Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.405

ZigBee 네트워크에서의 안전한 멤버쉽 프로토콜*

김 봉 환,† 박 창 섭‡
단국대학교

Secure Membership Protocol for ZigBee Network*

Bong-hwan Kim,† Chang-seop Park‡
Dankook University

요 약

ZigBee는 WBAN이나 스마트 그리드를 위한 차세대 표준 인프라로 인정받는 무선네트워크 통신프로토콜이다. 보안은 몇몇의 ZigBee 어플리케이션에서 중요한 역할을 한다. 특히, ZigBee안에서 멤버가 가입이나 탈퇴를 하는 상황에서는 엄격한 멤버관리가 필요하다. 본 논문에서, 우리는 현재 ZigBee에서 사용 중인 탈퇴 과정의 보안 취약점에 대하여 조사하고, 문제 해결을 위한 새로운 보안 스키마를 제시하고 그것의 보안능력 및 성능을 분석한다.

ABSTRACT

ZigBee is a wireless sensor network protocol recognized as a next-generation standard infrastructure for WBAN and Smart Grid. Security plays an important role in several ZigBee applications. Especially, strict membership control should be enforced when the membership is changed during the join and leave operations in ZigBee. In this paper, we investigate the security weakness of the current leave operation in ZigBee and propose a new security scheme to address it as well as its security and performance analysis.

Keywords: ZigBee, Authentication, Leave command

I. 서 론

시대의 흐름은 거리의 제약이 없는 무선의 시대로 흘러가고 있다. 최근에는 언제 어디서나 무선네트워크에 접속하여 필요로 하는 정보를 주고받을 수 있다. 따라서 다양한 형태의 통신네트워크가 나타나고 있는데 ZigBee도 그중 하나이다. ZigBee는 근거리 네트워크의 통신프로토콜로서 전력소모가 적고 구축비용이 적게 드는 장점을 가지고 있다. 최근 많은 분야에서 이러한 ZigBee를 활용하여 센서네트워크와 결합하려는 시도가 있다. 특히 실시간 양방향 지능형 전력시스템인 스마트 그리드와, 신체에 부착된 장치를 사용하여 건강에 대한 관리를 해주는 WBAN(Wireless Body Area Network)에서는 ZigBee를 표준 사양처럼 사용되고 있다. ZigBee는 IEEE의 근거리 통신 표준 중 하나인 802.15.4를 기반으로 하여 그 위에 몇 개의 계층을 더 추가한 형태이다.[1][2] ZigBee에서 사용되는 장치는 프로세서의 능력은 비교적 낮은 편이지만 활용분야에서 필요로 하는 목적에는 충분히 부합할 수 있으며, 전력소모가 낮은 편이기 때문에 긴 수명을 보장할 수 있다.

ZigBee도 무선네트워크 프로토콜이기 때문에 통신과정에서의 데이터암호화는 필수적인 기능이다. 문제는 ZigBee의 장치들이 본래의 목적으로 사용하기에는 무리가 없지만, 전송과정에서의 고도의 암호화작

접수일(2013년 2월 12일), 수정일(1차: 2013년 5월 9일, 2차: 2013년 6월 13일), 게재확정일(2013년 6월 13일)
* 본 연구는 한국연구재단 연구과제(NRF-2012R1A1A2000677) 지원 및 한국대학교 논문연구소 관리로 수행하였습니다.
† 주저자, kbh4365@naver.com
‡ 교신저자, csp0@dankook.ac.kr(Corresponding author)

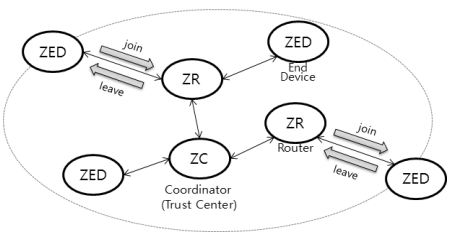
업까지 수행하기에는 성능이 부족하다는 점이다. 이를 해결하기 위하여 ZigBee 또한 자체적인 보안프로토콜을 구현하여 제공하지만 몇몇 부분에서 보안에 대한 취약점을 가지고 있다. 특히 네트워크에 가입되어 있는 장치가 탈퇴하는 과정에 대한 보안취약점이 나타나는데 이는 결국 네트워크 전체의 붕괴를 초래할 수 있기 때문에 적절한 대응방법이 필요하다.

ZigBee의 개발을 이끌어 가는 ZigBee Alliance는 ZigBee Specification을 통하여 ZigBee에 대한 사양과 상세한 구성을 설명해주고 있다. 그중에는 보안에 관련된 부분도 있는데, 범위가 방대하고 너무 세부적인 정보까지 설명하고 있어 그 내용을 이해하기에 어려움이 많다. [7], [8], [9]들이 ZigBee의 일반적인 보안과 관련된 논문들을 발표하였으나 부족한 면이 많았었다. 최근 Yüksel이 [3]을 통하여 ZigBee Specification의 내용 중 보안에 관련된 내용을 추출하고 서로 연관관계가 있는 부분들을 정리하였다. 또한 [7]을 통하여 ZigBee 네트워크의 가입과정에서 나타나는 비동기화 공격에 대한 취약점에 대한 해결책을 제시하였다. 하지만 이들 논문은 가입과정에서의 보안취약점에 대하여 논의하고 있을 뿐, 탈퇴과정에서의 보안취약점에 대한 연구는 이루어지지 않았다. 따라서 본 논문에서는 ZigBee의 탈퇴과정에 대한 보안취약점을 분석하고 이에 대한 해결책을 제시하고자 한다.

본 논문은 2장에서 ZigBee의 기본적인 구성에 대하여 설명하고, 3장에서는 가입 및 인증, 탈퇴과정을 설명한다. 4장에서는 탈퇴상의 보안 취약점에 대하여 조사하고, 5장에서 보안 취약점에 대한 해결책을 제시하며, 6장에서 제시한 해결책에 대한 평가를 한다.

II. ZigBee 네트워크

2장에서는 ZigBee Specification과 [3]에서의 ZigBee 네트워크에 대한 구성에 대하여 설명한다.

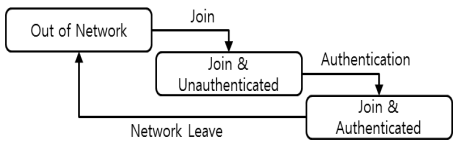


[그림 1] ZigBee 네트워크

2.1 ZigBee네트워크의 구성

ZigBee 네트워크는 한 개의 ZC(ZigBee Coordinator)에 다수의 장치가 연결되어진 형태로 구성되어진다. ZC에는 ZigBee 네트워크의 보안을 관리하는 TC(Trust Center)가 위치한다. ZC는 ZR(ZigBee Router)혹은 ZED(ZigBee End Device)와 연결될 수 있으며 ZED은 다시 ZR과 연결되어 계층구조를 형성한다.

ZigBee 네트워크는 구성장치들이 가입과정과 인증과정을 거쳐야만 네트워크의 사용권한을 획득할 수 있다. 가입과정만 거쳐서는 네트워크를 사용할 수 없으며, 추가적으로 인증과정까지 거쳐야만 네트워크를 사용할 수 있다. [그림 2]는 ZigBee 네트워크에서 각 장치들의 상태를 나타낸 것이다.



[그림 2] ZigBee네트워크에서의 장치상태[3]

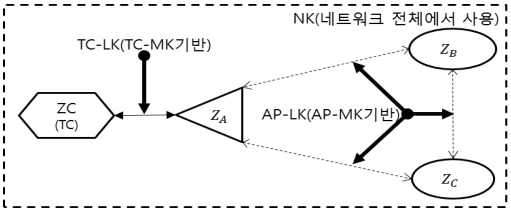
ZigBee의 장치들은 초기에 Out of Network 상태로 유지되다가 네트워크에 가입(join)하게 되면 Join&Unauthenticated 상태가 된다. 이는 가입과정만 거친 상태로 아직은 네트워크를 사용할 수는 없다. 인증(Authentication)까지 끝마치면 장치는 Join&Authenticated 상태가 되어 네트워크를 사용할 수 있게 된다. 작동 중 탈퇴해야할 경우가 생기게 되면 탈퇴(Network Leave)을 거쳐서 보안과 관련된 정보를 삭제한 후 Out of Network의 상태로 돌아가 대기하게 된다.

2.2 ZigBee의 키 유형과 Pre-installation

2.2.1 암호화 키 유형

ZigBee에서 사용하는 암호화키는 마스터키 MK, 링크키 LK, 네트워크 키 NK가 있으며 사용목적에 따라 다르게 사용된다. [그림 3]은 ZigBee 네트워크에서 사용되는 키를 표현한 것이다.

Z_A와 Z_B는 각각 ZigBee 네트워크에서의 장치들을 의미한다. 본 논문에서는 ZigBee 네트워크의 용어 및



〔그림 3〕 ZigBee 네트워크 키

장치에 대한 이해를 원활하게 하기 위하여 〔표 1〕의 정의들을 이용하기로 한다.

〔표 1〕 용어 Notation

용어	정의
Z_X (X=A,B,C…)	X를 ID로 가지는 ZigBee 장치.
TC - (MK or LK)	TC와 ZigBee장치가 공유하는 MK 또는 LK
AP - (MK or LK)	ZigBee장치간에 공유하는 MK 또는 LK
MK_{AB} or LK_{AB}	A, B를 ID로 가지는 두 장치가 공유하는 키

일반적으로 Z_A는 ZR을, Z_B는 ZED를 나타내지만 네트워크에 따라서는 중간에 ZR이 없이 ZC와 ZED만으로 구성되는 경우도 존재하기 때문에, 이후의 내용에서는 장치의 표시를 Z_A와 Z_B만을 사용하여 나타내기로 한다.

ZigBee네트워크에서의 MK는 네트워크의 초기 설정과정에서 LK의 생성을 위해 사용된다. LK는 MK를 기반으로 SKKE(Symmetric Key Establishment Procedure)를 기동시켜 획득할 수 있으며, 응용계층(Application Layer)에서 유니캐스트로 전달되는 메시지를 암호화한다. LK와 MK는 키를 공유하는 대상에 따라서 다시 세부적으로 구분되어 질 수 있다. TC와 각각의 장치 사이에 공유되는 키를 TC-MK와 TC-LK라고 하며, 두 개의 ZigBee 장치 사이에 공유되는 키를 AP-MK와 AP-LK라고 한다. NK는 네트워크전체의 모든 장치가 함께 공유하는 그룹 키로, 네트워크 전체의 보안을 담당하고 있다.

2.2.2 ZigBee 키 설정 유형

ZigBee에서 사용되는 모든 키들은 Key-transport나 Key-establishment, 또는 Pre-installtion 방법을 사용하여 획득할 수 있다. Key-transport는 무선통신을 통하여 사용할 키를 TC로부터 전송받는 방법으로, 키의 전달과정에서 제3자에 의한 통신도청이 가능하다는 위험성을 가지고 있다. key- establishment는 두 장치가 주고받은 데이터를 가지고 새로운 키를 생성하는 방법이다. ZigBee에서는 MK를 사용하여 LK를 획득하는 과정에서 사용된다. Pre-installation은 사전에 장치의 메모리에 키를 저장해두었다가 초기 기동 시에 사용하는 방법이다.

ZigBee 장치들은 암호화키들을 사용하여 필요한 작업을 수행하는데, 각각의 키들은 서로 다른 방법을 통하여 획득되어 질 수 있다. 〔표 2〕는 ZigBee에서 사용하는 키들이 획득되어 질 수 있는 방법을 나타낸 것이다.

〔표 2〕 키 종류별 획득방법〔3〕

	MK	LK	NK
key-transport	YES	YES	YES
key-establishment	NO	YES	NO
Pre-installation	YES	YES	YES

ZigBee네트워크에서는 어떤 키를 어떤 방법으로 획득하는가에 따라서 초기설정의 진행과정이 다르게 나타날 수 있다. 그러나 Key-transport는 전달과정에서의 위험성이 존재하기 때문에, 일반적인 경우 Pre-installation의 방법을 더 선호한다. Key-establishment의 경우 LK를 생성하는 경우에만 사용되기 때문에 일반적인 조건으로는 적합하지 않다. 하지만 일반적으로 사용되는 Pre-installation의 경우에도 사전에 저장하는 키의 종류에 따라서 세부적인 진행과정에 차이가 발생한다. MK를 저장해두었다가 사용하는 경우가 일반적이지만, 필요에 따라서는 초기 진행과정을 생략하고 바로 LK나 NK를 Pre-installation할 수도 있다.〔5〕

이 논문에서 ZigBee네트워크에서의 모든 설정과정에 대한 것을 분석하는 것은 비효율적이기 때문에, 이후의 내용은 특정한 하나의 기준을 놓고 설명하기로 한다. 선택된 기준의 조건은 다음과 같다.

Q1. "생략된 부분이 없이 모든 진행과정을 파악할 수 있는가?"

Q2. "기본적인 안정성을 확보할 수 있는가? "

ZigBee 네트워크의 설정과정 중에서 위의 조건에

가장 적합한 방법은 TC-MK가 Pre-installation된 환경이다. MK를 저장하는 방법이기 때문에 생략되는 진행과정이 없고, 무선통신을 통하여 키가 전달되지 않기 때문에 기본적인 안정성도 확보할 수 있기 때문이다. 따라서 이후의 내용에서는 TC-MK의 Pre-installation을 기준으로 한다.

III. 네트워크의 가입 및 탈퇴

이번 장에서는 ZigBee 네트워크에서 장치의 가입과정 및 탈퇴과정에 대하여 논의한다. 장치의 가입과정과 인증과정을 알아본 다음, 필요한 키를 분배받는 과정과 장치가 네트워크에서 탈퇴하는 과정을 알아본다. II, 에서와 마찬가지로 진행과정에 대한 이해를 원활하게 하기 위하여 사용되는 공식에 대하여 다음의 〔표 3〕의 수식들을 사용하기로 한다.

〔표 3〕 수식 Notation

수식	정의
$kdf(.)$	괄호 안의 정보를 사용하여 새로운 키를 생성하는 함수
$h(Key)$	Key를 사용하여 선택부분에 대한 인증데이터를 생성하는 해쉬함수
$[.]_{Key}$	Key를 사용하여 〔〕안의 내용을 암호화하는 함수
$MIC(Key)$	Key를 사용하여 MIC(Message Intergrity Code)를 생성하는 함수

3.1 SKKE 와 MEA

ZigBee에서는 *SKKE*(Symmetric-Key Key Establishment Protocol)를 수행하여 MK로부터 LK를 획득한다. 접속을 시도하는 장치 Z_A의 ID를 A, 응답하는 장치 Z_B의 ID를 B라고 할 때, Z_A와 Z_B가 상호간에 공유하고 있는 AP-MK인 MK_{AB}를 사용하여 링크키 LK_{AB}를 획득하는 과정이다. 본 논문에서 정한 기준조건에 따라서 MK는 미리 장치에 저장이 되어있어야 하기 때문에, SKKE에서 사용되는 MK_{AB}는 미리 장치에 저장되어 있다. 따라서 각 장치는 저장되어 있는 MK_{AB}와 상호간에 전달되는 난수(RN_A, RN_B)와 장치ID (A, B)를 기반으로 하여 LK_{AB}를 계산한다. 계산된 LK_{AB}를 상대방에게 전달하면 수신 측에서도 동일한 과정으로 LK_{AB}를 계산하고 수신한 키와 비교하여 상호간에 동일한 키를 만들어냈다는 것을 간접적으로 확인하게 된다. 장치 Z_A와 Z_B는 서로 ID와 RN(Random Number)를 전달하고, 전달된 ID와 RN을 사용하여 LK_{AB}를 획득한다. LK는 키 도출 함수인 $kdf(.)$를 사용하여 계산되며, 사용되는 LK_{AB}의 계산공식은 다음과 같다. 〔3〕〔4〕

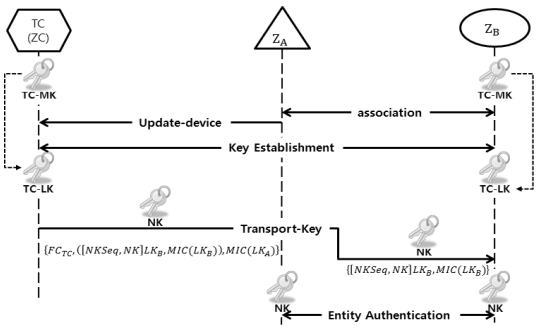
$$LK_{AB} = kdf(A, B, RN_A, RN_A, MK_{AB})$$

계산된 LK는 다시 상호간에 전달되어 자신이 계산한 LK와 동일한지 확인하는 과정을 거친다. 이를 통하여 두 장치는 상호간에 동일한 키가 계산되었는가를 확인할 수 있다.

MEA(Mutual Entity Authentication)는 ZigBee에서 사용하는 개체 확인 프로토콜로 Z_A와 Z_B가 동일한 NK를 가지고 있다는 것을 기반으로 상호인증을 수행하는 과정이다. MEA도 SKKE와 마찬가지로 상호간에 ID와 RN을 주고받는다. 전달된 ID와 RN, NK를 이용하여 확인데이터를 생성하고 이를 상호간에 전달하여 동일한 데이터가 계산되었는가를 비교함으로써 동일한 NK를 가지고 있는 ZigBee 네트워크내의 장치란 것을 확인하는 방법이다.〔3〕

3.2 가입 및 인증

〔그림 4〕는 ZigBee의 가입과정과 인증과정을 표현한 것이다. Z_B가 자신의 정보를 전송하여 가입과정(association)을 수행하면 〔그림 2〕에서의Join & Unauthenticated 상태가 된다. 이 상태는 네트워크에 가입은 되어 있지만 인증은 되지 않은 상태로 아직 네트워크를 사용할 수는 없다. 가입과정이 끝나면 Z_A는 Z_B에 대한 인증을 위하여 TC에게 장치목록에 대한 갱신을 요청(update-device)하게 된다. TC는



〔그림 4〕 Secured 네트워크의 가입과정〔5〕

인증요청을 한 Z_B와 Key-establishment를 수행한다. 이 과정은 TC와 Z_B가 SKKE를 수행하여 상호간의 TC-LK를 획득하는 과정이다. 획득한 TC-LK를 사용하여 암호화된 전송구간을 설정하면, 이 구간을 통하여 NK가 TC로부터 Z_B로 전송된다. 표준프로토콜에서 전달되는 데이터의 전체내용은 다음과 같다.〔6〕

$$\{FC_{TC}, ([NKSeq, NK]LK_B, MIC(LK_B)), MIC(LK_A)\}$$

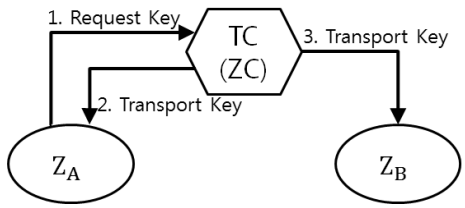
FC_{TC}(Frame Counter)는 데이터의 freshness를 보장하기 위한 파라메터이고, MIC(Message Integrity Codes)는 전달되는 데이터의 무결성을 보장하기 위하여 추가된 데이터이다. MIC를 함께 전달하는 것은 메시지의 전달과정에서 변조가 이루어지지 않았다는 것을 보장하기 위함이다. MIC는 해시함수 $h(key)$와 무결성을 보장하려는 데이터를 결합하여 작성된다. 전달 데이터에서 $MIC(LK_A)$는 TC와 Z_A 사이에 설정된 TC-LK를 key로 사용하여 MIC를 제외한 나머지 부분에 대한 무결성을 보장하기 위한 확인 데이터이다. LK_A는 TC-LK이기 때문에 이 키를 모르고 있는 상태에서 데이터를 변조한다면 도착 위치에서의 계산 결과와 LK_A를 사용한 MIC의 값이 다르기 때문에 데이터의 변조여부를 확인할 수 있다. NK와 NKSeq는 현재 네트워크에서 사용되고 있는 NK와 그 순서를 전달하는 파라메터이다. NK는 주기를 가지고 새로운 NK로 갱신이 되기 때문에, 현재의 NK가 몇 번째의 NK인지 구별하기 위한 순번정보가 필요하다. 따라서 순번정보도 NK와 같이 전달해야 하는데, 이런 역할을 하는 파라메터가 NKSeq이다. TC에서 Z_A로 전달된 데이터 중 일부분은 다시 Z_B로 전달되어 NK를 설정하는데 사용된다. Z_A로부터 Z_B로 전달되는 데이터는 다음과 같다.〔6〕

$$\{[NKSeq, NK]LK_B, MIC(LK_B)\}$$

이 메시지까지 전달받고 나면 Z_B는 NK를 획득할 수 있으며, Join & Authenticated 상태가 되어 네트워크의 사용이 가능하게 된다. 또한 Z_A와 Z_B는 NK를 기반으로 MEA를 수행하여 상호간에 인증을 마치게 되고 네트워크에서 자신의 역할을 수행한다.

3.3 Key-distribution

ZigBee의 키 분배 프로토콜은 Z_A와 Z_B가 공유할 AP-LK를 TC로부터 분배 받을 때 사용된다. 키 분배 프로토콜은 3개의 메시지를 전달하여 진행되며 각각의 메시지들은 TC와 장치 간에 공유되는 TC-LK (LK_A, LK_B)를 사용하여 암호화된다. 〔그림 5〕는 키 분배프로토콜에서 전달되는 3개의 메시지의 전달 순서를 표현한 것이다.



〔그림 5〕 ZigBee 키 분배

먼저 Z_A가 TC에게 Z_B와 공유할 키를 요청하는 *Key-Request* command를 전달한다.

$$1.\ Key-Request(Z_A, TC): \{Z_B, FC_A, MIC(LK_A)\}$$

Z_B는 분배받을 키를 공유하려는 상대방이고, FC_A는 Z_A의 Frame Counter이며, MIC는 메시지의 무결성을 보장하기 위한 데이터이다. TC는 키 분배 요청에 대하여 *Transport-Key* command를 사용하여 Z_A와 Z_B가 공유할 키인 LK_{AB}를 각각 전달하게 된다. *Transport-Key* command에서 사용되는 $\{.\}_{key}$는 key를 사용하여 괄호안의 데이터를 암호화하는 함수이다. 따라서 LK_{AB}는 $\{LK_{AB}\}_{TC-LK}$ 의 형태로 전달된다.

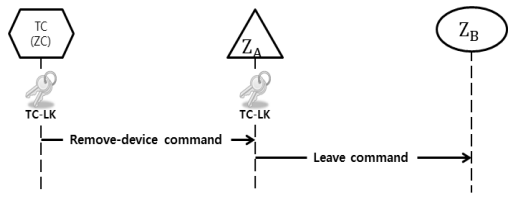
$$2.\ Transport-Key(TC, Z_A):$$
$$\{Z_B, FC_{TC}, \{LK_{AB}\}LK_A, MIC(LK_A)\}$$

$$3.\ Transport-Key(TC, Z_B):$$
$$\{Z_A, FC_{TC}, \{LK_{AB}\}LK_B, MIC(LK_B)\}$$

처음에 나타나는 파라메터는 키를 공유할 상대 장치의 ID이며, 두 번째 파라메터는 TC의 Frame Counter이다. 세 번째 파라메터는 각 장치와 TC사이의 TC-LK로 암호화된 공유키이고, 마지막 파라메터는 무결성을 보장하기 위한 확인데이터이다.

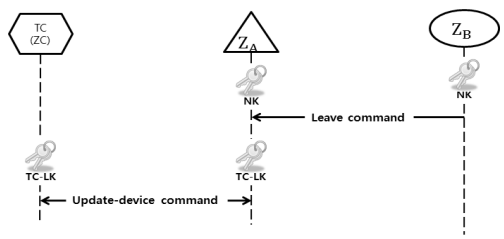
3.4 탈퇴

ZigBee 네트워크의 탈퇴과정은 메시지를 전송하는 주체에 따라서 2가지의 방법이 있으며 메시지의 전달방향이 다르다.



〔그림 6〕 Secured 네트워크의 탈퇴과정(TC에서 Z_B로)〔5〕

〔그림 6〕은 TC가 Z_B를 탈퇴시키는 과정을 나타낸 것이다. TC는 탈퇴시키려는 장치 Z_B의 ID를 자신의 장치목록에서 삭제하고, Z_A에게 장치제거에 대한 Remove-command를 전송한다. Remove-command는 TC와 Z_A간에 공유되는 TC-LK인 LK_A로 암호화되어 전송된다. Z_A는 전달받은 command에 따라 Z_B를 네트워크에서 제거하게 되며, Z_B에게 Leave-command를 전달하여 네트워크에서 떠나야 함을 알린다. Leave-command를 전달받은 Z_B는 자신이 가지고 있던 NK 및 LK를 삭제하며, 다시 가입과정을 거치기 전까지는 네트워크를 사용할 수 없게 된다.



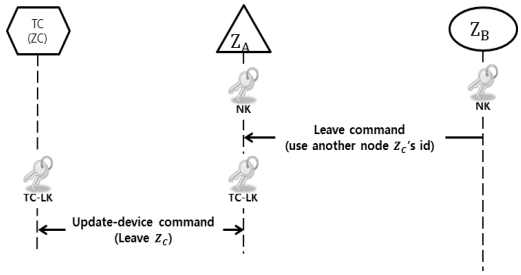
〔그림 7〕 Secured 네트워크의 탈퇴과정(Z_B로부터의 요청)〔5〕

〔그림 7〕은 Z_B가 먼저 네트워크를 탈퇴하겠다는 것을 전달하는 과정을 나타낸 것이다. 〔그림 6〕과는 메시지의 전달방향이 반대로 진행된다. 말단장치인 Z_B가 현재 사용 중인 NK를 사용하여 Z_A로 네트워크를 탈퇴하겠다는 Leave-command를 전달하면 Z_A는 이것을 확인하고, TC에게 탈퇴하는 장치가 있다는 것을 알리는 Update-device command를 전달한다. command를 전달하고 나면 〔그림 6〕에서와 마찬가지로 Z_B는 자신이 가지고 있던 키들을 삭제하게 된다. Z_A가 전달하는 Update-device command는 LK_A로 암호화하여 전달되며, TC는 해당 command를 전달받으면 장치목록에서 탈퇴를 요청한 장치를 삭제하게 된다.

IV. 취약점 및 개선방향

4.1 Leave-command에 대한 취약점

ZigBee 네트워크에서 무선으로 전달되는 대부분의 데이터는 NK를 사용하여 암호화된다. 탈퇴 command를 전송할 때도 NK를 사용한다. 각각의 장치는 NK로 암호화한 탈퇴 command를 전송한다. 그런데 NK만을 사용하여 탈퇴 command를 작성하면, 어떤 장치가 해당 command를 작성하였는지는 확인할 수가 없다. 이는 중요한 문제인데, 신뢰성이 보장된 TC에서 탈퇴 command 작성하는 첫 번째 방법에서는 command 작성자에 대한 문제가 없지만, 장치가 먼저 탈퇴 command를 작성하는 두 번째 방법에서는 command 작성자가 누구인가에 대한 큰 문제점이 발생한다. 다른 장치의 ID를 사용하여 위조 command를 전송하여 탈퇴요청을 한다고 하더라도 Z_A나 TC에서는 해당 ID의 장치가 command를 직접 작성한 것인지는 확인할 수가 없기 때문이다.



〔그림 8〕 ID위조에 의한 노드의 강제 탈퇴

〔그림 8〕와 같이 Z_B가 자신과 같은 네트워크에 위치하는 장치인 Z_C의 ID를 사용하여 탈퇴 command를 작성하고 Z_A에게 전달하더라도 Z_A나 TC에서는 이것을 어떤 장치가 작성한 command인지는 확인할 수가 없다. ZigBee 네트워크에서는 NK로 암호화되었는가만 확인할 수 있기 때문에 command를 작성하여 전송한 장치에 대해서는 구별이 불가능하다.

이는 ZigBee 네트워크에서의 탈퇴 command에 대한 모든 처리과정을 NK에만 의존하도록 만들어졌기 때문이다. ZigBee 네트워크에서는 네트워크 안에 위치하는 장치들이 상호간에 인증을 시도하는 과정에서 ID를 주고받기 때문에 쉽게 상대방의 ID를 획득할 수 있다. 따라서 악의적인 목적을 가지는 장치가 존재한다면 다른 장치와의 인증을 시도하여 상대방의 ID를 획득한 다음, 이 ID를 사용하여 탈퇴 command를 위조하는 것이 어렵지 않다. 그러나 NK에만 의존하는 표준프로토콜의 방법으로는 TC가 위조 command를 구별해 낼 수 있는 방법이 없다. 도착한 탈퇴 command는 현재 사용 중인 NK를 사용하여 암호화 하였는가만 확인되기 때문에 위조된 탈퇴 command라도 NK로 암호화만 되어있다면 문제점이 발견되지 않는다. 따라서 위조된 command가 도착하더라도 Z_A는 이를 정상으로 인식하여 TC에 Update-device command를 전달하게 되며, TC는 해당 command에 나타나는 장치인 Z_c를 네트워크에서 제거하게 된다.

이렇게 목록에서 제거된 Z_c는 자신이 탈퇴된 것을 알 수 없기 때문에 이전과 마찬가지로 네트워크의 사용을 시도하게 된다. Z_C는 현재 작동중인 NK를 그대로 가지고 있기 때문에 NK가 업데이트되기 전까지는 네트워크 내에서 데이터의 전송이 가능하다. 그러나 네트워크의 장치목록에서는 해당 장치가 제거된 것으로 처리되기 때문에 Z_C가 전송하는 데이터는 네트워크 내에서 충돌이 발생시키고 데이터의 계산과정에서 심각한 오류를 만들어낸다.

따라서 하나의 장치가 자신과 통신할 수 있는 주변의 모든 장치들에 대하여 탈퇴 command를 위조하게 된다면 네트워크의 일정부분을 마비시킬 수 있다. ZigBee에서는 상대방의 ID를 알아내는 것은 어렵지 않기 때문에 따라서 악의적인 목적을 가진 장치가 네트워크 안에서 위치를 옮겨 다니면서 주변장치의 ID를 획득한 다음 탈퇴 command를 위조하게 된다면 네트워크의 여러 부분을 순차적으로 마비시킬 수 있다. 결국 이런 상황이 반복된다면 네트워크 전체가 붕괴하게 된다.

4.2 개선 프로토콜

결국 4.1에서 제시한 취약점을 해결하기 위해서는 command의 전달 과정에서 command 작성자에 대한 식별을 필요로 한다. 작성자에 대한 식별만 가능하게 되면 다른 장치의 ID를 사용한 위조 command가 도착하더라도 이를 구분해내어 제거할 수 있기 때문이다. 하지만 표준프로토콜처럼 NK만을 사용하는 command전달 방법으로는 작성자를 식별해 낼 수 없다.

본 논문에서는 이런 식별에 대한 문제를 해결하기 위하여 장치 Z_A와 Z_B만이 공유하는 별도의 키인 LK_{AB}를 사용하는 방법을 제안한다. LK_{AB}는 Z_A와 Z_B만 공유하는 AP-LK로 두 장치만을 위하여 생성되는 LK이기 때문에 다른 장치는 이 키를 알아 낼 수가 없다. 따라서 LK_{AB}를 사용하여 command를 암호화하고 이를 전달하게 되면 command를 작성하여 전달하는 장치에 대한 구분이 가능해지게 된다. 장치간의 인증을 시도하는 과정에서 Z_C는 자신과 다른 장치인 Z_B의 ID는 획득할 수 있지만 Z_A와 Z_B가 공유하고 있는 LK_{AB}는 획득할 수 없기 때문에 Z_B에서 Z_A로 보내는 어떠한 command도 위조할 수 없게 된다.

또한 제안프로토콜은 표준프로토콜과 다르게 가입과정과 인증과정에서 Z_A와 Z_B에게 LK_{AB}를 분배해주는 과정을 포함하고 있다. 제안프로토콜에서는 LK_{AB}의 사용이 선택적인 것이 아니기 가입 및 인증과정과 키 분배과정을 하나로 합치게 된다. 만약 표준프로토콜처럼 인증과 키 분배의 과정을 따로 거치게 될 경우 많은 전력소모가 발생하게 된다. 그러나 제안하는 방법처럼 과정들을 하나로 합칠 수 있게 되면 불필요한 전력소모량을 줄일 수 있다.

제안프로토콜을 사용하여 가입과정과 인증과정을 마치게 되면 Z_A와 Z_B는 NK와 함께 LK_{AB}를 획득할 수 있다. LK_{AB}는 두 장치만을 위하여 TC로부터 분배받는 AP-LK이다. LK_{AB}는 TC-MK인 MK_B를 기반으로 생성되며 표준프로토콜의 계산과정 다음과 같다.

$$LK_{AB} = kdf(MK_B, TS_{TC}, A, B)$$

TS_{TC}는 LK_{AB}를 생성하는 순간의 TC에서의 TS(Time Stamp) 값이다. 이 값은 이후에도 계속하여 순번의 의미로 사용되기 때문에 별도로 기록해둔다. 표준프로토콜에서 제공되는 FC는 바이트수가 작아 한계가 크기 때문에 좀 더 큰 수를 Counter로 사용해야 할 경우에 기록해둔 TS를 사용할 수 있다. TC는 생성된 LK_{AB}를 LK_A로 암호화하여 Z_A에게 분배해준다. Z_B에게는 NK를 전달하는 데이터에 TS_{TC}를 추가하여 전송한다. 다음은 TC로부터 Z_A와 Z_B에

게 전달되는 메시지의 내용이다.

$$TC \rightarrow Z_A : [LK_{AB}]LK_A$$

$$TC \rightarrow Z_B : [TS_{TC}, NKSeq, NK]\, LK_B$$

이를 바탕으로 표준프로토콜에서 전달했던 Trans-port-key command의 내용을 변경하면 다음과 같다.

$$Transport-key(TC \rightarrow Z_A):$$
$$\{FC_{TC}, ([TS_{TC,} NKSeq, NK]LK_B, MIC(LK_B)),$$
$$[LK_{AB}]LK_{A,} MIC(LK_A)\}$$

$$Transpory-key(Z_A \rightarrow Z_B):$$
$$\{FC_A, [TS_{TC,} NKSeq, NK]LK_B, MIC(LK_{AB})\}$$

Z_A에서 Z_B로 전달되는 프레임에 대한 무결성 체크를 위해서 LK_{AB}를 사용하는 것은 데이터를 전달받은 그 순간에 Z_B가 Z_A와 공유하고 있는 키가 없기 때문이다. Z_B는 전달받은 TS_{TC}를 사용하여 LK_{AB}를 생성하면 전달받은 메시지에 대한 무결성을 확인할 수 있으며, 제대로 된 LK_{AB}를 생성했다는 것도 간접적으로 확인할 수 있다. 여기까지의 진행과정이 끝나면 Z_A와 Z_B는 공유키인 LK_{AB}에 대한 분배가 끝난 상태로 이후의 진행과정은 모두 LK_{AB}를 사용하게 된다.

V. 분석 및 평가

5.1 안정성 분석

표준프로토콜의 진행과정에서는 장치 Z_A와 Z_B 사이에 전달되는 데이터가 모두 NK를 사용하여 암호화되기 때문에 어느 장치에서부터 데이터가 전달된 것인지 식별할 수 없다. 모두가 같은 키를 사용하기 때문에 실제로 어떤 장치가 해당 데이터를 작성한 것인지는 확인할 방법이 없기 때문이다.

제안프로토콜은 이런 문제점을 해결하기 위하여 인증과정에서부터 Z_A와 Z_B사이에 두 장치만이 공유하는 키인 LK_{AB}를 설정하게 한다. LK_{AB}는 두 장치 Z_A와 Z_B만이 공유하는 키이기 때문에, 다른 장치인 Z_C는 해당키를 알 수가 없다. 만약 Z_C가 Z_B의 ID를 사용하여 탈퇴 command를 전달하고자 가정하자. Z_C는 Z_B의 ID는 알아낼 수 있지만, Z_A와 공유하는 LK_{AB}을 알 수가 없다. 따라서 Z_C가 Z_B의 탈퇴 command를 작성하여 Z_A에 전달하더라도, LK_{AB}로 암호화된 데이터가 아니기 때문에 Z_A는 해당 command를 드롭시켜 버린다. 즉, 제안프로토콜을 사용하면 어떤 장치로부터 온 것인지 식별해낼 수 있어, 위조 command에 대한 대응이 가능하게 되는 것이다. 각각 장치들은 상호간에만 공유하고 있는 키를 사용하여 전달되는 데이터를 암호화하기 때문에, 다른 장치들이 이를 위조해낼 수 없기 때문이다.

제안프로토콜에서는 새로운 키를 설정하기 위해서 표준프로토콜의 Trans-port key command에 TS와 LK_A로 암호화된 $[LK_{AB}]LK_A$를 추가데이터로 삽입하여 전달한다. 이후의 인증 및 데이터전달은 LK_{AB}를 통하여 하기 때문에 다른 장치의 ID는 위조할 수 있어도 암호화를 할 수 없기 때문에 command를 위조를 방지할 수 있어 4.1에서의 취약점을 해결할 수 있다.

만약 LK_{AB}가 노출된다면 표준프로토콜과 마찬가지로 command에 대한 위조가 가능하기 때문에, 4.1에서 나타났던 탈퇴 command상의 보안 취약점이 생길 수 있다. 하지만 이런 상황이 되더라도 문제가 발생하는 것은 Z_B뿐이다. 표준에서는 NK만을 사용하기 때문에 NK가 노출되면 전체 네트워크가 위험해졌지만 제안프로토콜에서는 두 장치만 공유하는 키인 LK_{AB}만 노출된 것이기 때문에 네트워크 안의 장치전체가 아닌 해당 장치만 command위조에 대한 위협에 노출된다. 제안프로토콜에서는 command를 위조하더라도 Z_B의 command만이 위조되기 때문에 문제가 발생하더라도 그 피해는 Z_B로 한정된다.

5.2 성능분석

ZigBee 네트워크 프로토콜의 성능을 분석하기 위해서는 각각의 장치들이 소모하는 전력량을 분석할 필요가 있다. ZigBee의 장치들은 전력소모를 줄여서 배터리의 수명을 늘릴 수 있게 만드는 것을 목표로 하기 때문에 과도한 전력소모가 생기는 프로토콜은 적합하지 않다. 따라서 본 논문에서는 ZigBee 명세서의 표준프로토콜과 제안하는 프로토콜에서 각각 TC, Z_A, Z_B가 소모하는 에너지를 계산하여 성능을 분석하고자 한다. 각각의 장치에 공급되는 전력 및 사용전류의 양은 동일하다고 가정한다.

ZigBee의 장치들이 실제 사용하는 에너지의 대부

분은 메시지의 송신 및 수신에서 이루어진다. 암호화 알고리즘을 수행하는데 사용하는 에너지도 있지만 송수신에 비해서는 매우 작은 양이기 때문에 본 논문에서는 메시지의 송신과 수신에 대한 소모량만 계산하기로 한다.[7]

본 논문에서 제안하는 프로토콜은 ZigBee 명세서에 나타나는 표준프로토콜의 데이터 필드 중 일부를 사용하여 추가 데이터인 TS와 $[LK_{AB}]LK_A$를 전달한다. 표준프로토콜에서는 Z_A와 Z_B가 TC로부터 키를 분배받기 위해서 3개의 메시지를 추가로 교환해야 하지만 제안프로토콜을 수행하게 되면 이 과정을 추가데이터의 포함만으로 인증과정에 포함시킬 수 있다. 따라서 추가로 전달하는 데이터를 포함한 프로토콜의 진행에 사용되는 에너지양과 표준프로토콜의 진행과정과 추가키 분배에 필요한 3개의 메시지 전송에 사용되는 에너지의 소모량을 비교해야 한다. 표준 프로토콜과 제안프로토콜의 진행과정에는 메시지를 교환하는 도중에 ACK의 전달 및 송·수신모드로의 전환과정 등을 포함해야 하는데, 여기에 들어가는 에너지 소모량은 전체의 소모량에 비하여 매우 적은양이고, 실질적으로 중요한 부분이 아니기 때문에 비교과정에서는 이 부분을 배제하고 에너지소모량을 계산한다. 에너지 소모량 계산에 이용되는 기호 및 수식은 다음과 같다.

〔표 4〕 에너지단위 기호[8]

기호	설명	단위
U	노드의 전력공급량 값	V
I	Tx모드 동안의 현재 전류 소비량 값	A
t	메시지 처리시간	sec

〔표 5〕 에너지 소모율 공식[8]

에너지 소모율
$ETx = U[V] \times I[A] \times t[s]$

〔표 5〕의 수식을 사용하면 소모되는 에너지를 실제 수치 값으로 측정할 수 있다. 실제 소모량 계산 시에는 U와 I의 값과 t의 값에 대한 단위가 서로 일치하지 않기 때문에, 각각을 별도로 계산한 다음 수치를 통일한다.

ZigBee는 장치를 제조하는 제조사별로 사용하는 칩과 사용 기능이 다르기 때문에 소모되는 에너지의 양도 모두 다르다. 따라서 장치마다 사용하는 에너지양이 다르기 때문에 이를 일반화 시키는 것은 무리가 있다. 따라서 본 논문에서는 특정 상황을 가정하고 가정조건하에서 두 프로토콜이 사용하는 에너지양을 비교하기로 한다. 각 노드에 공급되는 전력은 2V로 일정하고, 전류량 또한 15mA로 동일하다고 가정한다. 또한 사용되는 칩의 전송속도는 250kbps로 가정한다. 이를 사용하면 메시지의 길이에 따른 전송처리시간을 계산할 수 있다. 메시지의 길이를 k byte라고 하면 k byte를 전송하는데 걸리는 시간 tk는 다음과 같다.[8]

$$tk = (k \times 8) / (250 \times 1000)$$

여기서 메시지의 길이와 전송속도에 곱해지는 숫자들은 단위를 바이트로 통일시키기 위함이며, 이를 통하여 실제의 수치를 가정할 수 있다. 처리시간을 계산하는데 사용되는 수식의 기호는 다음과 같다.

〔표 6〕 처리요청 명령어[8]

기호	설명
Key-Request	키 요청 메시지
Transport-key	키 전송 메시지

이를 사용하여 표준프로토콜에서의 추가키 분배과정을 표현하면 다음과 같다.

$$Z_B \rightarrow TC: Key-Request\{FC_B, Z_B, MIC(LK_B)\}$$

$$TC \rightarrow Z_B: Transport-key \{FC_{TC}, Z_A, [LK_{AB}]LK_B, MIC(LK_B)\}$$

$$TC \rightarrow Z_A: Transport-key \{FC_{TC}, Z_B, [LK_{AB}]LK_A, MIC(LK_A)\}$$

결국 두 프로토콜의 진행과정을 따라가면 프로토콜별로 필요한 바이트수를 비교할 수 있다. 단, 전송과정에서 소모되는 전력양은 송신측만 나타나는 것이 아니라 수신측도 고려되어야 한다. 수신과정도 송신과정과 동일한 전력양이 소모가 되기 때문에 이 부분도 고려가 되어야 한다. 따라서 바이트 수에 따라서 소모되는 전력량을 계산하면 다음과 같은 결과를 얻을 수 있다.

〔표 7〕과 〔표 8〕의 수치는 장치1개를 기준으로 했을 때 TC와 Z_A, Z_B가 소모하는 총 에너지양이며 표준프로토콜과 제안프로토콜의 에너지 효율은 제안프

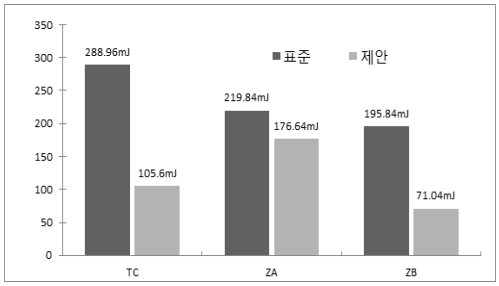
〔표 7〕 데이터 전송에 필요한 패킷의 길이

	표준	제안
가입		
Transport-key (TC->Z_A)	86bytes	110bytes
Transport-key (Z_A->Z_B)	66bytes	74bytes
분배		
Key-Request (Z_B->TC)	61bytes	N/A
Transport-key (TC->Z_B)	77bytes	N/A
Transport-key (TC->Z_A)	77bytes	N/A

〔표 8〕 프로토콜에 따른 전력소모량

		표준	제안
전력 소모량	가입	291.84mJ	353.28mJ
	분배	415.80mJ	N/A
	합계	704.64mJ	353.28mJ

로토콜이 약 50%정도 더 우수하다. TC와 Z_A, Z_B가 각각 소모하는 전력량을 비교하면 다음과 같다.

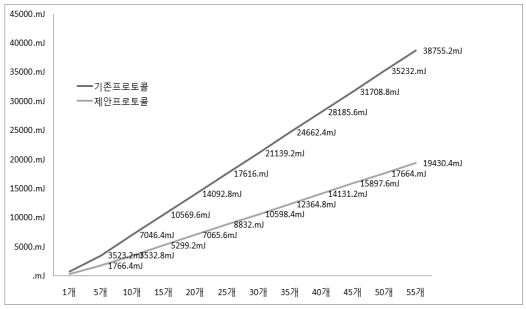


〔그림 9〕 장치별 전력소모량

〔그림 9〕처럼 제안프로토콜이 표준프로토콜에 비하여 전력소모량이 적은 것을 확인할 수 있다. 특히 TC와 Z_B는 표준프로토콜에 비하여 적은 전력을 사용한다는 것을 확인할 수 있다.

단, 〔표 6〕이나 〔그림 9〕에서의 수치들은 장치 1개를 기준으로 한 것이다. ZigBee는 네트워크는 여러 개의 장비가 추가되기 때문에 여러 대의 장비가 추가된 상황도 가정하여 비교해 보아야 한다. 장치수의 증가에 따른 에너지 소모량의 차이를 계산하여 그래프로 표현하면 다음과 같다.

이처럼 장치의 개수가 증가할수록 사용되는 에너지



〔그림 10〕 장치 개수별 전력소모량

양의 차이는 더 크게 난다. 전체적인 차이를 비교할 때 제안프로토콜이 표준프로토콜에 비하여 50%의 전력만을 사용하는 것을 볼 수 있다. 비율로만 생각한다면 50%지만 소모되는 에너지의 수치로 본다면 차이는 더욱 크게 벌어진다. 〔그림 10〕는 55개까지만 계산하였지만 ZigBee에서는 하위에 추가할 수 있는 장치의 최대수가 255대이기 때문에 수치상의 차이는 더욱 커지는 것을 확인할 수 있다. 255개의 상황을 가정하였을 때 표준프로토콜의 전력소모량은 179683.2mJ의 전력을 소모하며, 제안프로토콜은 90086.4mJ의 전력을 소모한다. ZigBee는 적은 에너지 사용을 목표로 하기 때문에 이런 에너지사용량의 차이는 장치의 배터리 수명과 관련하여 큰 차이로 돌아올 수 있기 때문에 소모되는 전력량이 줄었다는 점에서 의미가 있다.

VI. 결론

ZigBee는 활용되는 분야인 스마트그리드와 WBAN에서 중요한 정보를 전달하는 역할을 맡고 있다. 따라서 보안은 매우 중요한 부분이며, 표준명세서에도 보안에 관련된 계층 및 필드를 별도로 명시하고 있다. 그러나 ZigBee는 탈퇴 command의 전달과정에서 command자체를 위조할 수 있는 보안 위협이 발생할 수 있으며, 위조가 된 command를 식별해 낼 수 있는 방법이 없다. 본 논문에서는 이를 해결하기 위하여 가입 및 인증과정에서부터 ZigBee Router와 말단 장치 사이에 두 장치만이 공유하는 LK를 별도로 설정함으로써 이러한 보안취약점에 대한 문제를 해결하고, 표준프로토콜에서의 추가키 분배과정을 인증과정에 접목시킴으로써 더 나은 에너지 효율을 가지는 새로운 프로토콜을 제안하였다. 인증과정에서 Time Stamp를 활용하여 AP-LK를 생성하여 NK의 사용

을 대체시켰고, 이를 통하여 command를 전달한 장치가 어떤 장치인가를 구분해내어 command의 위조를 방지하였다. 또한 피해가 발생하더라도 피해범위는 해당 장치만 피해를 입을 뿐 네트워크내의 다른 장치들은 피해가 없도록 개선하였다.

참고문헌

〔1〕 ZigBee Alliance, "ZigBee-2007 Specification," ZigBee Document 053474r17, JAN. 2008.

〔2〕 IEEE Computer Society, "IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific Requirements Part 11," IEEE Standards, pp.1-25 March. 2012.

〔3〕 Ender Yüksel, Hanne Riis Nielson, Flemming Nielson, "ZigBee-2007 Security Essentials," Proceedings of The 13th Nordic Workshop on Secure IT Systems NordSec, pp.65-82 October. 2008.

〔4〕 임준현, 한규석, 김광조, "ZigBee WPAN에서의 안전한 키 관리기법과 인증 프로토콜," CISC-S'10 Proceedings, pp.249-254 June. 2010.

〔5〕 김봉환, 임정미, 박창섭, "Analysis of ZigBee Security Mechanism," 보안공학연구논문지 vol.9, No.5, pp.417-430 September. 2012.

〔6〕 Shahin Farahani, "ZigBee WIRELESS NETWORKS AND TRANSCEIVERS," ELSEVIER/Newnes, 2008

〔7〕 Ender Yüksel, Hanne Riis Nielson, Flemming Nielson, "A Secure key Establishment Protocol for ZigBee Wireless Sensor Networks," The Computer Journal, Vol.54, No.4, pp.589-601 November. 2011.

〔8〕 오수민, 최수경, 권예진, 박창섭, "ZigBee 무선 센서 네트워크에서의 안전한 키 분배 프로토콜," 한국정보보호학회논문지 vol.22, No4, pp.745-759 August, 2012.

〔9〕 P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen and S. Carlsen, "ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys," Proceedings of the 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 465-470, Nov. 2010.

〔10〕 H. Li, Z. Jia and X. Xue, "Application and Analysis of ZigBee Security Services Specification," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 494-497, Apr. 2010.

〔11〕 G. Dini and M. Tiloca, "Considerations on Security in ZigBee Networks," Proceedings of the 2010 IEEE International Conference on SUTC, pp.58-65, Jun. 2010.

〈저 자 소 개〉

김 봉 환 (Bong-hwan Kim) 학생회원
2012년 2월: 단국대학교 컴퓨터과학과 졸업
2012년 2월~현재: 단국대학교 전자계산학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안

박 창 섭 (Chang-seop Park) 종신회원
1983년 2월: 연세대학교 경제학과 졸업
1987년 2월: Lehigh University 컴퓨터과학과 석사
1990년 2월: Lehigh University 컴퓨터과학과 박사
1990년 3월~현재: 단국대학교 컴퓨터과학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 무선 인터넷 및 모바일 컴퓨팅 보안, 금융보안