논문 2009-46CI-1-4

# 이웃탐지와 ACL을 이용한 ZigBee 기반의 홈네트워크 보안 시스템 구현

## ( Implementation of the ZigBee-based Homenetwork security system using neighbor detection and ACL )

박 현 문*, 박 수 현**, 서 해 문*

( Hyun-Moon Park, Soo-Hyun Park, and Hae-Moon Seo )

요 약

홈네트워크(Home Network)와 같이 개방된 환경에서 여러 개의 아토셀(Ato-cell)로 구성된 ZigBee 클러스터는 측정 및 수집 정보의 전달에 대한 안전한 보안이 요구된다. 또한 ZigBee 디바이스간 인증을 위해 발생되는 마스터 키 관리 및 Access Control List(ACL), 디바이스 자원 등 여러 가지 보안의 문제점이 논의되고 있다. 선행연구로 부모-자식 간의 해쉬체인 기법(Hash Chain Method)이나 토큰 키( token-key), 공개키(public-key) 인증기법 등이 연구되고 일부는 표준에 반영되었다. 이와 관련하여 본 논문에서는 홈네트워크 ZigBee 구현 시스템에서 디바이스의 복제와 사이빌 공격(Sybil Attack)에 대한 탐지 기법으로 이웃 디바이스 검색을 보안에 적용, 확대하였다. 이웃 검색(neighbor detection)의 응용기법은 주변 디바이스에 대한 정보를 활용하여 새로운 디바이스와 이웃 디바이스의 ACL 정보를 포함 및 비교하여 인증을 한다. 이를 통해 악의적인 디바이스(malicious device)의 사이빌 공격, 디바이스 복제에 대한 침입 탐지 및 해킹 방지를 구현하였다. 또한 홈네트워크 기기를 ITU-T SG17와 ZigBee Pro를 고려하여 사용자 접근 권한, 시간, 날짜, 요일의 4개를 적용하여 레벨과 룰로 구분하여 구현하였다. 결과적으로 볼 때 제안방식이 악성 디바이스의 탐지 성공 및 시간 측면에서 우수한 것으로 나타났다.

Abstract

In an open environment such as Home Network, ZigBee Cluster comprising a plurality of Ato-cells is required to provide intense security over the movement of collected, measured data. Against this setting, various security issues are currently under discussion concerning master key control policies, Access Control List (ACL), and device sources, which all involve authentication between ZigBee devices. A variety of authentication methods including Hash Chain Method, token-key method, and public key infrastructure, have been previously studied, and some of them have been reflected in standard methods. In this context, this paper aims to explore whether a new method for searching for neighboring devices in order to detect device replications and Sybil attacks can be applied and extended to the field of security. The neighbor detection applied method is a method of authentication in which ACL information of new devices and that of neighbor devices are included and compared, using information on peripheral devices. Accordingly, this new method is designed to implement detection of malicious device attacks such as Sybil attacks and device replications as well as prevention of hacking. In addition, in reference to ITU-T SG17 and ZigBee Pro, the home network equipment, configured to classify the labels and rules into four categories including user's access rights, time, date, and day, is implemented. In closing, the results demonstrates that the proposed method performs significantly well compared to other existing methods in detecting malicious devices in terms of success rate and time taken.

**Keywords :** ZigBee Security, ACL, Ato-cell, Homenetwork testbed, Malicious Tempering

* 정회원, 전자부품연구원 (Korean Electronics Technology Institute)
** 종신회원, 국민대학교 비즈니스 IT (Department of Business Information Technology, Kookmin University)
※ "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-C1090-0801-0044)
※ 본 연구는 2008년도 국민대학교 교내연구비 지원을 받아 수행되었음.
※ "본 연구는 한국 과학재단 기초 연구 프로그램의 지원을 받아 수행되었음" (R01-2006-000-10941-0)
접수일자: 2008년12월10일, 수정완료일: 2009년1월12일

## Ⅰ. 서 론

홈네트워크는 월패드 기능와 가전제품 기기의 제어 서비스 형태에서 댁내의 무선네트워크 인프라 기반의 서비스로 변화하고 있다. 그러나 기기간 인터페이스 표준화 작업의 부진과 보안 및 프로토콜 문제로 원격 검침이나 조명제어 등의 단순 홈 오토 수준이며, 홈네트워크에서 주력인 홈서버와 디지털가전을 기반한 엔터테이먼트와 정보 서비스 분야에서의 보안문제에 있어서는 걸음마 단계를 벗어나지 못하고 있다. 홈네트워크는 2007년부터 네트워크와 서비스에서 융합과 연동 두 개의 화두를 가지며 큰 변화가 이루어지고 있다. 무선 통신사업자 중심의 HNB(Home (e) NodeB)와 유선 통신사업자 및 방송 사업자 중심의 IPTV 그리고 댁내에서 무선 고속통신 기술인 IEEE 802.11n이 있다[1~3]. 그 밖에 백색가전과 A/V, 제어기기 등 제어, 생활가전도 '정보가전'의 특징은 융합과 함께 근거리 네트워크와의 연동이 중요하게 떠오르고 있다.

홈네트워크를 3GPP2와 같이 셀 단위로 구분할 때 홈은 하나의 펨토셀(Femto-cell)과 그 안에 여러 개의 아토셀로 구성된다. 홈네트워크 연구에서는 최근 펨토셀 기반의 모뎀들이 적용, 서비스되고 있으며, 2008년 9월 ITU-T SG17에서는 7개 연구과제(Question)를 13개로 확대하면서 USN 미들웨어 및 라우팅 보안이 새롭게 포함되어 2012년까지 활발하게 연구가 진행될 예정이다. 이와 함께 펨토셀 보다 더 작은 단위 영역에 대한 서비스 및 보안 논의가 활발하게 진행되고 있다[1, 3~4, 6]. 특히 이러한 작은 단위의 서비스 영역은 유선에서 무선 중심으로 무선은 WiFi와 ZigBee등 근거리 WPAN으로 변화하고 있으며 HNB에서 예를 들었듯이 외부 무선 통신망과 빠르게 융합하고 있다[2~5]. 여러 종류의 가전 및 생활기기, 멀티미디어 등의 다양한 기기가 통합되고, 기존 홈서버 중심보다는 아토셀 단위의 10m이내 근거리 제어 및 정보가전을 기초하는 무선 네트워크 보안에 주요한 관심이 집중되고 있다. 펨토셀에서 HNB의 서비스 영역을 셀룰러(Cellular)와 IEEE 802.11n의 결합을 위한 홈서비스와 외부망과 연결을 위한 중계기를 포함한다면, 아토셀은 펨토셀과 연동하는 WiFi와 아토셀 안에서 여러 개의 독립적인 WPAN을 구성하는 Bluetooth, ZigBee, UWB 등으로 구분할 수 있다. 홈네트워크 환경에서 ZigBee의 역할은 정보를 수집하고 필요한 정보를 가공하여 사용자에게 실시간으로 정보를 제공하는데 목적이 있다. 아토셀의 중심이 되는 ZigBee는 다수의 디바이스 제어 및 구성에 유리하다는 장점이 있으나 도청 및 서비스 거부 공격으로 키 관리(Key Management), ACL 관리, 메시지 보호, 디바이스 자원 문제 등 여러 가지 형태의 공격에 취약성이 지적되고 이러한 문제 때문에 PNA 그룹에서는 네트워크 모니터링 하는 방안을 고려하고 있다[2, 4]. 본 연구에서는 앞서 언급한 문제점에 대한 논의를 하고 ZigBee에서 사용하는 이웃 검색을 이용하여 해당 디바이스의 ACL에 이웃 디바이스를 추가하는 기법을 통해 악의적인 디바이스에 대한 침입 탐지 및 해킹 방지를 구현하였으며, 사용자의 계층적 접근 방안을 제시하였다. 2장에는 ITU-T SG17에서 논의되고 있는 홈네트워크 모형과 타입(Type)에 따른 ZigBee의 역할 및 구성을 설명한다. 홈 가전에서 새로운 ZigBee 디바이스 인증 및 등록과정을 설명하며, 더불어 키관리(Key-management) 및 ACL, 디바이스 자원 등의 보안 취약성으로 발생되는 문제점과 기존 연구내용을 설명한다. 3장에서는 논의 된 취약성에 대한 시나리오 및 일부 해결책을 설명하고, 계층적(Layer) 기반의 인증시스템에 대한 논의를 통해 ZigBee 디바이스간 사용자 인증 정책에 대한 제안을 한다. 4장에서는 홈네트워크 침입대응을 위한 테스트환경과 테스트 시나리오를 설명하고, 성능결과 분석을 한다. 그리고 마지막장은 결론을 맺는다.

## Ⅱ. 홈네트워크 보안

### 1. 홈네트워크 구성

그림 1은 X.1111과 J.190에서 정의한 홈디바이스 타입과 네트워크 기본 구조에 3GPP2에 HNB를 결합한 것이다. 외부망(External Network)은 PSTN(Public Switching Telephony Network), 인터넷망, 모바일 사용자가 홈네트워크와 연결할 때 인증하도록 하는 공인 CA(Certificate Authority)로 구성되며, 내부망(Internal Network)에서는 접근 네트워크(Home Access, HA)와 홈 게이트웨이와 연결 역할을 하는 HB(Home Bridge), 홈패드나 PC, HC(Home Client), 셋톱박스 등 홈네트워크를 관리하는 디바이스로 구성된다. HG(Home Gateway)는 홈 내부에서 Internal CA를 통해 자체인증(Self-signed Cert)과 댁내장치인증(Home Device Cert)을 지원한다[1~3].

X.1111는 복합 네트워크(Complex Network)에 홈디

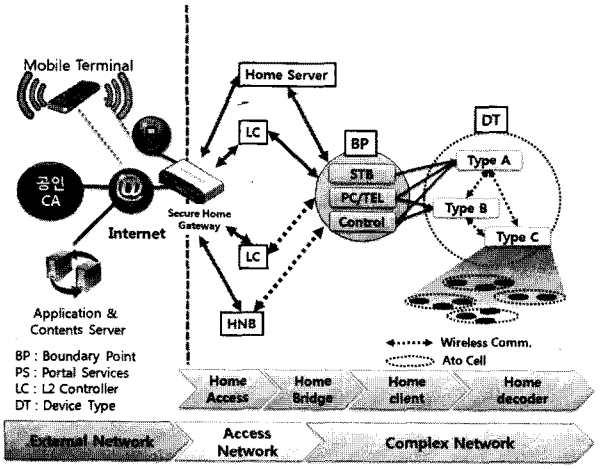



그림 1. 홈네트워크 보안 모델
Fig. 1. Homenetwork model.

바이스를 3가지 타입(Type)으로 구분하고, 홈 기기간의 유연한 통신을 위한 원격터미널과 홈디바이스의 기능을 정의하였다[4, 7, 21]. 타입 A는 컨트롤 디바이스로 홈패드, 컴퓨터 등 사용자 인터페이스가 존재해 사용자가 인증 가능하며, 인증 디바이스를 통해 다른 하위 디바이스도 제어 가능하다. 타입 B는 멀티미디어, A/V 기기 상위 디바이스로 타입 C의 디바이스를 제어하며, 전화, 비대, 전원 콘센트, 수도・전기계량기 등 다른 디바이스와 통신 할 수 없는 기기도 포함된다. 마지막 타입 C는 타입 B가 전달하는 명령에 따라 제어되는 정보가전 디바이스로 이루어진다. ZigBee 스펙을 고려 할 때 많은 기기를 원격 제어하는 모바일 디바이스와 전원 콘센트, 보일러, 냉장고 등에 사용 가능한 End 디바이스로 B, C 타입이 대부분을 이루게 된다[9~11]. ZigBee로 구성된 디바이스는 특성과 공간에 따라 아토셀 단위의 별도 클러스터를 구성하여 해당 영역에 디바이스의 인증 및 수행 정보를 등록하게 된다.

## 2. 홈네트워크 구성

### 가. 디바이스 인증 및 절차

그림 2는 ZigBee Pro와 SG9, 17에서 논의된 홈네트워크 보안에서 구축된 홈디바이스 환경에 새로운 디바이스의 인증 및 보안의 문제점을 1), 2), 3)으로 설명하였다. 코디네이터(PAN Coordinator, PAC)는 [12]에서 Trust Center라고 지칭되며, 분배키, 마스터키 등을 클러스터의 End-End 디바이스들에게 할당해주는 역할을 한다. 그 밖에 네트워크키와 링크키를 이용하여 디바이스레벨과 네트워크레벨로 구분하여 전송할 수 있다.

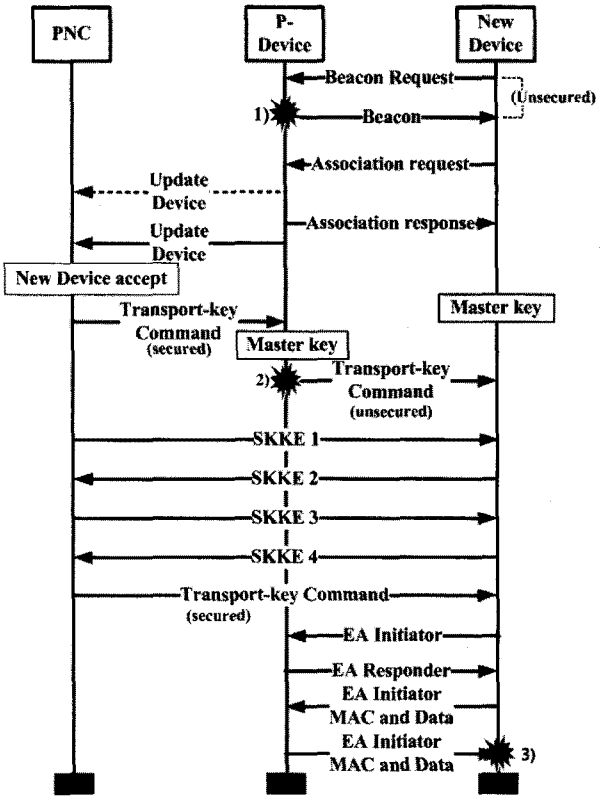



그림 2. 디바이스 인증 및 절차 문제점
Fig. 2. Device authentication and Process Problem.

1) 기존 클러스터에 접속 정보를 요구하는 새로운 단말은 ZigBee 코디네이터나 게이트웨이(GW)에 질의를 한다. GW는 HS(Home Server)에 미리 등록된 DB의 채널 정보를 요청하거나 해당 클러스터의 코디네이터에게 채널 모니터링을 요청하고 각 채널에 대한 정보를 수집한다. 검색된 정보는 코디네이터를 통하여 DB에 저장 되고, 최소셀로 구성된 여러 클러스터 각각의 디바이스 채널 상태를 종합적으로 분석하여 각 셀에 대한 최적화된 채널을 선택하게 된다. 채널 선택은 각 아토셀 영역에 구성되어 있는 Bluetooth, WiFi 등 다양한 무선통신에 의한 신호 간섭에 공존성(Coexistence) 문제을 최소화하기 위해 RSSI와 CCA로 기반 한다.

2) 채널 정보를 습득한 새로운 디바이스는 코디네이터에게 승인(New Device accept) 받아 상위 디바이스로부터 마스터키를 수신할 수 있다. 하지만, 새로 접속된 디바이스는 구성된 네트워크와는 어떠한 보안 메커니즘도 없기 때문에 마스터키를 평문 형태로 수신할 수 밖에 없는 문제를 가진다. 2)에서와 같이 인증 값을 생성하기 위해 새로운 디바이스는 인증에 필요한 인자를 구하고, 이 인자는 해쉬 알고리즘을 이용하여 인자 Q 값을 얻는다. 이 때 보다 작은 범위의 소수(k)와 랜덤

넘버 2개를 생성하고 인증 값에 대한 소수(k) 및 2개의 랜덤 넘버를 클러스터 맴버인 ZigBee의 디바이스 및 코디네이터에 전송한다[6, 11~12]. 코디네이터에서 생성된 고유의 검증 값 및 링크키(Link-key)를 비교하여 일치 할 경우 인증메시지를 새로운 디바이스에게 보낸다. 만약 새로운 디바이스가 제어 장치일 경우 코디네이터로부터 클러스터 영역에 속해 있는 End 디바이스에 대한 제어 권한을 갖게 된다. 인증 및 키 업그레이드를 위해 코디네이터의 고유 데이터 값과 인증 데이터를 동일하게 한다. 이와 같은 과정에서 평문 마스터키를 스누핑(snooping)하여 링크키 복제뿐 만 아니라, 코디네이터로 복제 해킹 할 수 있다.

3) 2)에서 얻은 마스터키로 기존의 클러스터를 구성하는 멤버 디바이스는 3) 영역에서 암호화된 프레임 데이터(Frame Data)를 XOR 함으로써 마스터키의 해킹을 통한 악의적인 디바이스는 코디네이터로 가장하고, 거짓 비콘 메시지로 디바이스간 통신에 악영향을 줄 수 있다. 또한 키 카운터 정보를 임의적으로 조작하여 전송할 수 있기 때문에 클러스터에 속한 멤버 디바이스들은 보관하고 있는 키 카운터를 잘못된 값으로 갱신하거나 수신 할 수 있다. 이렇게 복제된 해킹 디바이스는 클러스터 내의 디바이스들이 주고받는 비콘, 제어, 데이터, 응답(ACK)패킷을 알 수 있기 때문에 전체 디바이스에 대한 재밍공격을 통해 다른 디바이스간의 메시지 교환을 방해 할 수 있다.

홈가전의 디바이스는 작은 단위 영역으로 구성되기 때문에 ZigBee 디바이스는 다른 셀로 이동해 참여하는 과정에서 키 교환을 통한 클러스터 맴버 디바이스에 악의적 이동을 유도함으로써 End 디바이스에 대한 서비스 거부 공격이 가능하다. 이때 여러 개의 ID를 획득하여 그림 3에 $N_6$, $N_7$과 같이 코디네이터에 대한 사이빌 공격이 이루어질 수 있다.

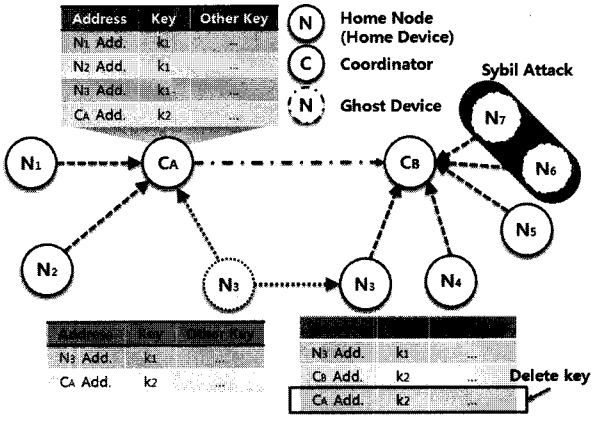



그림 3. 이동 디바이스로 인한 ACL 에러문제
Fig. 3. Mobile Device for ACL error Problem.

그림 3과 같이 ACL에는 디바이스들의 주소와 마스터키를 지닌다. ACL에는 클러스터를 변별하는 키가 없기 때문에 각 클러스터에는 각기 다른 키를 할당하여 구분한다. 클러스터의 디바이스들은 코디네이터와 키를 공유하기 때문에, 서로 다른 디바이스들이 전송되는 도착 메시지를 감청하고, 사용하는 마스터키를 감청메시지에 XOR 함으로써 넌스(Nonce)값을 알 수 있다. 그 밖에도 아토셀 간의 ZigBee 디바이스 이동은 ACL key에 대한 중복 문제가 발생가능하다. 새롭게 연결된 클러스터의 코디네이터를 추가 등록(Entry)하고 기존 부모의 등록 정보를 이동 디바이스의 ACL에서 삭제한다. $N_3$와 같이 이동 디바이스 ACL는 잠시동안 $C_A$ Key를 지니고 $C_B$ 클러스터에 접속요청 하면서 동일한 키를 지니게 된다. 새로운 $C_B$는 ACL에러로 인한 악의적 공격자로 오인하거나 ACL 중복으로 손실이 발생할 수 있다.

그 밖에도 디바이스의 자원 한계로 발생하는 ACL 중복 및 링크, 마스터, 네트워크키 유지, 프로세서 자원 문제 등이 존재하지만 본 연구 제안과는 연관성이 적음으로 논의하지 않는다.

### 나. 악의적 공격에 대한 연구

앞 장에서 악의적인 디바이스의 여러 형태의 해킹을 해결하기 위해 많은 연구가 이루어지고 있다. 그림 2는 1) 같이 악의적인 디바이스가 해당 클러스터에 채널을 스캔하여 재밍공격을 할 경우, 코디네이터는 다른 채널 상태를 파악하여 클러스터 디바이스들에게 채널 변경을 요청(Broadcasting)한다[12, 20].

마스터키에 대한 보안 방법으로 해쉬 체인을 이용해 보안채널(Secured Channel)을 생성한 후 마스터키를 전송해주는 기법과 부모 디바이스와 자식 디바이스 사이에 네트워크키를 전송하는 알고리즘이 있다[12, 21]. 이 기법은 초기 해쉬로 생성된 키 값을 부모, 자식 모두 가지고 있어야 한다는 문제가 있다. 그 밖에, 기존의 엠버 EM260에서 지원하는 16bytes 토큰 저장 키 기법(re-shared EZSP)으로 코디네이터와 참여 디바이스들의 이웃 디바이스에 대한 링크키 재분배를 통해 마스터키를 보호하는 방법이 제시되어 있으며, ZigBee Pro R16/R17 표준을 지원한다[13~15, 17].

디바이스의 복제와 사이빌 공격에 대한 탐지기법을

두 가지로 나눌 수 있다. 코디네이터에서 주기적으로 메시지를 전파하여 설정된 시간 내에 응답이 있는지를 확인하여 탐지하는 방안[12, 14]과 클러스터의 코디네이터는 클러스터 암호키를 클러스터 자신의 모든 디바이스에게 별도의 새로운 키를 1:1로 분배하는 방법으로 별도의 공유키를 추가하는 방법이다[16, 18, 20]. 각 디바이스들은 자신의 주변에 있는 이웃 디바이스의 키를 수집하고, 코디네이터는 자신의 등록키와 클러스터 디바이스의 등록된 랜덤 키를 통해, 타임스탬프와 넌스를 n번 암호화하여 브로드케스팅 메시지를 보낸다. 클러스터의 멤버 디바이스는 수신 메시지를 n번 복호화하여 코디네이터의 등록키를 확인하고 자신키와 램덤키를 암호화된 메시지에 포함하여 코디네이터에게 보낸다. 이 때 악의적인 디바이스는 자신이 가지고 있는 ID Address 등에 대해 모두 암복화 해서 보내거나 아니면 응답을 할 수가 없게 된다. 해당 ID Address를 암호화 한다고 하여도, 코디네이터가 할당해 준 타임스탬프 이내에 응답이 어려울 뿐만 아니라 타임스탬프 이후에 응답을 하여도 코디네이터가 할당해 준 시간 내에 응답을 한 것이 아니기 때문에 버리(discard)게 된다. 그밖에도 SKKE(Symmetic Key Key Establishment)에 고정된 마스터키를 보안하는 방법으로 공개키(Public Key)기반의 상호인증 및 보안 알고리즘으로 설정한 키와 Trust 데이터를 주기적으로 업데이트하는 기법이다[16, 18]. 네트워크 복잡도 면에서 크게 증가되거나 별도의 키를 사용하여 디바이스 호환성에 문제 및 디바이스 자원의 고려가 없었다.

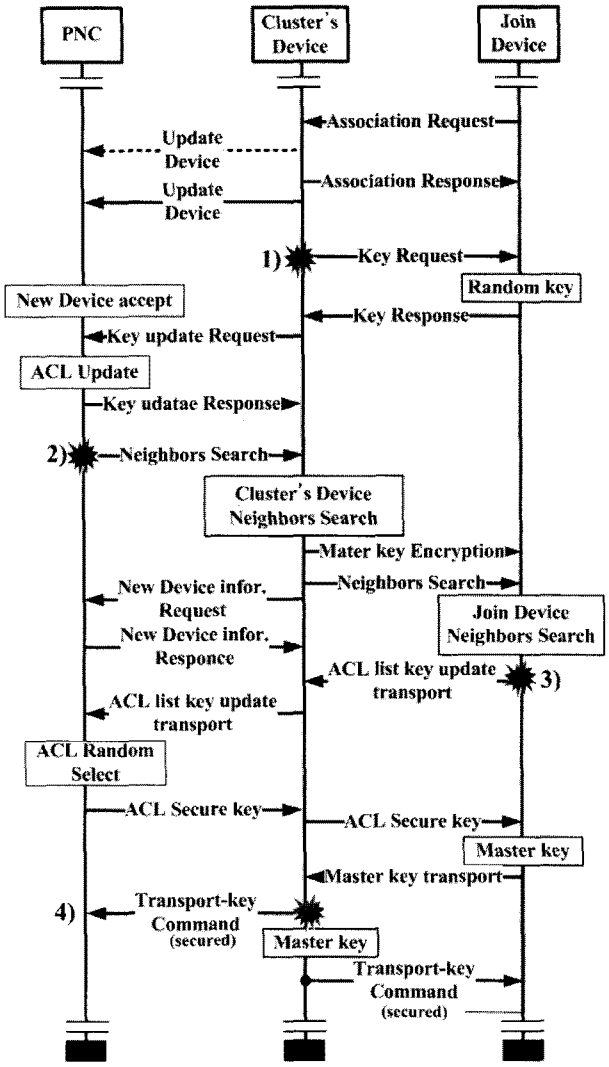



그림 4. 이웃 디바이스를 이용한 접근방지기법
Fig. 4. Neighbor device detection using Intrusion Prevention Scheme.

## Ⅲ. 제안 기법

### 1. 홈네트워크 구성

#### 가. 이웃 디바이스 기반 ACL 접근방지기법

테스트 베드는 ZigBee에서 이웃 검색과 디바이스 ACL에 검색된 이웃 디바이스의 정보를 등록하는 기법으로 악의적인 디바이스에 대한 침입 탐지 및 해킹 방지를 구현하였다. 이웃 검색과 ACL을 이용하여 마스터키 공개 및 링크키의 복제 방지를 목적한다. 악의적인 디바이스가 가상 디바이스를 생성하여 코디네이터에 잘못된 정보를 보내는 사이빌 공격을 예방한다. 그림 4는 이웃 디바이스를 이용한 제안된 기법을 나타낸 것이다. 그림에서 비콘(Beacon)에서 인증과정까지의 자세한 연결명령(Association command)은 생략되었다. PNC와 상위 디바이스(Cluster's Device)는 보안에 무결하다.

1) 상위 디바이스는 클러스터에 접속하는 새로운 디바이스(Join Device)에게 주소와 임의의 난수키(Random key, h)를 요청한다. 새로운 디바이스는 난수키(h)를 생성하고 상위 디바이스에게 전송(Key Response)한다. 상위 디바이스는 PNC에게 새로운 디바이스의 난수키(h)와 주소 정보를 전송한다.

2) 새로운 디바이스와 상위 디바이스로부터 1)의 메시지를 수신한 코디네이터는 새로운 디바이스에 이웃 검색을 요구한다. 새로운 디바이스는 수집된 암호화된 마스터키(Mater key Encryption)를 기반으로 이웃 디바이스 탐색을 시작한다. 이때, 새로운 디바이스는 마스터키가 암호화되어 있기 때문에 복호화 할 수 없다. 이웃

디바이스는 바로 상위 연결 디바이스도 가능하다. 새로운 디바이스로부터 받은 암호화된 마스터키를 이웃 디바이스들은 코디네이터로부터 약속된 해쉬 값으로 복호화하고, 이웃 디바이스들은 코디네이터로부터 새로운 디바이스의 정보를 요청(New Device infor. Request)한다. 코디네이터는 새로운 디바이스의 키(h) 정보와 주소, 마스터키, 새로운 디바이스의 이웃 디바이스 ACL에서 특정 디바이스를 선택하여, 해쉬 체인으로 암호화하여 송신(New Device infor. Response)한다. 이웃 디바이스들은 초기 코디네이터로부터 약속된 해쉬값으로 복호화를 한다. 이를 통해 새로운 디바이스로부터 받은 마스터키 및 난수키(h), 새로운 디바이스의 MAC 주소를 코디네이터로부터 수신 키들과 비교할 수 있다.

코디네이터로부터 수신된 여러키 중 코디네이터의 ACL에서 추출한 새로운 디바이스의 여러 이웃 디바이스 ACL 중에 하나를 램덤하게 선택한 이웃 디바이스 주소를 포함하고 있다. 이웃 디바이스들도 이웃 검색을 통해 이웃 디바이스들의 ACL 값을 지니고 있기 때문에 코디네이터에서 임의로 선택된 ACL 값과 비교할 수 있다. 코디네이터로 받은 메시지를 디바이스들은 그 메시지를 n번 복호화하여 메시지를 확인하면, 그에 따른 응답 메시지를 이웃 디바이스에게 전송한다. 이에 따라 이웃 디바이스가 공유한 키($replay, E_k[N, \times tamp, nonce]$)를 한번만 암호화($replay, E_k[N, \times tamp, nonce+1]$)한다.

3) 새로운 디바이스에서 만들어진 ACL list key update와 비교하며, 이웃 탐색결과와 비교해서 무결하다면, 상위 디바이스는 갱신된 ACL list key update를 만들어 PNC에 보낸다. PNC는 자신에 속한 모든 디바이스 정보는 ACL에 등록되어 있는 상태이다. 그렇기 때문에 ACL의 등록정보와 비교하여 무결성을 확인한다. PNC는 새로운 디바이스에 이웃 ACL과 새로운 디바이스가 초기에 송신한 난수키(h), 마스터키를 XOR해서 ACL Secure key로 만들어 전송한다. 새로운 디바이스는 난수키(h), 이웃 ACL을 복호화하여 마스터키를 획득한다.

4) 상위 디바이스는 새로운 디바이스로부터 마스터키를 수신한다. 이것이 무결하다면, 마스터키를 새로운 디바이스와 해쉬 체인을 사용하여 암호화된 마스터키를 새로운 디바이스의 상위 디바이스에게 전송한다. 이 과정이 끝나면 코디네이터와 새로운 디바이스는 동일한 키를 공유하고 안전한 관계(Secure Relationship)를 맺게 된다. 이를 통하여 새로운 디바이스와 이웃 디바이스 간의 채널과 링크키를 안전하게 공유할 수 있고, 상대의 특정키를 실제로 지녔는지(key confirmation)를 알 수 있다.

초기 해쉬값을 통한 암·복호화로 동일한 암호키 생성이 확인가능하다. 이웃 디바이스들 중 상위 디바이스는 코디네이터로부터 약속된 해쉬값을 새로운 디바이스에게 송신한다. 수신한 새로운 디바이스는 해쉬값을 통해 본인이 지니고 있는 마스터키 및 램덤 이웃 디바이스ACL로부터 얻어진 값을 복호화 한다. 이후에는 SKKE를 통한 통신이 이루어지며, 기존의 방식과 다른 것이 있다면 $HMAC = MAC_{key}(MACData)$의 생성에 포함되는 $MACData = Oct \| U \| V \| QEV \| QEU \| [Text]$의 값 중 이웃 디바이스의 MAC 주소를 이용한 k개 키를 확보한다. k를 선별 할 때에 ACL에 등록되어 있는 이웃 디바이스의 MAC을 카운터 값과 함께 Random 함수를 통해 k를 임의적으로 추출한다. 이 임의로 추출한 k는 MACkey의 Text영역에 포함한다. Text는 새로운 디바이스가 여러 개의 이웃 디바이스 주소 중 임의의 하나를 선택한 이웃 주소(Neighbors Address)이며 64bit를 가진다.

본 제안에서는 코디네이터가 새로운 디바이스의 이웃검색을 통해 k개 키를 확보할 수 있는 이점을 지닌다. 이웃 디바이스 검색을 통한 ACL 비교로 새로운 디바이스의 무결성을 입증할 수가 있다. 또한 임의의 키를 별도로 생성할 필요 없이 ACL 값을 이용하기 때문에 별도의 처리절차가 필요 없다. k를 선별 할 때에 ACL에 등록되어 있는 이웃 디바이스의 MAC을 카운터 값과 함께 Random 함수를 통해 k를 임의적으로 추출한다. 이후 타임스탬프(time stamp)와 넌스를 n번 암호화한 것을 메시지에 포함한다. 또한 새로운 디바이스에게 오픈된 마스터키를 전달하지 않는 방안도 될 수 있다. 이를 통해 마스터키의 유출로 인한 디바이스 복제 방지를 할 수 있으며, 사이빌 공격에서도 이웃 디바이스에 대한 여러개의 키(k)를 알 수 없기 때문에 코디네이터가 할당해 준 타임스탬프 이내에 응답이 어려울 뿐만 아니라 타임스탬프 이후에 응답을 하여도 코디네이터가 할당해 준 시간 내에 응답을 한 것이 아니기 때문에 버리(discard)게 된다.

### 나. 계층적 레벨 기법

사용자와 홈네트워크를 구성하는 기기간의 사용자 레벨의 구성은 ZigBee에서는 [11], [14]와 같이 서비스와 클러스터의 크기에 따라서 구분되고 있으며, 본 구

현에서는 디바이스를 [11], [12]의 표준안과 [3], [5]를 참고하여 홈네트워크 기기를 용도에 따른 2가지 Type으로 정의하여 사용자 권한을 부여하였다. 복합적으로 사용자에게 장치별 접근 권한을 할당하는 DAC (Discretionary Access Control) 방식과 사용자 디바이스의 레벨을 두어 그 레벨에 적합한 장치별 권한을 할당하는 MAC(Mandatory Access Control) 방식이며 DAC는 주로 식별자(ID)를 통해서 홈네트워크에 접근한다. 접근 제어는 네트워크에서 객체에 따라 임의적으로 사용자가 주게 된다. 이러한 접근 제어 정책은 접근 그룹 별, 디바이스 별로 설정이 가능하며 ID를 통해 구분되므로 접근 허가를 결정하는데 있어서 데이터의 큰 의미가 없다. 만약 악의적인 의도로 ID를 복제해서 접근을 한다면 DAC는 이러한 사용을 감지할 방법이 없으며, 이를 방어 할 방법도 없는 통제 불능의 상태로 빠진다. 이러한 문제를 해결하기 위해 MAC 방식을 사용한다. MAC 방식은 사용자 개별적으로 객체 디바이스에 비밀등급(classification level)으로 정의하여 구성 디바이스 특성에 따라서 결합하고, 사용자에게 허가등급(clearance level)을 부여한다. 각각의 사용자가 각 홈네트워크 가전에 접근할 때마다 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 사용자에게만 접근 권한을 부여하는 강제적인 보안정책이다. 이 방법은 보안 및 접근성에 강하다는 장점이 있지만, 효용성에서 문제를 가진다. 본 구현에서는 이러한 문제 때문에 두 개를 복합하여 홈네트워크를 구성하는 디바이스를 사용형태나 접근사항에 따라서 그림 5와 같이 레벨과 룰로 구분하였다. 그리고 2개의 레벨을 시나리오에 따른 사용자 접근 권한, 시간, 날짜, 요일의 4개를 사용자 룰로 구분하였으며, 이러한 방법은 보안요구사항을 만족하기 위해 필요로 하는 보안기능들을 기기 디바이스에 따라 Y(해당 보안기능을 반드시 적용), K(표시된 보안 기능으로 강화), X(선택적 보안기능 추가) 등으로 구분하여 제공하였다.

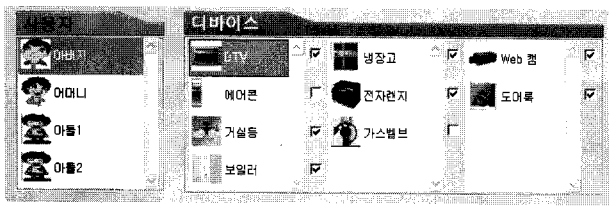



그림 5. 계층적 관리 시스템
Fig. 5. Hierarchical Management System.

## Ⅳ. 테스트 베드 환경 및 구성

### 1. 테스트 환경 구성

구현된 홈네트워크 시스템에 ZigBee 디바이스는 ATmega128L을 사용하고 있으며, 15개의 가전기기에 장착된 디바이스에서 Tree기반 구조를 통해 코디네이터에 전송을 하고 있다. 그렇기 때문에 전송주기도 가전기기의 특성에 따라 규칙·불규칙할 뿐만 아니라 전송기기 특성에 따라서 사용되는 데이터 프레임의 길이도 틀리다. 때문에, 동시에 많은 디바이스가 버스트(bust) 데이터를 코디네이터로 전송 할 경우 4k라는 매우 작은 공간 제약에서 메모리를 효율적으로 관리해야 하는 문제를 가진다. 코디네이터 4k 메모리 영역에 다른 계층(layer)에서 사용되는 전역변수영역과 스택(Stack)일부를 제외하고 나면 2k 정도 영역이 사용가능하다.

그림 6과 같이 ZigBee 기반의 본 시스템은 크게 4개의 영역으로, ZigBee 디바이스 가전기기 모듈과 시스템

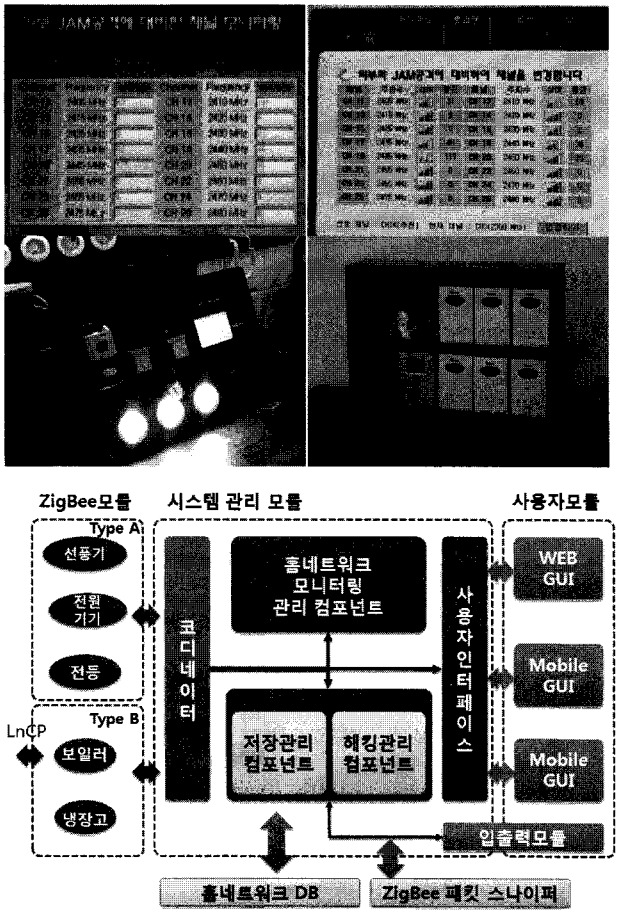



그림 6. 테스트 환경 및 구조
Fig. 6. Homentwork Test-bed and architecture.

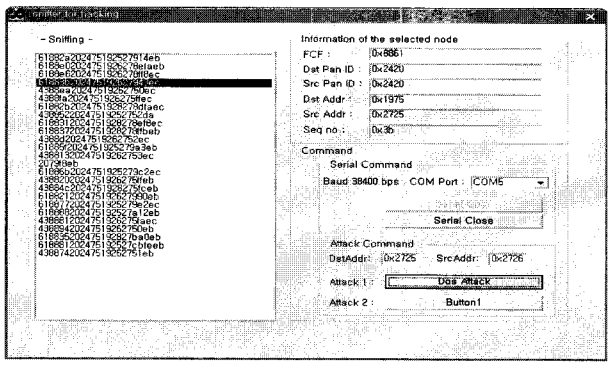



그림 7. ZigBee 해킹 툴 및 패킷 스니퍼
Fig. 7. ZigBee Hacking tool and Packet Sniffer.

관리 모듈 그리고 사용자 모듈, 외부 관리 지원 모듈로 구성되어 있다. 본 시스템에서 ZigBee 기반의 가전기기는 3장 2절에 따라 Type A와 Type B로 구분되어 있다. Type A는 사용자의 사용빈도가 무작위인 가전기기로 선풍기 및 전원을 제어 및 모니터링하기 위한 디바이스, 몇 개의 전등 제어 디바이스로 구성되어 있다. 그리고 Type B는 일정한 모니터링의 주기를 갖는 보일러 및 냉장고 등의 제어장치로 나뉜다. 또한 시스템 관리 모듈에서는 코디네이터와 이와 연결된 모니터링 관리 컴포넌트로 구성 되며, 외부 DB의 저장 및 사용자 입출력을 처리한다.

ZigBee 패킷 스니퍼는 현재 RF 상에서의 각 디바이스들의 패킷 이상 유·무 및 시간, 코디네이터 전송주기 등을 확인하며, 디바이스들이 정해진 시간에 일정하게 동작을 하는지를 모니터링을 하는 역할을 한다. 이를 통해 외부의 악의적인 공격 및 알림 역할까지도 이루어지지만, 본 논문의 연구영역에 적합하지 않기 때문에 ZigBee 패킷 스니퍼 영역은 모니터링으로 한정된다. 마지막으로 사용자 모듈은 다양한 정보를 각 플랫폼별 GUI에 따라 출력모형으로 나타낸다. 본 시스템에서는 앞서 설명한 것과 같이 Type A와 Type B는 동일 채널로 코디네이터에 접속을 하고 있지만 가전기기의 역할에 따라 다르다.

## 2. 테스트 시나리오

그림 8과 같은 네트워크 구조를 이루고 있으며, 코디네이터와 디바이스 그리고 악의적인 디바이스로 구성되어 있다.

### 가. 시나리오

#### (1) 가정 시나리오

패킷 스니핑을 통한 패킷 포맷을 알 수 있으며, 디바이스 캡쳐나 스니핑을 통한 네트워크키 및 마스터키의 획득이 가능하다. 또한 획득한 마스터키로 코디네이터에 등록할 수 있으며, Type B의 디바이스들은 이동하지 않는다.

#### (2) 공격 시나리오

첫 번째 시나리오는, ZigBee 클러스터를 구성하는 네트워크 중의 $N_{21}$번 디바이스가 감염되거나, 또는 악의적인 디바이스가 정상적으로 진입해 있다고 가정하며, 네트워크상의 디바이스들은 측정한 온도 및 전원 상태를 코디네이터 및 게이트웨이에게 전송한다. 악의적인 디바이스가 정상적인 디바이스의 정보를 가로 채거나 실제 존재 하지 않는 디바이스로 정의하여 코디네이터에게 접근 메시지를 송신하고 네트워크 진입을 요청한다.

두 번째 시나리오는, 악의적인 디바이스가 마스터키를 획득 했다고 가정할 때, 코디네이터는 정상적인 디바이스라고 판단함으로 ACL 리스트에 정상적인 디바이스로 등록한다.

악의적인 디바이스가 네트워크 공격을 위해 등록된 다수의 가상 디바이스를 생성하여, 수집정보와 다른 정보의 메시지를 코디네이터나 상위 디바이스에게 보낸다. 홈 디바이스들의 송수신 정보 상태를 그림 9와 같이 이상무(Normal)라 가정할 때, 홈 코디네이터와 게이트웨이는 그림 10과 같이 악의적인 디바이스로부터 다수의 정보를 바탕으로 화재 및 가스 누출 정보를 수신

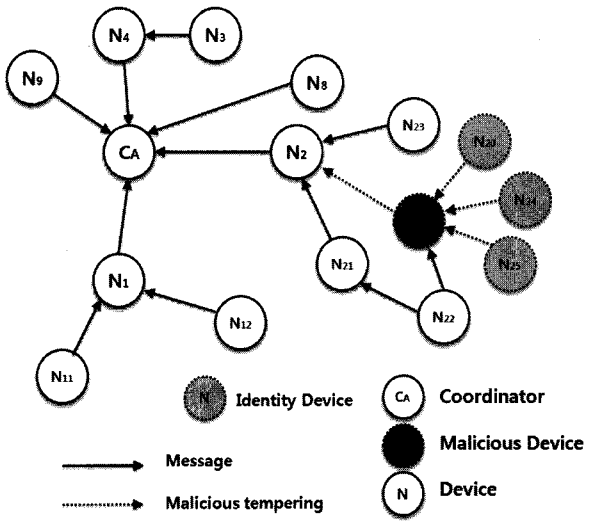



그림 8. 시나리오 네트워크 모형
Fig. 8. Network model of scenario.

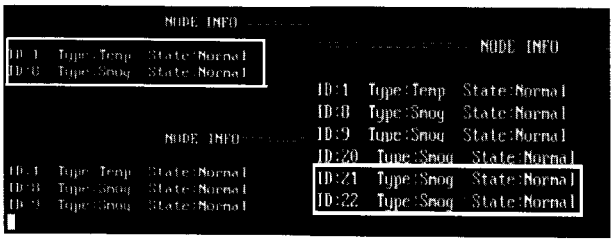



그림 9. 정상적인 네트워크와 악의적인 디바이스의 침입

Fig. 9. Normality Network and malicious device invasion.

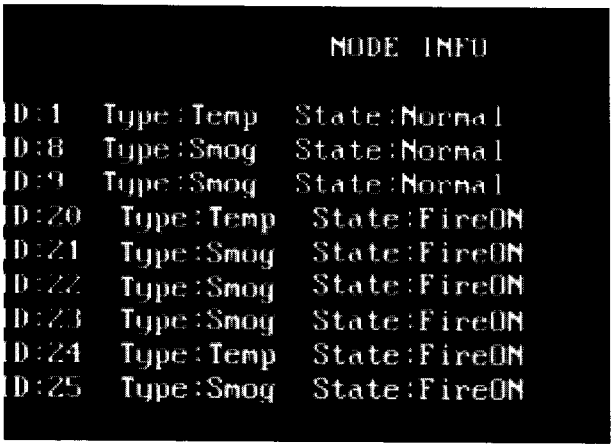



그림 10. 악의적 홈 디바이스로 인한 화재 발생

Fig. 10. Malicious Home device of fire incidents.

받아 오인하게 된다.

그림 9은 시나리오에 따라서 정상 상태(좌)에서 악의적인 디바이스가 침입한 상황을 알려주고 있으며, 악의적인 디바이스가 정보를 보내는 과정을 그림 9의 (우)에서 볼 수 있다. 그림 10은 악의적인 디바이스가 $N_{21}$을 복제하여 잘못된 정보를 코디네이터에 전송하는 동시에 쓰레기 디바이스(Identity Device)를 가상으로 생성하여 잘못된 정보를 코디네이터에 전송하여 전체적인 네트워크에 잘못된 정보를 알려주는 것이다.

### 3. 성능비교

이웃 디바이스를 이용한 침입 탐지 시간과 홉에 따른 키연결 시간에 대해 비교하였다. 침입탐지는 [11], [12]에서 규정한 High/Normal Security Mode일 때의 침입 상태와 제안한 방법에 대한 시간을 패킷 스니퍼를 통해 살펴보았다.

해킹이 성공했을 때 악의적인 디바이스에 대한 탐지 시간을 그림 11로 나타내었다. 그림 11에서 본인이 제안한 방식과 ZigBee R15*와 평균적으로 비교했을 때

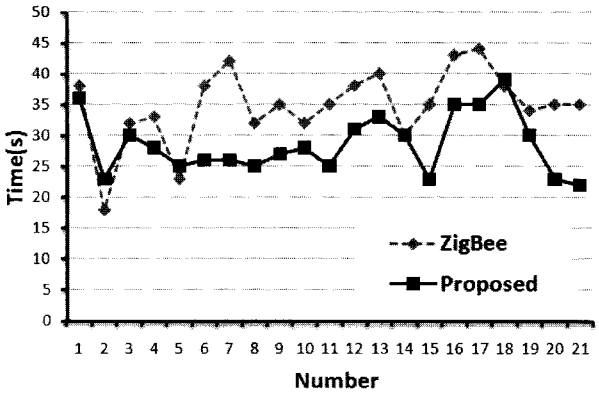



그림 11. 악성 디바이스 탐지 시간

Fig. 11. Mmalicious Home device detection time.

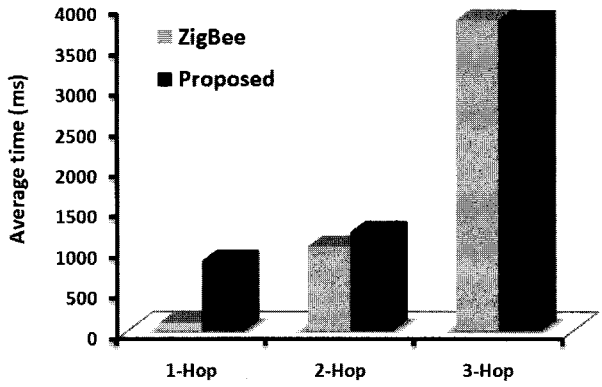



그림 12. 홉에 따른 키 수신 시간

Fig. 12. Key received time of Hop count.

약 21%정도로 악의적 디바이스에 대한 침입탐지 성능이 우월하다. 이는 제안한 방식이 이웃 디바이스 기반의 탐지기법을 통해 찾기 때문에 코디네이터가 할당해 준 타임스탬프 내에 모든 이웃키를 복호화하여 응답이 어려울 뿐만 아니라 타임스탬프 이후에 응답을 하여도 해킹이라 판단되기 때문이다. 제안된 방식이 악의적 디바이스 탐지에 매우 유용하다. 뿐만 아니라 침입 탐지 테스트에서도 총 10번의 해킹 탐지를 5번을 반복하여 시도하였을 때, 악의적인 디바이스의 탐지 횟수는 평균 9번이며, 1번의 실패를 하였다. 즉 총 50번의 탐지에서 4번의 실패를 하였고, 46번을 탐지 성공하였다. 그러나 ZigBee R15에서 50회의 악의적 디바이스 탐지 중 34회만 성공하였고, 16회 실패를 하였다. 즉 악의적 디바이스에 대한 탐지결과는 제안한 방식이 훨씬 높은 것으로 나타났다.

클러스터를 구성한 디바이스들이 그림 8과 같은 구조를 가지고 1홉과 2홉, 3홉일 때 코디네이터에게 네트

* 테스트 펌웨어는 ZigBee R15로 실행되었음

워크 키 및 새로운 디바이스에 대한 링크키를 수신하는 시간을 비교하였다. 1홉에서는 제안 방식이 기존 방식보다 나쁜 성능 결과를 보였지만, 홉 수가 증가할수록 제안한 방식이 기존방식과 비슷한 결과를 보여주었다. 홉 수가 증가할수록 이웃 기반 인증 방식이 기존 방식보다 영향이 적다는 것을 알 수 있다.

## Ⅳ. 결 론

본 연구는 실제 테스트 베드를 통해 악의적인 디바이스에 대한 침입 탐지를 방안으로 이웃 디바이스 정보를 각 디바이스의 ACL에 포함하고 이를 등록, 선택하는 기법을 통해 악의적인 디바이스에 대한 침입 탐지 및 해킹 방지를 구현하였다. 제안 방식은 기존의 ACL과 이웃검색을 혼합한 인증기법으로 네트워크 복잡도 면에서 일부 증가하지만 디바이스간 호환을 높일 수 있으며 표준에서 정의된 프로세스를 이용하기 때문에 쉽게 적용이 가능하다. 또한 디바이스 정보를 이용하기 때문에 별도의 프로세서 처리가 요구되지 않는 장점을 가지고 있다. 다만 제안방식이 보안 복잡도에서 높기 때문에 Computation time이 증가하는 문제점을 지니고 있다. 현재는 위치기반으로 디바이스의 인증 및 보안과정에 대한 복잡도를 낮추는 기법을 연구하고 있다. 홈디바이스의 인증·인가 기술이 활발하게 연구된다면 사용자는 여러 개의 다양한 디바이스에 대한 안전한 홈서비스를 제공받는 것이 가능해질 것이다.

## 참 고 문 헌


[1] 김태근, 박재형, "홈네트워크 기반의 차세대 통방융합 서비스 : UTV(Ubiquitous TV)," 한국통신학회. 제 23권 ,제8호, 65-73쪽, 2006년 8월

[2] Femtocell Forum, http://www.femtoform.org

[3] Picochip Inc, "The Case for Home Base stations," September 2008.

[4] 이덕규, 김도우, 한종욱, "홈네트워크 보안 기술 및 표준화 동향," 전자통신동향분석, 제23권, 제 4호, 89-101쪽, 2008년 8월

[5] ITU-T Study Group 17, http://itu.int/ ITU-T/studygroups/com17

[6] Naveen Sastry and David Wagner, "Security Considerations for IEEE 802.15.4 Networks," Proceedings of the 3rd ACM workshop on Wireless security, pp.32-42, Philadelphia, PA,USA, 2004.

[7] 김도우, 한종욱, 정교일, "홈디바이스 인증/인가 기술동향," 정보통신연구진흥원, 주간기술동향, 제 1326호, 1-11쪽, 2008년 1월

[8] 김양섭, "Zigbee 네트워크를 위한 코디네이터 중심의 침입탐지시스템," 중앙대학교, 2007년

[9] 이윤경, 한종욱, 정교일, "홈네트워크 보안 표준화 동향," 전자통신동향분석, 제22권, 제1호, 73-81쪽, 2007년 2월

[10] Ember Inc.," EmberZNet 3.1 New Features and Changes," April 2008.

[11] ZigBee Alliance, "Home Automation Profile Specification R25, ZIGBEE HOME AUTOMATION PUBLIC APPLICATION PROFILE," October, 2007.

[12] ZigBee Alliance, "ZigBee 2007 specification Document R17," October 2007.

[13] Gunhee Lee, Jaesung Lim, Dong-kyoo Kim, SungHyun Yang and MyungHyun Yoon, "An Approach to Mitigating Sybil Attack in Wireless Networks using ZigBee," ICACT2008. 10th International Conference on, pp.1005-1009, Gangwon-Do ,KOR, 2008.

[14] Ken Masica, "Securing ZigBee Wireless Networks in Process Control System Environments," CSSP, pp1-22, 2007.

[15] J. Douceur, "The Sybil Attack", in Proc. of the First International Workshop on Peer-to-Peer Systems.(IPTPS'02), Cambridge, MA, March 2002.

[16] 서대열, 김진철, 김경목, 오경환," ZigBee 네트워크에서 효율적인 Parent-Child 키 연결 알고리즘," 한국전자공학회, 제 43권, 제 10호, 35-46쪽, 2006년 10월

[17] 김진철, 오영환, "공개키 방식의 LR-WPAN보안 알고리즘," 한국전자공학회, 제 43권, 제 11호, 54-67쪽, 2006년 11월

[18] Moazzam Khan , Fereshteh Amini and Jelena Mišić, "Key Exchange in 802.15.4 Networks and Its Performance Implications." Mobile Ad-hoc and Sensor Networks, Vol. 4325, pp497-508, 2006.

[19] David Boyle and Thomas Newe, "Securing Wireless Sensor Networks: Security Architectures," JOURNAL OF NETWORKS, Vol. 3, No. 1, January 2008.

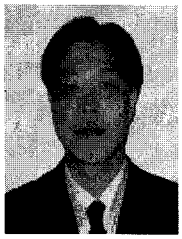
[20] Texas Instruments Incorporated (2007) Z-Stack ZigBee Protocol Stack [online], available: http://focus.ti.com/docs/toolsw/folders/print/z-stack.html

[21] Wander, A., Gura, N., Eberle, H., Gupta, V., Shantz, S. C (2005) ''Energy Analysis of

Public-Key Cryptography for Wireless Sensor Networks", Proceedings of the Third IEEEInternational Conference on Pervasive Computing andCommunications PerCom2005, pp 324-328. Mach 2005.
[22] ITU-T Study Group, "Framework of security technologies for home network," February 2007.

## 저 자 소 개

박 현 문(정회원)
2004년 한세대학교 공학사
2006년 국민대학교 전자공학과 정보통신학 석사
2006년~2008년 8월 국민대학교 BIT 비즈니스 정보통신 박사수료
2008년 9월~현재 전자부품연구원 연구원
<주관심분야 : 위치인지, USN, WLAN, 해양 통신>



서 해 문(정회원)
2000년 경북 대학교 전자공학 공학석사
2002년~2004년 삼성전자 통신연구소 R&D 센터
2004년~현재 전자부품연구원 선임연구원
<주관심분야 : RFIC, RF 시스템, 통신시스템>

박 수 현(종신회원)-교신저자
1988년 고려대학교 컴퓨터학과 이학사
1990년 고려대학교 대학원 전산학 이학석사
1998년 고려대학교 대학원 컴퓨터학 이학박사
1990년 (주) LG 전자 중앙연구소 선임연구원
1999년~2001년 동의대학교 공과대학 소프트웨어공학과 조교수
2002년~현재 국민대학교 비즈니스 IT학부 부교수
<주관심분야 : USN, UW-ASN>