Attacks)과 능동적 공격(Active Attacks)으로 분류하며, 수동적 공격은 네트워크에 대한 직접적인 위해 없이 네트워크 트래픽을 수집하거나 분석하는 행위로, 감청과 트래픽 분석으로 분류할 수 있다. 능동적 공격은 공격자가 네트워크에 대한 직접적인 위해를 가하는 행위들을 말하며, 변장 공격(Masquerade attack), 재전송 공격(Replay Attack), 메시지 수정 공격(Message Mdoification Attack), 서비스 거부 공격(Denial-of-Service)등으로 분류한다.

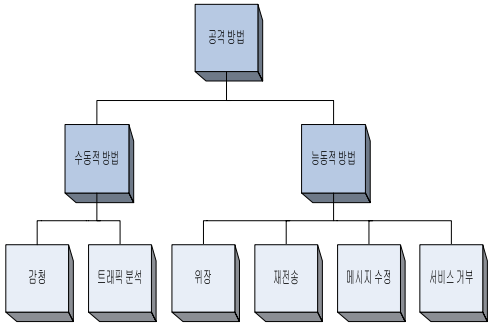

그림 1. 무선 센서네트워크 공격 분류
Fig. 1. Attacks of Wireless Sensor Network

Ⅱ. ZigBee 보안 취약점 분석

ZigBee 프로토콜은 다양한 어플리케이션들을 지원하고 있으며 제공되는 서비스들은 보안 문제에 대해 민감하게 다루어져야 한다. 하지만 ZigBee 스펙 자체에 여러 보안 취약점을 가지고 있어서 이를 힘들게 하고 있다. 이 장에서는 ZigBee 스펙이 지니고 있는 취약점 들을 기술하고 있으며 이는 크게 키 관리문제, ACL(Access Control List) 관리 문제, 네트워크 관리 문제, 메시지 보호의 4가지로 분류 할 수 있다[5-8].

1.1 키 노출

안전한 노드간의 통신을 위해 각 노드들은 여러 종류의 키를 보유해야 하며, 분배된 키들을 이용해서 보내고자 하는 메시지를 암호화함으로써 안전성을 보장할 수 있다. 키를 분배하고 노드 내에서 보관하는 방법에 있어서는 다양한 보안 메커니즘을 사용하여 보안 수준이 유지되어야 한다.

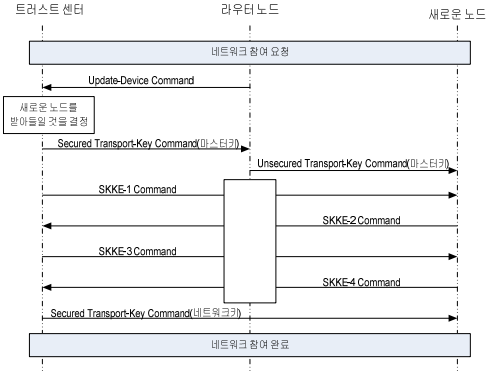

그림 2. Commercial Mode 노드 Join 과정
Fig. 2. Process of Joining Commercial Mode

ZigBee 네트워크에 새로운 노드가 참가할 때 그 노드는 트러스트센터(Trust Center)로부터 그 네트워크에서 사용할 마스터키를 전송 받아야 한다. 그렇지만 새로 참가한 노드와 기존의 네트워크 간에는 미리 설정된 어떠한 보안 메커니즘도 없기 때문에 마스터키를 평문 형태로 전송 할 수밖에 없다.

그림 2는 트러스트 센터의 보안 모드가 커머셜 모드일 때의 노드 조인과정을 설명하고 있다. 키 전송 후에 이루어지는 통신들은 해당 키를 사용하여 암호화를 하고 있지만 정작 마스터키는 보안이 적용되지 않은 방법으로 전송되고 있는 것을 볼 수

있다. 이렇게 키가 쉽게 노출될 수 있음에 따라 공격자는 이 정보를 감청하여 해당 네트워크의 마스터 키를 알아 낼 수 있다. 만약 마스터키가 노출된다면 공격 노드는 자신이 네트워크 코디네이터인 것처럼 행동 할 수 있고, 거짓된 비콘 메시지를 생성하는 것이 가능해짐으로써 네트워크 전반에 걸친 위해를 가할 수 있다[13].

1.2 ACL 관리 문제

ZigBee 네트워크의 노드는 자신이 키를 공유하고 있는 노드들에 대한 데이터베이스인 ACL을 가지고 있으며, 여기에 저장되는 정보들은 통신의 보안성을 다루는 중요한 것이기에 조심스럽게 다루어져야 한다.

서로 다른 엔트리 간에 동일한 키 등록 방법은 다음과 같다. ZigBee 네트워크가 암호화 방법으로 AES-CTR 모드를 이용하며, 위에서 언급한 대로 여러 가지 이유로 인해 서로 다른 노드의 ACL 엔트리에 동일한 키를 등록해서 사용한다면 메시지를 전송하는 노드의 넌스 값이 노출되는 위험을 가지고 있다. 공격자는 ACL에서 동일한 키를 사용하여 암호화된 두 노드에게 전송되는 동일한 내용을 담고 있는 메시지를 감청한다. 공격자는 이렇게 알아낸 2개의 암호화된 메시지를 XOR함으로써 두개의 평문을 XOR하는 것과 같은 결과를 얻어 낼 수 있고, 이를 통해 넌스값을 추출 해 낼 수 있다. ACL 내에 동일한 키를 가지는 2개 이상의 노드가 존재할 수 있는 예로는 다음과 같은 경우가 있다[10].

그림 3 을 보면 이 노드는 ACL내의 노드들이 동일한 키를 소유하는 그룹을 구성하고 있다는 것을 표현하기 위해 2개의 다른 노드들에 대한 ACL 엔트리에 같은 키를 저장하고 있다.

그림 3은 ZigBee 네트워크에서 노드의 이동이 발생했을 때 해당 노드의 ACL의 변화를 나타내고 있다. 노드가 이동을 하게 되어 부모 노드가 바뀌게 되면 새롭게 연결을 맺은 부모 노드를 위해 엔트리를 하나 더 생성하게 되고 이것은 기존의 부모 노드의 ACL 엔트리를 복사해서 사용한다. 하지만 부모노드가 바뀌었음에도 불구하고 이동 직전의 통신에 대한 연결로 인하여 이전 부모노드의 ACL 엔트리를 잠시 유지하게 되는데 이 짧은 순간에 서로 다른 두 노드가 동일한 키를 가지게 된다.

주소	키	추가보안 요소
디폴트	k1	xxxxx
p	k2	yyyyy

→

주소	키	추가보안 요소
디폴트	k1	xxxxx
p	k2	yyyyy
P'	k2	yyyyy

그림 3. 부모 노드가 바뀌었을 때의 ACL 테이블 변경
Fig. 3. ACL Table Alteration when parent node changes

1.3 무선 인프라 자체의 취약점

ZigBee 네트워크는 무선 네트워크의 특성인 특정한 주파수를 이용하여 통신을 하고 있다. 만약 공격자가 네트워크가 사용하고 있는 주파수를 알아낸다면 별다른 어려움 없이 네트워크에서 발생하는 트래픽들을 감청할 수 있다. 비록 네트워크의 통신들이 암호화 기법들을 사용한다 하더라도 감청된 트래픽들을 이용해서 네트워크의 토플로지를 알아내거나 보안 메커니즘에서 사용하고 있는 키를 분석해 낼 수 있다.

1.4 네트워크 관리 문제

ZigBee 네트워크는 기본적으로 트리 구조의 토플로지를 형성하고 있다. 각 노드들이 네트워크에 참여하고 탈퇴할 때마다 토플로지가 변경되고 이를 이용한 공격이 발생할 수 있다.

네트워크의 확장성 제한의 문제점을 있으며, ZigBee 네트워크는 코디네이터를 중심으로 한 트리 구조의 토플로지를 이루고 있고, 트리구조의 특성상 각 노드들은 부모 노드와 자식 노드를 가지게 된다. 하지만 원활한 네트워크의 구성을 위해 부모 노드가 가질 수 있는 자식 노드들의 수를 제한하고 있기 때문에 새로운 자식 노드가 네트워크에 참여하거나 노드가 다른 부모 노드의 자식 노드로 위치를 이동하였을 때 부모 노드에서 새로운 자식 노드를 위한 주소 공간을 할당 할 수 없는 문제가 발생한다.

신규노드 추가 정책의 단순함이 있으며, 키 노출 취약점에서 알 수 있듯이 사실상 ZigBee는 접근하는 노드들에 대해 별다른 인증을 하지 않는 단순한 정책을 사용하고 있다. 인증 메커니즘을 사용하지 않고 새로운 노드를 모두 허용함으로써 공격자가 네트워크에 조작된 노드들을 삽입하기가 상당히 유용하며 이 노드들은 조작된 노드이지만 트러스트

센터로부터 정상적인 키를 받았기에 공격자는 조작 노드들을 이용해서 다양한 공격들을 행할 수 있다.

토플로지 노출 가능성이 있으며, 네트워크상에서 전송되고 있는 트래픽들을 감청하여 분석함으로써 네트워크의 대략적인 토플로지를 알아 낼 수 있다. 센서 네트워크에서는 Sink 노드에 가까운 노드들일수록 다루는 트래픽의 양이 많아지기 때문에 각 노드들 주변에서 발생하는 트래픽의 양을 분석함으로써 네트워크의 중요한 노드들의 위치를 파악 할 수 있다. 무선네트워크의 특성상 네트워크에서 발생하는 통신들은 감청당하기 쉽고 이를 악의적으로 이용하여 개인정보의 유출, 보안 시스템의 노출 등의 문제가 발생할 수 있다.

잘못된 정보 삽입 가능성이 있으며, ZigBee 네트워크에서는 각 센서 노드들로부터 수집된 정보를 기반으로 하여 서비스와 관련된 판단을 내리고 있으며 이 경우 센서 노드의 잘못된 행동으로 인해 잘못된 판단을 내릴 수 있다. 예를 들어 어느 공간에 노드가 하나일 경우 그 노드로부터 수집한 정보가 그 곳의 상황에 대한 판단을 좌우한다. 만약 이 노드가 공격자에 의해 오염이 되었다면 Sink 노드는 정상적인 모니터링을 수행할 수 없게 된다. ACK에 대한 인증 부재 문제가 있으며, ZigBee 에서는 노드들이 주고받는 패킷을 비콘 패킷, 제어 패킷, 데이터 패킷, ACK 패킷으로 나눈다. ZigBee 스펙에서는 이 네 가지 타입의 패킷 중 ACK 패킷에 대해서는 어떠한 보안정책도 마련해 놓고 있지 않다. 공격자는 손쉽게 ACK 패킷을 생성할 수 있으며 jamming 공격과 함께 이용해서 전송 노드가 모르게 정상적인 메시지의 전송을 방해할 수 있다[11, 12, 13].

1.5 메시지 보호 문제

무선네트워크의 특성상 네트워크에서 발생하는 통신들은 감청당하기 쉽고 이를 악의적으로 이용하여 개인정보의 유출, 보안 시스템의 노출 등의 문제가 발생할 수 있다.

잘못된 정보 삽입 가능성이 있으며, ZigBee 네트워크에서는 각 센서 노드들로부터 수집된 정보를 기반으로 하여 서비스와 관련된 판단을 내리고 있으며 이 경우 센서 노드의 잘못된 행동으로 인해 잘못된 판단을 내릴 수 있다. 예를 들어 어느 공간에 노드가 하나일 경우 그 노드로부터 수집한 정보가 그 곳의 상황에 대한 판단을 좌우한다. 만약 이 노드가 공격자에 의해 오염이 되었다면 Sink 노드는 정상적인 모니터링을 수행할 수 없게 된다.

ACK에 대한 인증 부재의 문제가 있으며, ZigBee 에서는 노드들이 주고받는 패킷을 비콘 패킷, 제어 패킷, 데이터 패킷, ACK 패킷으로 나눈다. ZigBee 스펙에서는 이 네 가지 타입의 패킷 중 ACK 패킷에 대해서는 어떠한 보안정책도 마련해 놓고 있지 않다. 공격자는 손쉽게 ACK 패킷을 생성할 수 있으며 jamming 공격과 함께 이용해서 전송 노드가 모르게 정상적인 메시지의 전송을 방해할 수 있다.

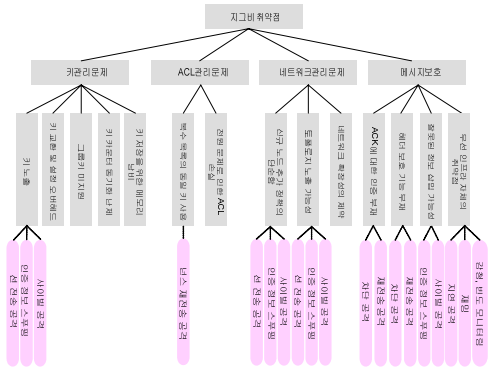

그림 4. ZigBee 취약점과 공격 방법
Fig. 4. ZigBee Vulnerabilites and Attacks

2. ZigBee 홈 네트워크 가상 공격 시나리오

ZigBee 네트워크의 취약점들을 이용해서 다양한 공격들이 일어날 수 있다. 많은 공격 방법들 중에서 네트워크에 치명적인 것들을 선택하여 그 공격들이 실제로 ZigBee 네트워크상에서 어떻게 이루어지는지에 대한 세부적인 시나리오를 작성하였다.

* 사이빌 공격을 이용한 방재 시스템 무력화

t잘못된 센싱 정보의 지속적 전달을 통한 방재 시스템의 판단 오류를 유도하는 시나리오 이며, 이 시나리오의 공격을 통해서 댁내의 침수 등으로 인한 재산 피해를 유도 할 수 있다.

① 가정

▪ 방재 시스템 관련 노드(온도감지, 연기감지)는 1초에 한 번씩 계속해서 온도 또는 연기 정보를 홈 게이트웨이(Home Gateway)로 전송한다.

▪ 방재 시스템의 경우 2개 이상의 노드에서 일정 시간 이상(예:10초) 지속적으로 기준값 이상의 비정상적으로 판단되는 정보가 전송 될 경우 홈 게이트웨이는 화재가 발생한 것으로 판단한다.

② 시나리오

▪ 공격자에 의해 컨트롤 될 수 있는 악의적 노드를 이용하여 창가 등의 노출된 노드를 통해 4개(IDa, IDb, IDc, IDd)의 ID를 차례로 자식 노드로 등록한다. (온도감지 노드 2, 연기감지 노드 2)

▪ 악의적 노드는 정상범위 이상의 비정상적인 온도 정보를 연기정보를 가진 메시지를 IDa, IDb와 IDc, IDd의 이름으로 각각 만들어 일정시간(10초)이상 지속적으로 1초마다 보낸다.

▪ 홈 게이트웨이는 수집된 정보를 바탕으로 2개 이상의 노드에서 정해진 일정시간(10초) 이상 동안 지속적으로 비정상 정보가 오는 것으로 판단 한다.

▪ 스프링클러 또는 소화기 등의 소방 시스템이 작동하고 화재 신고를 하는 등의 조치가 취해진다.

③ 공격 효과

▪ 비정상적인 화재 발생 경보로 인한 불필요한 소화 시스템장치 작동으로 정상적인 주거가 불가능하게 된다.

▪ 스프링클러나 소화기의 작동으로 인한 가정 집기 손상, 침수 등으로 재산 피해가 발생할 수 있다.

표 1. ZigBee 공격 방법 및 방어 기술

공격 방법	본 논문에서 제안한 방어 기술
패킷 스니핑	암호화/키관리
Node Capture	침입 탐지/대응 엔진 기능 구현
Sybil Attack	키 관리/침입 탐지 대응 기능 구현
재밍 공격	Coexistence 회피 기능 구현

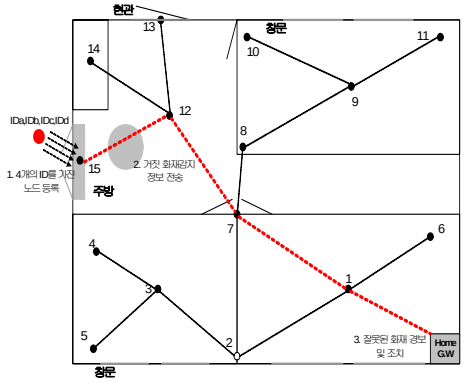

그림 5. 사이빌 공격을 이용한 방재시스템 무력화 시나리오

Fig. 5. Anti-Fire System Attack Scenario by Sybil Attack

Ⅲ. ZigBee 기반 End-to-End 보안 솔루션

본 논문에서는 ZigBee 표준화가 가지는 한계점인 응용어플리케이션에 대한 보안 기능 정의를 하였고, 관련 기능들을 End-to-End 기반으로 구현하였다. ZigBee 디바이스의 특징인 메모리, 프로세서등의 하드웨어적 미약한 자원으로 인한 기존 네트워크 보안 메커니즘을 사용하기가 불가능하다. 이상과 같은 제한적 상황에 맞게 ZigBee 기반 응용 어플리케이션을 위한 End-to-End 보안 기술 개발을 개발하였다. 본 기술의 특징은 ZigBee 디바이스에 비하여 비교적 자원이 풍부한 응용 단말기의 하드웨어적 자원을 활용하여, 보안 관련 컴퓨팅 자원을 소비하였고, ZigBee 디바이스는 보안을 위한 최소한의 자원을 사용하여 ZigBee 디바이스, ZigBee 게이트웨이/코디네이터, ZigBee 응용 단말기와 핸드 세이킹을 이용한 최소한의 보안 데이터 트래픽을 통한 기능 구현을 하였다.

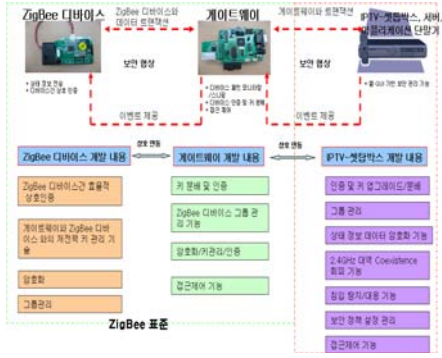

그림 6. ZigBee 기반 End-to-End 보안 기술

Fig. 6. ZigBee (End-to-End Security Solution)

그림 7. ZigBee 기반 End-to-End 보안 기술 구현 화면

Fig. 7. The GUI of ZigBee Security

1. ZigBee 홈 네트워크 보안 기술 개발

1.1 인증 기능

홈 네트워크 제품을 직비 디바이스 사용시에 직비용 디바이스 구입시에 사용자가 제어 할 수 있도록 직비 디바이스 고유의 번호와 홈 서버 단말기에서 인증해 주는 경량화된 직비용 인증 기능을 개발하였다.

1.2 키 업그레이드/분배 기능

키 값 해킹을 방지하기 위한 주기적인 키 값 변경 및 수동으로 키 값 변경 기능 및 그룹 별 키 분배 기능 구현하였다. ZigBee 기술이 가지는 초기 네트워크 설정시에 키 해킹 기능 방지를 위하여 컴퓨팅 자원이 풍부한 응용 단말기에서의 키 관리 기술을 개발하였다.

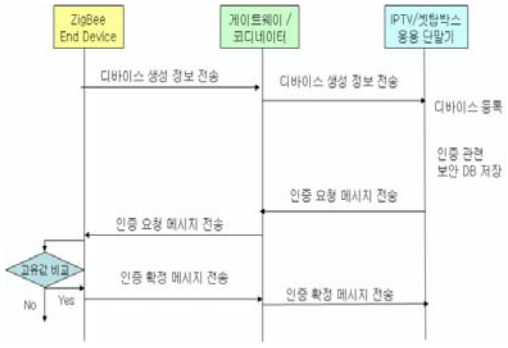

그림 8. ZigBee 디바이스 인증 메커니즘
Fig. 8. Authentication Mechanism of ZigBee Device

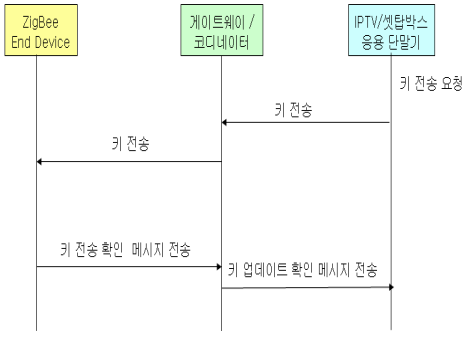

그림 9. ZigBee 키 관리 메커니즘
Fig. 9. Key Management of ZigBee

1.3 그룹 관리

홈 네트워크 직비 디바이스들의 그룹 별 관리를 위한 그룹 관리 기능을 구현하였다.

1.4 상태 정보 암호화 기능

직비 디바이스들의 상태 정보가 주기적으로 단말 플래폼 전송시에 데이터 암호화 기능을 구현하였다.

1.5 2.4GHz 대역 Coexistence 회피 기능

직비 기술은 각 채널당 캐리어 신호를 연속적으로 발생시키게 하면, 무선 재밍 공격이 가능하다. 이 상태에서는 직비 네트워크는 통신이 불가능한 상태가 된다. 본 기술은 재밍 공격을 방어하기 위한 기능 구현을 확장하여 무선랜, 블루투스, 전자오븐 등이 2.4GHz 대역을 사용시에 발생할 수 있는 주파수 대역 충돌 회피 기능 구현하였다. 직비 다바이스 별 각 채널별 채널 상태 정보 전송에 의하여 단말 응용 플랫폼에 설정된 회피 기능에 의한 직비 디바이스 채널 변경 기능 구현하였다.

그림 10. ZigBee Coexistence 회피 기능
Fig. 10. ZigBee Coexistence GUI

1.6 침입 탐지/대응 기능

직비 디바이스의 상태 정보를 데이터베이스화하여 침입 탐지 패턴 검색 엔진에 의하여 침입 탐지 기능을 구현하였다. 침입 탐지 엔진 기능에 의한 탐지된 악의적인 직비 노드 격리 기능 및 키 업그레이드 기능을 구현하였다.

* 테스트 환경: 악성 노드 추적에 관련한 기술은 개발 내용 검증 시나리오 의하여 다음에 절차에 의하

며, 그림 30은 악성 노드 추적을 위한 개발 내용 검증 시나리오에 따른 테스트베드이며, 동 테스트베드에서 악성 노드 추적 표 1을 작성하였다.

표 1. 악성 노드 추적 테스트 환경

노드 수	디바이스용 10개 코디네이터 1개 침투용 노드 1개
침입 방법	침투용 노드에 의한 DoS 및 데이터 위변조
악성 노드 판단 기준	침입 대응 엔진 기술에 의한 악성 노드 추적
시험 횟수	500회 실시
침입 시나리오	㈀. 직비 네트워크 형성할 시에 nlme_network_join시에 패킷 스니핑을 통하여 네트워크 키 값을 해킹 ㈁. 보일러 연동한 직비 디바이스를 스니핑하여 해킹 툴을 이용한 악의적인 노드로 가장하여 Dos 공격 실행 ㈂. 서버의 상태정보 DB에 저장된 침입탐지 엔진에 의하여 침입을 탐지 ㈃. 침입 대응 엔진 기술에 의한 악성 노드를 추적하여 직비 네트워크에서 배제 시킴

* 테스트베드

그림 11. 침입 탐지/대응 테스트베드
Fig. 11. Testbed of ZigBee Intrusion Detection/Action

* 테스팅 결과: 개발 내용 검증 시나리오에 의한 악성 노드 추적 확률은 계산하면 DoS 공격시에 악의적인 노드가 공격을 시도 할 시에 추적 확률은 90% 정확도 기술을 개발하였다.

표 2. 침입 탐지/대응 테스팅 (악성 노드 DoS 공격 10차를 50회 실시하여 평균적으로 10차 중 1회 정도 실패 확률을 가짐)

	성공	실패
악성 노드 DoS 공격 1차	○	
악성 노드 DoS 공격 2차	○	
악성 노드 DoS 공격 3차	○	
악성 노드 DoS 공격 4차	○	
악성 노드 DoS 공격 5차	○	
악성 노드 DoS 공격 6차		○
악성 노드 DoS 공격 7차	○	
악성 노드 DoS 공격 8차	○	
악성 노드 DoS 공격 9차	○	
악성 노드 DoS 공격 10차	○	

1.7 보안 정책 관리 설정 기능

직비 보안 관련 기능들을 단말 응용 플랫폼에서 사용자의 보안 요구 사항 및 특성에 맞게 정책 설정 기능 구현하였다.

1.8 접근 제어 기능

각 사용자의 등급별 직비 디바이스의 제어 권한 차별화 기능, 인증되지 않은 직비 디바이스 사용 금지 기능을 구현하였다.

2. ZigBee 홈 네트워크 공격 시나리오

그림 6과 같이 개발한 내용에 대한 검증을 위한 공격 시나리오를 작성하였고, 침입 탐지/대응 기술을 통하여 본 개발 내용을 검증하였다. 보일러 연동한 직비 보드 패킷 스니핑을 통한 악의적인 노드의 직비 패킷 서버에 데이터 전송시에 서버에서는 상태정보 DB에 저장된 침입탐지/대응 엔진 기술에 따라서 침입을 탐지하여, 키 값 변경을 통한 대응 기술 개발 및 침입 패턴 업그레이드 기능을 구현하였다.

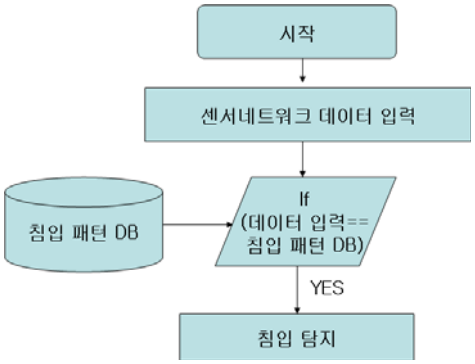

그림 12. 침입 탐지 엔진
Fig. 12. ZigBee Intrusion Detection Engine

IV. 결 론

본 논문에서는 유비쿼터스 홈에서 ZigBee 기술을 사용시에 침해를 최소화 할 수 있는 End-to-End 보안 기술을 개발하였다. 본 기술의 특징은 표준화에서 정의한 디바이스간 보안 기능만 정의되어 있으나, 실제 서비스를 위한 보안 기술은 응용 단말기 단에서 보안 기술도 필요하다. 또한 ZigBee 디바이스의 하드웨어 자원의 빈곤함으로 인한 보안 기능의 구현의 어려움이 있다. 본 논문에서는 End 디바이스가 가지는 하드웨어 자원의 풍부함을 이용한 보안 기술을 구현하였으며, 유비쿼터스 홈 침입 환경 예측 기능, 개별 침입 시뮬레이션 기술, 보안 통신 모듈 기술, 네트워크 서비스 기기용 보안 모듈등을 개발하였다.

참고문헌

[1] A. Perrig, R.Szewczyk, V. Wen, D. Culler, "SPINS: Security Protocol for Sensor Networks," Proc. of the 7th ACM. pp. 342 - 340.

[2] J. Deng, R. Han, and S. Mishra, “"Security Support for In-Network Processing in Wireless Sensor Networks,"" Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN), 2003.

[3] L. Eschenauer and V. Gligor, “A Key - Management Scheme for Distributed Sensor Network,” Proc. of the 9th ACM Conference on Computer and Communications Security, 2002. pp. 124 - 130.

[4] P. Brutch and C. Ko., "Challenges in intrusion detection for wireless ad-hoc networks. In 2003 Symposium on Applications and Internet Workshops, 2003. pp. 125 - 132.

[5] IEEE 802.15.4, Draft Standard: Low Rate Wireless Personal Area Networks, Feb. 2003.

[6] ZigBee Alliance, http://www.zigbee.org. 2006.

[7] ZigBee Network Specification, V 1.0, Dec. 2004.

[8] ZigBee Security Services Specification, V1.0, Dec. 2004.

[9] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Dept. of Commerec/N.I.S.T, Nov. 2001.

[10] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM), "RFC 3610, SPT. 2003.

[11] Jianliang Zheng, Myung J. Lee, Michael Anshel, "Toward Secure Low Rate Wireless Personal Area Networks", IEEE Transactions on Mobile Computing, Vol.5, No.10, OCT. 2006, pp. 203-212,

[12] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Network,"Proc. 2004 ACM Workshop Wireless Security, Oct. 2004, pp. 343-350.

[13] A. Perrig, R. Szewczyk, V.Wen, D.Culler, and J.D.Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless Networks J., Sept. 2002, pp. 123-132.

저 자 소 개

박 우 출
1995년 한양대 전자공학과 학사
1997년 한양대 전자공학과 석사
2002년 한양대 전자공학과 박사
현재 전자부품연구원 선임연구원
관심분야 : 통신 시스템, 센서네트워크
Email : wcpark@keti.re.kr

이 명 수
현재 전자부품연구원 수석연구원

윤 명 현
현재 전자부품연구원 수석연구원

김 성 동
1983년 경북대 전자공학과 학사
1990년 경북대 전자공학과 석사
1996년 Texas A&M Univ 전기전자공학과 박사
현재 전자부품연구원. 유비쿼터스 컴퓨팅 연구센터
센터장.
관심분야 : 센서네트워크, u-city, 무선통신
Email : sdkim@keti.re.kr

양 성 현
1983년 광운대학교 전기공학과 학사
1987년 광운대학교 전기공학 석사
1992년 광운대학교 전기공학 박사
현재 광운대학교 전자공학과 교수