스마트 그리드 네트워크에서 효과적인 Zigbee 인증 프로토콜에 관한 연구

정회원 임 송 빈*, 오 영 환*

A Study Effective Zigbee Authentication Protocol in Smart Grid Network

Song-Bin Im*, Young-Hwan Oh* *Regular Members*

요 약

고압 전력망과 IT 영역에서 응용되고 있는 스마트 그리드 네트워크(Smart gird networks)는 정보의 도청이나, 비정상적 패킷의 유통, 메시지의 재사용 등 데이터의 위·변조와 같은 외부의 공격에 쉽게 노출되는 환경에서 동작하기 때문에, 보안은 필수적으로 갖추어져야 하는 중요한 기능이다. 저전력, 초소형 저비용 장점을 갖는 Zigbee는 스마트 그리드 네트워크를 구현하는 최적의 기술로 주목받고 있다. 스마트 그리드 네트워크가 효율적으로 사용되기 위해서는 수집된 정보는 많은 경우에 네트워크 상에서 적들로부터 보호가 요구된다. 네트워크 상에서 수집되는 정보에 보안 매커니즘이 적용되어야 한다. 그러나 Zigbee 프로토콜은 보안에 취약점을 지니고 있다. 본 논문에서는 스마트그리드의 대표적인 예로 Zigbee 보안 시스템이 가지고 있는 문제점들을 자세히 분석하고, 이를 해결하여 스마트 그리드에 적합한 보안 프로토콜을 새롭게 제안하고 그 효율성을 비교·분석한다

Key Words : SmartGrid, ZigBee security, authentication, key management, Hamming Distance

ABSTRACT

Security is critically important for smart grid networks that are usually used for the electric power network and IT environments that are opened to attacks, such as, eavesdroping, replay attacks of abnormal messages, forgery of the messages to name a few. ZigBee has emerged as a strong contender for smart grid networks. ZigBee is used for low data rate and low power wireless network applications. To deploy smart grid networks, the collected information requires protection from an adversary over the network in many cases. The security mechanism should be provided for collecting the information over the network. However, the ZigBee protocol has some security weaknesses. In this paper, these weaknesses are discussed and a method to improve security aspect of the ZigBee protocol is presented along with a comparison of the message complexity of the proposed security protocol with that of the current ZigBee protocol.

Ⅰ. 서 론

전력망에 통신망을 접목시켜 전력계통시스템의 제어를 통하여 발전·송전·배전의 전 과정에 대한 통제가 가능하여 지고, 결과적으로 에너지 사용의 효율성을 높이고자 하는 것이 에너지 인터넷이라고 불리는 지능형 전력망(Smart Grid)의 목표이다. 즉 기존 전력망에 정보 기술(IT)을 융합하여 전력 공급자와 소비자가 양방향으로 실시간으로 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이라고 할 수 있

* 광운대학교 전자통신공학과 통신망 연구실 (songbine@hotmail.co.kr)
논문번호 : KICS2010-11-575, 접수일자 : 2010년 11월 30일, 최종논문접수일자 : 2011년 2월 23일

다. 지능형 전력망의 핵심기술로는 첨단 검침 인프라(AMI: Advanced Meter Infrastructure), 첨단 송배전 자동화, 분산 발전, 전기자동차 충전 하부구조 및 재생 에너지 발전 등이 있다. AMI는 지능형 전력망, 통신 하부구조 및 지원 정보 하부구조의 융합으로 이루어진다.[1-3]

현재 스마트 그리드 환경에서는 그림 1과 같이 고객구내 Smart 기기 연결을 위한 HAN(Home area network)과 SUN(Smart energy Utility Network)으로 나눠진다. SUN은 크게 소비자와 전력회사를 연결해 주는 통신망으로서 수십에서 수백가구를 연결하는 NAN(Neighborhood Area Network)과 장거리 전송을 위한 WAN(Wide Area Network)으로 구성된다.

통신방식으로는 광케이블, WiMAX, D-TRS, PLC, Zigbee, B-CDMA, RF등 다양하게 적용되고 있다. 이 중 ZigBee는 스마트 그리드의 일부로서 이미 표준화를 주도하고 있고 건물 내의 무선 네트워크 시장에서 적용 중이며, 국제전기위원회(IEC)에서 이미 승인을 받았다.[4-6]

스마트 그리드 환경에서 NAN에서 주로 적용하고 있는 Zigbee[16]는 IEEE 802.15.4[17]의 물리 계층(Physical layer)과 매체 접근 제어 계층(Medium access control layer)을 도입하여 네트워크 계층부터 새롭게 정의한 산업체 동맹이 작성한 표준으로 다른 무선 통신 기술과 달리 전력 소모가 적고, 저가 제품의 구현이 가능하여 지능형 홈 네트워크 빌딩 등의 근거리 통신시장과 산업용기기 자동화 물류 환경 모니터링 휴먼인터페이스를 텔레매틱스 군사 등의 다양한 응용에 적합한 기술이다. 또한 ZigBee 통신은 반경 100m안 1에서 250kbps의 속도로 데이터를 전송하고

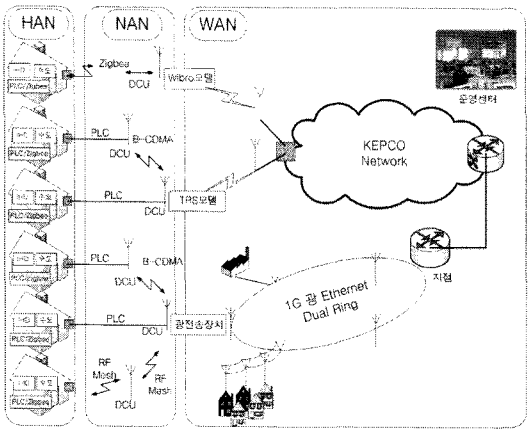

그림 1. 통신망 및 운영센터 구조
Fig 1. Architecture of communications network and Operation Center architecture.

멀티 홉(Multi-hop) 기능이 지원되어야 65000개 이상의 노드(Node)를 연결할 수 있어 확장성 있는 네트워크를 구성하는 것이 가능하다. 다대다(N-to-M) 통신인 그물망(Mesh) 으로 이루어진 확장된 네트워크에서는 공격자에 의한 데이터의 위·변조에 대응하기 위하여 노드들의 상호인증과 데이터 암호화가 중요하며 이때 사용되는 키 관리도 매우 중요한 보안요소 중 하나이다.

정보 유출이나 불법적인 침입자로 인한 도청 및 위·변조를 막기 위해서 ZigBee 128비트의 AES(Advanced encryption standard) 대칭키 암호방식[8]을 이용하여 두 노드간의 키 관리(Key management), 키 설정(Key establishment), 키 전송(Key transport)과 인증(Authentication) 과정을 수행하고 이 키를 이용하여 매체 접근 제어 계층, 네트워크 계층(Network layer), 응용 계층(Application layer)에서의 데이터 프레임에 대한 보안 기능을 제공한다. 그러나 ZigBee 보안시스템은 심각한 문제들을 가지고 있다. ZigBee는 신뢰센터(Trust center)라는 개념을 이용하여 네트워크상의 노드들의 키를 분배하고 노드간의 단대단(End-to-end) 보안을 가능하게 한다. 그리고 노드 사이의 비밀 키는 중간 노드들의 중계에 의하여 전달된다. 그러나 이때의 중간 통신채널의 안전성을 ZigBee 보안시스템에서는 완벽히 보장하지를 않는다. 이는 스마트그리드 환경에서 비밀 키의 안전성의 보장이 가장 중요한 대칭키 암호기반의 ZigBee에서의 심각한 문제가 된다. 또한 대칭키 암호시스템을 사용하는 ZigBee 시스템에서는 신뢰센터가 통신하는 모든 노드들의 비밀 키를 관리하도록 되어 있는 구조적인 약점을 가지고 있다.

본 논문에서는 위에서 언급한 ZigBee 보안시스템이 가지고 있는 여러 문제점들을 자세히 분석한다. 그리고 분석된 문제점들을 해결하고, 좀 더 신뢰성 있는 ZigBee 보안 프로토콜 알고리즘을 새롭게 제안한다. 제안하는 프로토콜은 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 암호방식[9]과 HD(Hamming Distance)[19]의 개념을 도입하여 신뢰할 수 있는 노드의 인증서를 바탕으로 다른 노드의 인증서를 검증하기 위해 필요한 인증서 경로구축을 보장할 수 있는 인증 프로토콜을 제안한다.

Ⅱ. SmartGrid ZigBee 취약성 분석

2.1 ZigBee 보안

ZigBee는 근거리통신을 지원하는 IEEE 802.15.4 표준중 하나를 말한다. 가정, 사무실, 산업현장 등의

무선 네트워킹 분야에서10~1100m 내외의 근거리 통신과 유비쿼터스 컴퓨팅을 위한 기술이다. ZigBee는 휴대전화 나 무선 LAN의 개념으로 기존의 기술과 다른 특징은 전력소모를 최소화하는 대신 소량의 정보를 소통시키는 무선 센서 네트워크 표준이다. ZigBee 네트워크는 지능형 홈 네트워크 빌딩 등의 근거리 통신시장과 산업용 기기자동화, 물류, 환경 모니터링, 휴먼 인터페이스, 텔레매틱스, 군사 등에 활용된다.

최근 전력 소모량이 적고 값이 싸 홈 네트워크 등 유비쿼터스 구축 솔루션으로 각광 받고 있다. 2003년 IEEE는 저가격, 저 전력과 간단한 네트워크 구조를 갖는 WPAN 기술을 정의하는 802.15.4를 발표하고, 2005년 ZigBee 얼라이언스(Alliance)는 IEEE 802.15.4에 네트워크·보안계층을 추가로 정의하여 ZigBee 표준화 스펙버전 1.0을 발표했다. 보안 특성으로 128bit 키의 AES-CCM*를 지원하여 데이터의 기밀성과 무결성을 보장한다. 또한 스마트 그리드에서의 활용을 위해 HAN(Home Area Networks) 영역에서의 지능형 에너지 관리를 위한 무선 통신 기술 연구가 진행되고 있다.[20]

ZigBee는 IEEE 802.15.4의 물리층과 매체접근제어층 위에 네트워크 계층과 응용 지원부 계층(APS: Application support sublayer), 응용 프레임워크(Application framework), ZigBee 디바이스 객체(ZDO: ZigBee device object)를 포함하는 응용 계층(Application layer)으로 구성된다. ZigBee 스택 구조를 살펴보면 그림 2와 같다.

응용 계층은 응용 프레임워크 ZDO, APS 사이의 인터페이스를 정의한다. 응용 프레임워크는 응용에 의해서 사용되는 주소 체계에 대한 내용과 응용들 간의 통신 원리에 대하여 기술을 하고, ZDO는 응용 객체

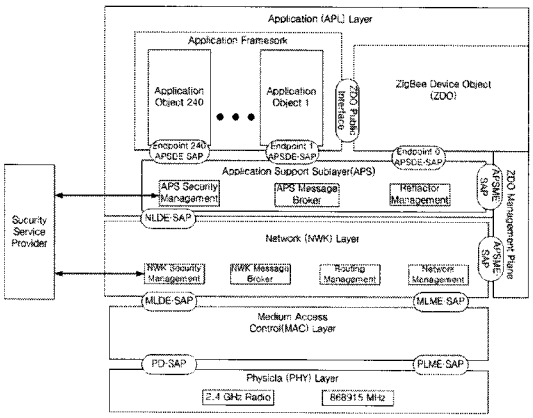

그림 2. ZigBee 스택 구조
Fig 2. Architecture of ZigBee stack.

의 디바이스 제어와 디바이스간의 바인딩 처리 및 보안 관계를 설정 해주고 응용 객체의 공용 인터페이스를 제공한다. 그리고 APS는 바인딩을 위한 테이블을 유지·관리한다. 네트워크 계층에서는 네트워크 보안 라우팅을 관리하고 연결된 디바이스간의 메시지를 전달하며 APS의 보안 관리를 지원한다. ZigBee 네트워크 계층은 네트워크에 합류(Join) 또는 이탈(Leave)하는 등의 메커니즘 전송 프레임에 대한 보안을 제공한다. ZigBee 보안서비스는 네트워크 계층과 응용 계층과 직접적으로 연관되어 있다. 네트워크 계층과 응용 계층에서 생성되는 프레임은 각층에서 데이터 암호화 및 무결성 검증을 위한 연산을 수행하도록 되어있고 이러한 기능을 담당하는 보안 서비스 제공자(SSP: Security service provider)가 모듈 형태로 존재한다. ZigBee의 보안 서비스는 대칭키 암호방식을 이용하여 두 노드간의 비밀 키 설정과 인증과정을 수행하고 이 키를 이용하여 매체 접근 제어 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 보안 기능을 제공한다. ZigBee에서 보안을 위해 사용되는 키는 마스터 키(Master key), 링크 키(Link key), 네트워크 키(Networkkey)의 세 종류의 키가 있다. 각 노드들은 링크 키를 이용하여 일대일(Point-to-point) 비밀 통신을 하고, 네트워크 키를 이용하여 그룹 비밀통신을 한다. 마스터 키는 링크키를 생성하기 위해 사용되는 비밀키이며, 생성된 링크키를 사용하여 네트워크 키를 안전하게 전송한다.

2.2 ZigBee에서의 새로운 디바이스의 키 설정 과정

ZigBee 네트워크는 코디네이터Coordinator), 라우터(Router), 엔드디바이스(End device)의 세 종류의 노드로 구성되어 있고 보안에서 가장 중요한 신뢰센터의 역할을 코디네이터가 하도록 정의하고 있다[6]. 코디네이터는 암호화를 위한 키 분배 및 관리 인증 등의 네트워크의 host 역할을 하며 라우터는 네트워크 구성을 위한 라우팅을 수행한다. 그리고 엔드디바이스는 라우터를 통해서 또는 신뢰센터와 직접 데이터를 주고 받을 수 있다. ZigBee 네트워크의 장점 중 하나는 새로운 디바이스를 쉽게 합류할 수 있다는 것이다. 새로운 디바이스는 네트워크를 제어하는 코디네이터에 간단한 요청을 통하여 합류될 수 있다. 즉, 네트워크에 진입한 디바이스는 먼저 비컨(Beacon) 메시지를 전송하여 합류를 위한 노드를 찾고, 선택한 라우터를 통하여 코디네이터와 메시지를 주고 받는다. 비컨메시지는 자신의 전파범위 내에 존재하는 라우터 노드들

에게 원 홉(One-hop)으로 브로드캐스트 된다. 새로운 디바이스의 합류를 위하여 코디네이터는 디바이스에게 마스터 키를 전달하고, 이 키를 이용하여 코디네이터와 디바이스간의 새로운 링크 키를 생성한다. 그리고 생성된 링크 키를 이용하여 디바이스는 네트워크 키를 안전하게 전송받아 네트워크에 성공적으로 합류하는 것이다. 그림 3는 새로운 디바이스가 코디네이터로부터 네트워크 키를 분배받는 과정을 나타낸 것이다. ZigBee에서는 디바이스가 네트워크 키를 얻으면 합류가 된 것이다.

네트워크에 합류하고자 하는 새로운 디바이스가 네트워크 키를 안전하게 전송받는 방법을 자세히 살펴보면 다음과 같다.

1. 디바이스가 네트워크에 연결되면 라우터는 코디네이터에게 업데이트 디바이스 명령을 보낸다.
2. 업데이트 디바이스 메시지를 받은 코디네이터는 새로운 디바이스가 네트워크에 참여되어도 되는지의 합류 여부를 판단한 후 디바이스에게 네트워크 키를 분배하는 과정을 다음과 같이 진행한다. 이때, 라우터는 중간에서 중계역할을 한다.
   i) 코디네이터는 마스터 키를 디바이스에게 전송한다.
   ii) 코디네이터와 디바이스는 마스터 키를 이용하여 SKKE(Symmetric-key key establishment) 프로토콜을 수행하여 링크 키를 생성한다.
   iii) 코디네이터는 링크 키를 이용하여 네트워크 키를 암호화한 값을 디바이스에게 전송한다.
   iv) 디바이스는 링크 키를 이용하여 코디네이터에게 전송받은 데이터로부터 네트워크 키를 획득한다.

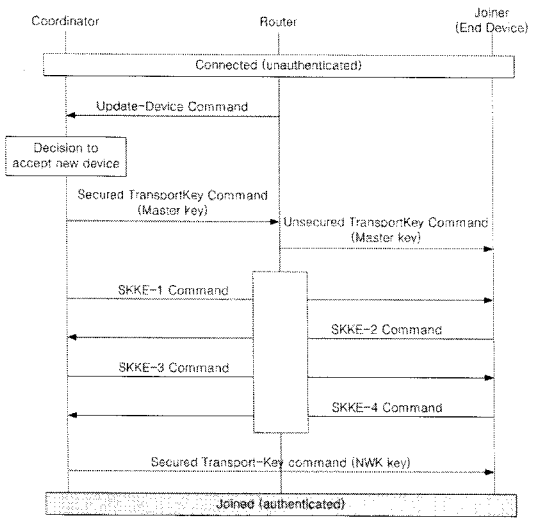

그림 3. ZigBee 네트워크에서의 키 설정 과정
Fig 3. Key establishment process in ZigBee network.

2.3 ZigBee 네트워크의 취약성 분석

저전력, 초소형, 저비용의 장점과 함께 ZigBee는 유비쿼터스 센서네트워크를 구현하는 최적의 기술로 주목받고 있다. 그러나 현존하는 ZigBee 네트워크는 다음과 같은 문제점들을 가지고 있다.

1. 코디네이터는 네트워크 키는 물론 네트워크에 합류한 모든 노드들의 개수만큼의 마스터키와 링크키를 다 가지고 있어야 할 뿐만 아니라 앞으로 통신하게 될 모든 노드들의 마스터키까지 전부 가지고 있어야 한다. 그렇기 때문에 네트워크 상의 노드수가 증가할수록 이에 비례하여 더 많은 저장 공간이 요구되는 키 관리상의 구조적 단점이 존재한다.
2. 코디네이터는 네트워크에 최초로 합류하는 디바이스들의 정당성에 대하여 확인을 해야 한다. 그러나 코디네이터에게는 그들의 정당성 유무에 대해 판별할 아무런 근거가 존재하지 않기 때문에 외부의 부정한 디바이스가 네트워크에 합류하게 될 여지가 된다. 최초로 합류하는 디바이스에 관련된 인증의 부재는 ZigBee 보안시스템의 심각한 문제점이다.
3. 만약 새롭게 합류하는 디바이스가 마스터 키를 가지고 있지 않다면 그림 3에서와 같이 코디네이터는 마스터 키를 디바이스에게 전송해야 하는데 이 과정에서 중계역할을 하는 라우터와 디바이스 사이에 안전한 채널이 확보가 되어 있지 않기 때문에 마스터키는 그대로 외부로 노출이 되어 버린다. 마스터 키가 노출이 되면 이 후에 수행될 통신채널의 안전성 여부와는 상관없이 누구든지 생성되는 링크 키 뿐만 아니라 네트워크 키까지도 알 수 있게 되어버리기 때문에 네트워크 전체 보안이 무력화 되어버린다. 그러므로 마스터 키의 노출 또한 ZigBee 보안시스템의 심각한 문제점이 된다.
4. 새롭게 네트워크에 합류하려는 모든 디바이스마다 코디네이터와 연결하여 마스터키, 링크 키와 네트워크 키를 전송받도록 함으로써 모든 트래픽이 코디네이터로 집중된다. 그렇게 때문에 만약 네트워크에 합류하려는 노드 수가 많아진다면 코디네이터에 부하가 치중되어 통신시간이 길어져 네트워크 시스템의 성능이 저하되는 문제점이 있다.

Ⅲ. 제안하는 방식

이 장에서는 Ⅱ장에서 분석한 ZigBee 네트워크의 문제점들을 개선한 새로운 ZigBee 프로토콜을 제안한다. 제안하는 프로토콜은 코디네이터의 키 관리를 간단히 하기 위하여 시스템 ID 자체를 공개키로 이용할 수 있는 개인 식별 방식의 공개키 암호방식[9]을 적용하였다. ZigBee에서 각 노드들은 네트워크 내에서 유일한 주소를 부여 받으며 자신만의 주소를 부여 받은 노드들은 이 주소를 통해 네트워크 내에서 독립적인 개체로 존재한다. 또한 노드의 인증서 경로의 hop 수와, 각 노드의 저장소 크기를 줄이기 위하여 Hamming Distance 방법을 이용하였다. 3. 1절의 (정의 1)과 (정의 3)을 이용하여 하나의 노드가 관리하여야 하는 네트워크내의 노드 수를 $\log_2 N$ 으로 제한하였다.

그리고 제안하는 프로토콜은 공개키 암호방식이 가지고 있는 계산량의 문제를 해결하기 위하여 Zigbee의 링크 키와 네트워크 키에서 사용하고 있는 128-AES 대신에 타원곡선 암호[10-14]를 기반으로 하여 설계한다. 타원곡선암호는 유한체에서 설계된 기존의 암호방식[15-17]과 비슷한 레벨의 보안성을 제공하면서도 훨씬 적은 키 사이즈를 요구하기 때문에 센서 네트워크에 충분히 적용 가능한 공개키 암호방식으로 알려져 있다[18]. 그림 4는 본 논문에서 새로운 디바이스가 라우터로부터 네트워크 키를 분배 받는 과정을 나타낸 것이다.

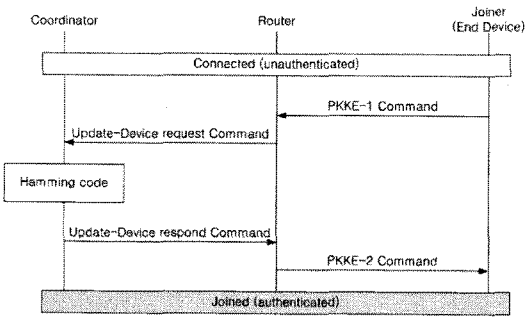

그림 4. SmartGrid ZigBee 네트워크에서 제안한 키 설정 과정
Fig 4. Proposed Key establishment process in SmartGrid ZigBee network.

3.1 개념 및 정의

본 논문에서는 각 노드의 공개키 인증서 저장소(이하, 저장소) 크기를 줄이고 공개키 인증서 경로구축이 가능하도록 하기 위하여 Hamming Distance(이하, HD)의 개념을 도입하였기 때문에, 우선 두 정수사이에 HD가 가지는 특성을 설명한다. 위에서 제기된 임의의 두 정수사이의 HD는 다음과 같은 특성을 가진다.

(정리 1) $a \in Z_N$이고 $R_a = \{x \in Z_n | HD(a,x) = 1\}$이면 $|R_a| = \log_2 N$, 여기서 $Z_N = \{0, 2, \cdots, N\text{-}1\}$, $N = 2^m, m > 0$.

(증명) 임의의 정수 $a \in Z_N$에 대하여 Z_N내의 a와 HD가 "1"인 정수의개수를 찾는 것은 Z_N내의 정수 중에 "0"과 HW(Hamming Weight)가 "1"인 정수의 개수를 찾는 것과 같다. 정수 "0"과 HW가 r인 정수의 수는 ${}_mC_r$(combination)로 계산될 수 있다. 여기서 m은 $\log_2 N$을 의미한다. 따라서 임의의 정수 a에 대하여 HD가 "1"인 정수의 수는 ${}_mC_1$로 $m(=\log_2 N)$과 동일하다.

또한, 본 논문에서 제안하는 프로토콜에 대한 설명의 편의를 위하여 다음과 같은 정의를 사용한다.

(정의 1) SmartGrid Zigbee 네트워크 내의 임의의 인증서 ID(Identification Number)는 Z_N의 원소이고, 네트워크 최대 크기를 N으로 정의한다.

(정의 2) 두 노드 a와 b의 공개키 인증서 ID를 각각 $a_{ID}(\in Z_n)$ 와 $b_{ID}(\in Z_n)$ 로 정의하고 이들 인증서 ID 간의 HD를 HD(a,b) 또는 HD로 정의한다.

(정의 3) SmartGrid Zigbee 네트워크내의 임의의 노드 a는 인증경로 구축을 위하여 네트워크 내의 노드들 중 일부의 공개키 인증서를 자신의 저장소에 관리하게 된다. 이때, 노드 a를 PN(Parent Node)이라 정의하고 PN의 저장소에 저장되어 관리되는 노드들의 집합을 CN(Child Node)이라고 정의한다. 그리고 CN 중의 하나를 CN_i라 정의한다. PN과 CN_i의 공개키 인증서 사이에 $HD(PN_i, CN_i)=1$인 관계가 성립하도록 각 노드의 ID를 구성한다.

(정의 4) 노드 a가 노드 b를 인증하고자 할 때, 노드 b에서 노드 a까지 인증경로 $Auth_p(a \rightarrow b)$로 정의한다. 이 때, 노드 a를 T_n이라 하고 노드 b를 V_n이라 정의하자. 또한 T_n과 V_n 사이에 인증경로가 찾으려는 시도가 존재한다면 $Auth_p(T_n \rightarrow_{sucess} V_n)$로 정의한다.

노드ID	000	001	010	011	100	101	110	111
000		●	●		●			
001	●			●		●		
010	●			●			●	
011		●	●					●
100	●					●	●	
101		●			●			●
110			●		●			●
111				●		●	●	

그림 5. ID들의 집합(HD=1)
Fig 5. IDs set(HD=1).

본 논문에서 사용한 인증서 경로 알고리즘을 이용할 때 인증서 경로의 길이는 $2\sqrt{N}$보다 작게 된다. 노드의 유연성을 보장하기 위하여 다음과 같은 방법을 이용하였다.

① 노드들 간의 사전 조율(negotiation)을 통해 현 네트워크에 존재하는 노드의 수(N_r)를 결정하고, 이에 따라 네트워크의 크기 N을 결정한다. 이때, N과 N_r은 N/2 ≤ N_r ≤ N-1의 관계가 성립되도록 한다.
② 네트워크 내의 실제 존재하는 노드들을 대상으로 순차적으로 ID를 부여받는다.
③ 노드의 이동으로 인하여 네트워크내의 실제 존재하는 노드의 수(N_r)가 N/2 이하로 되면 최대 네트워크 사이즈를 N/2 으로 변경한다. 이때, N/2 이상의 ID를 가지고 있는 노드는 N/2 이하의 ID로 재할당받아야 한다.
④ 만약 네트워크내의 노드의 크기가 N이상이 되면 해당 노드는 (N, N+1,...) 순으로 ID를 부여하고 해당 ID와 HD가 "1"인 노드들과 공개키 인증서를 교환한다. 물론 네트워크의 크기도 N에서 2N(=2^{m+1})로 변경된다.

위에서 설명한 특성들에 대하여 그림 6을 통하여 간략하게 설명한다. 그림 6을은 N=8인 정수의 집합에 대하여 HD가 "1"인 정수들 사이의 관계를 나타낸다. 즉, 정수 "001"과 HD가 1인 정수는 {"000". "011". "101"}등 3개(=$\log_2 8$)이다. 이는 '정리1"과 일치한다. 이 때, PN의 ID는 "001"이라면 CN의 ID들은

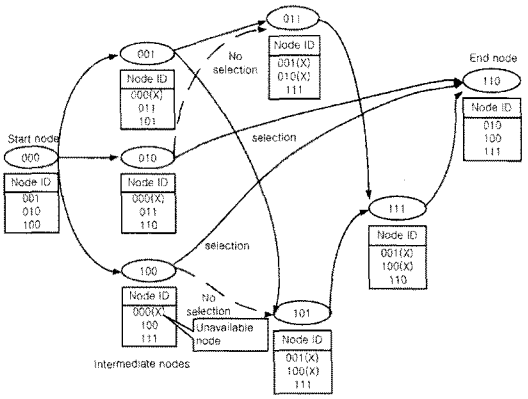

그림 6. 신뢰 경로
Fig 6. Certificate path.

{"000". "011". "101"}등 3개가 존재한다. 즉, R_{001}은 {"000". "011". "101"}이 된다. 정리 1과 정리3에 의하여 임의의 PN은 $\log_2 N$개의 노드에 해당하는 공개키 인증서만을 자신의 저장소에 관리한다.

즉, 그림 6에서 인증서 ID로 "001"을 부여받은 노드는 {"000". "011". "101"}에 해당하는 노드의 공개키 인증서만을 관리한다. 그림 6에서 "unavailable node"는 존재했던 ID를 의미하고, "selection"은 인증서 경로를 가장 짧게 하는 노드의 선택을 의미한다.

3.2 제안한 인증서 경로구축 알고리즘

신뢰경로란 PN이 CN에게 공개키 인증서를 발급하고, 이 CN은 각각의 하위 CN에게 공개키 인증서를 발급하여 모든 노드 간에 계층적으로 신뢰구조를 구성하는 것을 의미한다.

인증서 경로구축 알고리즘은 T_n부터 V_n까지 신뢰경로를 찾는 것을 말한다. 즉, 그림 7에서 보듯이

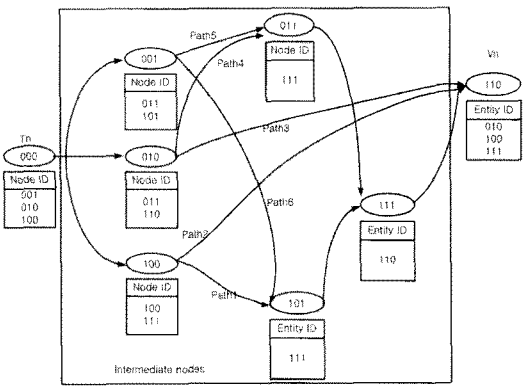

그림 7. T_n과 V_n 사이의 신뢰경로
Fig 7. Certificate path between T_n and V_n

T_n(000)부터 V_n(110)까지는 6개의 경로가 존재한다. 이들 중 하나의 경로가 T_n부터 V_n까지 구축되고, 경로에 존재하는 인증서에 이상이 없는 것으로 확인된다면 T_n은 V_n을 신뢰하게 된다.

본 논문에서는 이러한 신뢰경로를 구축하기 위하여 각 노드의 저장소 정보(CN)와 앞 절에서 설명한 HD의 특성을 이용하여 T_n부터 V_n까지 인증서 경로를 찾는 알고리즘을 그림 8과 같이 제안한다.

우선, 그림 8에서 사용하고 있는 용어들에 대하여 간단히 설명한다. path_nodes는 인증서 경로구축 과정에서 T_n부터 V_n까지 인증서 경로에 존재하는 공개키 인증서들의 집합을 나타낸다. 네트워크에서 실제 노드의 수는 n_r로 표시되고, empty_nodes는 네트워크에 사용하지 않는 ID들의 집합을 나타낸다. 본 논문에서 제안한 알고리즘은 PN의 CN에 대하여 V_n과 HD를 계산하는 부분과 HD가"1"이 아닌 경우 PN의 CN_i들 중의 하나를 선택(SN)하여 다음 PN으로 삼는 부분으로 나누어진다. 우선, HD(PN, V_n)=1이면 경로구축 알고리즘은 성공적으로 종료된다. 그렇지 않은 경우, PN의 CN에 대하여 HD(CN_i, V_n)=1을 만족하는 CN_i가 존재해도 역시 알고리즘은 성공적으로 종료된다. 여기서 $i=0,1,...,\log_2 N-1$. 만약, 모든 CN_i에 대하여 HD(CN_i, V_n)$\neq 1$ 이라면 CN_i들 중의 하나를 랜덤하게 선택하여 이를 새로운 PN으로 삼고, 이 PN의 CN을 이용하여 HD(CN_i, V_n)=1을 만족하는지 확인한다. 이러한 계산을 반복하여 수행하면 V_n까지의 인증서 경로를 찾을 수 있다. 물론 경로를 구축할 수 없는 경우도 존재한다. 또한, 네트워크의 크기는 N(=2^m)이지만 실제 존재하는 노드의 수 (n_r)는 N보다 작기 때문에 경로가 존재하지 않거나 경로가 존재함에도 불구하고 경로를 찾지 못하는 경우에 대비하여 다시 경로를 찾는 방법 등을 포함 한다. 즉, 그림 8에서 경로가 존재하지 않는 경우를 대비하여 exit_count를 정의하였고, 경로를 찾지 못하는 경우 경로구축 알고리즘을 반복적으로 수행하기 위하여 rep_count와 중지조건 C를 정의하였다.

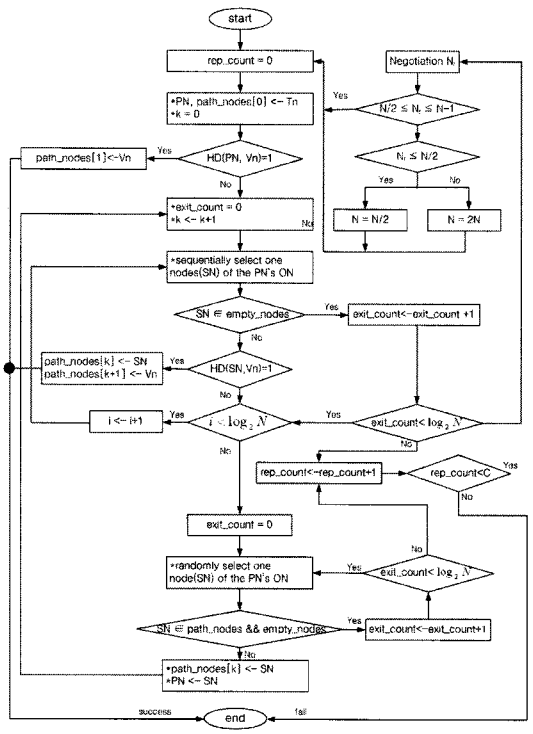

그림 8. 제안한 신뢰 경로 알고리즘
Fig 8. Proposed Certificate path algorithm.

그림7에서 T_n {"001", "010", "100"}등 3개의 노드에 공개키 인증서를 발행하였고, 이들을 자신의 저장소에 관리한다. 이때, T_n이 PN이 되고 {"001", "010", "100"}이 된다. 경로구축을 위해 T_n는 자신이 직접 V_n(110)에게 공개키 인증서를 발행하지 않았다면, 매개노드를 이용하여 V_n까지 경로를 찾는다. 이때, 다음 프로세스를 진행하기 위한 PN은 자신의 CN_i들 중에 하나를 랜덤하게 선택한다. 즉, {"001", "010", "100"}의 노드 중에 하나를 다음으로 선택한다. 만약 다음 PN으로 "010"을 선택하게 되면 경로구축(경로: "000" → "010" → "110")은 완료되지만, 다음 PN으로 "001"을 선택한다면 경로는 완료되지 못하고 해당 CN_i("011" 또는"101")들 중의 하나를 그 다음 PN으로 선택하여야 한다. 이때 PN으 로 "011"이 선택되면 경로는 "000" → "010" → "011" → "111" → "110" 로 완성된다.

Ⅳ. 성능평가

제안하는 프로토콜은 기존에 사용하였던 마스터 키를 없애고, Hamming distance를 이용하여 저장소 크기를 줄여, 비밀 키 개수와 통신횟수를 감소시킴으로써 효율성은 물론 안전성까지 개선시켰다. 또한, 인증경로 구축 시 나머지 노드는 중개 노드로 활용함으로써 각 노드가 자신의 저장소에서 직접 관리하여야 하는 노드 정보의 수를 log2N으로 줄이고, 인증서 경로의 길이를 보다 작게 할 수 있는 새로운 인증서 경로

구축 알고리즘을 제안하여 하였다.

그리고 코디네이터가 자신의 비밀 키와 네트워크 키, 그리고 자신과 직접 연결된 노드간의 링크키만 관리하도록 함으로써 코디네이터의 키 관리를 간편화하였고, 네트워크에 합류하려는 새로운 디바이스는 가까운 위치에 있는 라우터로부터 직접 네트워크 키를 전송 받을 수 있도록 설계하여 기존의 코디네이터로 집중되었던 트래픽을 여러 라우터에게 분산시킴으로써 네트워크의 부하를 해결하고 디바이스의 네트워크 합류시간을 감소시켜 네트워크의 효율성을 향상시켰다. 또한 디바이스가 가까운 위치에 있는 라우터로부터 직접 네트워크 키를 전송 받을 수 있도록 설계하였기 때문에, 제안하는 방식은 다중 멀티 홉(Multi-hop) 환경. 적용될 경우에 더욱 더 효율적인 인증 프로토콜이다.

ZigBee 네트워크는 스타, 트리, 메쉬 토폴로지를 지원한다. 본 논문에서는 메시지의 복잡도를 비교하기 위해서 CN이 2개인 2진 트리 구조의 네트워크와 임의의 위치에 노드를 생성하고 이에 따라 임의로 생성된 네트워크에서 키 분배를 위한 메시지 개수를 비교한다. 임의로 네트워크를 형성할 때 일정한 영역의 중심에 코디네이터 노드를 두고 코디네이터에서 가까운 노드가 첫 번째로 네트워크에 연결된다. 프로토콜의 성능을 측정하기 위해서 메시지 복잡도[24]를 이용하였다. 그림 9는 기존의 ZigBee 프로토콜과 제안한 프로토콜의 키 분배 방식에 대한 메시지 복잡도를 비교한 것이다.

그림 10은 위의 방법으로 만들어진 트리구조에서 신뢰센터와 각 노드 사이에 교환되는 메시지 개수를 나타낸다. 제안한 방법은 초기 네트워크를 구성할 때

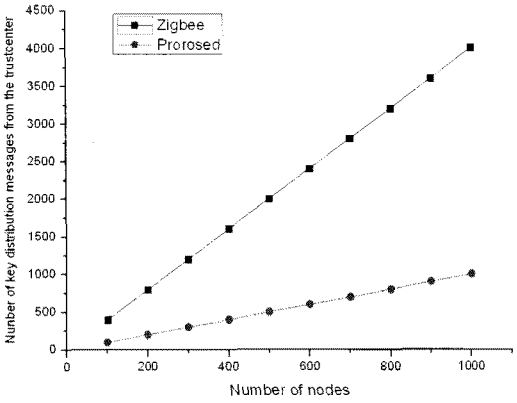

그림 10. 신뢰센터에서 전송되는 키 분배 메시지 개수
Fig 10. The number of the key distribution messages that transmitted from turstcenter.

보안 키 분배를 위해 사용되는 메시지 개수를 기존의 34% 수준으로 줄일 수 있다. 또한 그림 10과 같이 신뢰센터에서 전송하는 메시지의 개수도 29% 감소하며 그림 11에서처럼 각각의 노드에서 전송되는 메시지도 34% 이하 수준으로 감소한다.

그림 12에서는 네트워크 크기($N=2^m$,m=6,7,...,13)에 대한 경로길이를 나타내고 있다. 그림에서 보는 바와 같이 N=128 까지는 경로길이는 $\log_2 N$보다 작은 것으로 나타나고 있지만, N=128보다 큰 경우에는 점차적으로 증가함을 알 수 있다. 따라서 본 논문에서 제시한 프로토콜은 네트워크 크기가 증가할수록 노드의 저장소 크기($\log_2 N$)와 인증서 경로길이 사이의 조율이 필요하다. 비록 N이 증가함에 따라 인증서 경로

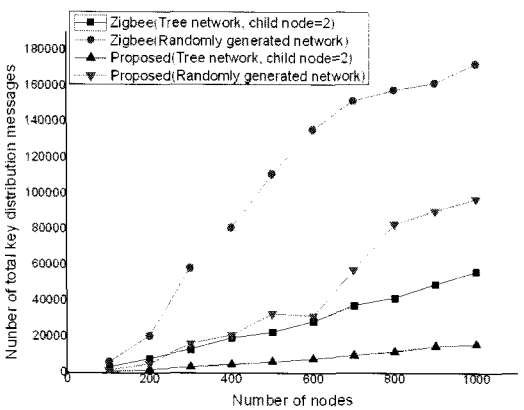

그림 9. 제안한 ZigBee 프로토콜과 기존의 ZigBee 프로토콜의 키 분배 메시지 수
Fig 9. The number of the key distribution messages of the proposed Zigbee protocol and typical Zigbee protocol.

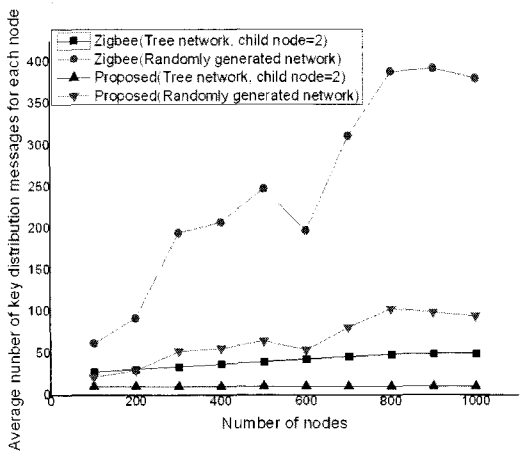

그림 11. 노드에서 전송되는 키 분배 메시지의 평균 개수 비교
Fig 11. The average number of the transmitted key distribution messages per node.

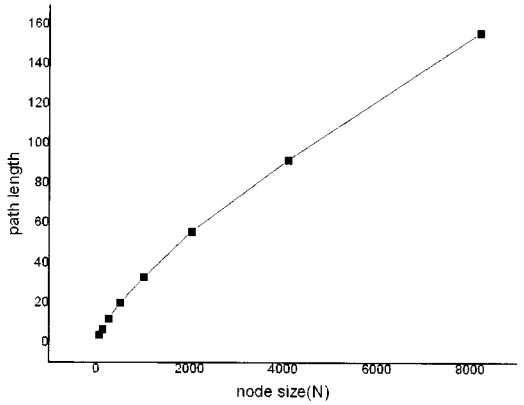

그림 12. 경로 길이 대 노드 사이즈(N)
Fig 12. Path length vs. node size

가 증가할지라도, N=8,192에서 인증경로의 길이는 $2\sqrt{N}$보다 작음을 알 수 있다.

그림 13에서의 경로구축 성공확률(P_b)에서 보는 바와 같이 r이 0.5까지는 신뢰수준 99%에서 경로구축이 97.9이상 성공하는 것을 볼 수 있다. r이 0.5인 경우는 $N/2=2^{m-1}$과 동일하다. 따라서 r 이 0.5보다 큰 경우에는 모든 노드의 ID를 N/2보다 작도록 조정함으로써 네트워크 사이즈를 N/2으로 변경할 수 있다. 이를 통하여 r이 $(N/2-N_r)/(N/2)$으로 조정되어 본 논문에서는 성능이 개선할 수 있다.

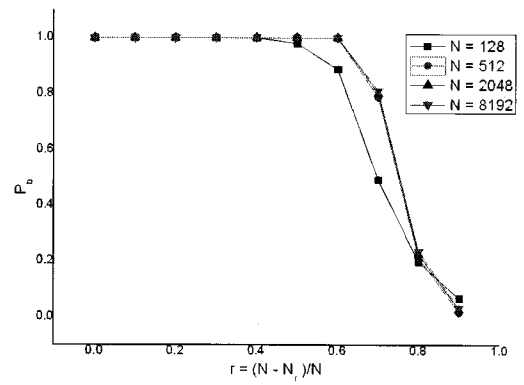

그림 13. 경로 구축 대 노드 감소율 r
Fig 13. path establish vs node decreasing rate

V. 결 론

ZigBee는 저 전력 초소형 저비용으로 제어와 모니터링을 가능하게 하는 표준으로 스마트 그리드 환경에 적용하기 위해 주목 받고 있다. 그러나 본 논문에서는 복잡한 키 관리와 인증 등의 부재로 ZigBee 보안시스템에 심각한 취약성이 있음을 밝히고 이를 해결하는 새로운 프로토콜을 제안하였다. 제안한 방식은 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 암호방식을 기반으로 Hamming distance를 이용하여 설계한 새로운 프로토콜로써 스마트그리드 네트워크에서 공개키 인증서의 저장 및 관리에 필요한 저장소 크기를 개선하기 위하여 모든 노드에 ID를 부여하고 각 노드는 자신의 공개키 인증서 ID와 HD가 "1"인 노드에 대해서만 공개키 인증서를 발급, 갱신, 폐지하는 방안을 제안하였다. 그리고 인증경로 구축 시 나머지 노드는 중개 노드로 활용함으로써 각 노드가 자신의 저장소에서 직접 관리하여야 하는 노드 정보의 수를 log2N으로 줄이고, 인증서 경로의 길이를 보다 작게 할 수 있는 새로운 인증서 경로구축 알고리즘을 제안하여 하였다. 향후 이 인증서 경로구축 알고리즘이 스마트그리드, 즉 지능형 전력망의 보안기술에 적용하기 위해 Zigbee 네트워크와의 호환성 등을 고려하여 연구된다면 좀 더 효율적인 알고리즘이 되리라 기대한다.

참 고 문 헌

[1] U.S. Department of Energy, National Energy Technology Lab., Modern Grid Initiative, http 자료.

[2] Wikipedia encyclopedia, Smart Gird. May, 2009.

[3] DOE Office of Electricity Delivery and Energy Reliability, Integrated Communications, July 2007.

[4] 정수환, "융합보안 R&D 이슈 및 방향", 정보보호학회지 제 19권 제 3호, 한국정보보호학회, pp. 11-13, 2009년 6월.

[5] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "proactive Secret Sharing, or: how to cope with perpetual leakage," Advances in Cryptography - Crypto 95' Proceedings, LNCS Vol 963, 1995.

[6] ZigBee Alliance, "ZigBee specification," Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, 2005.

[7] "Standard for part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPAN)," IEEE Std

802.15.4, 2003.

[8] NIST, "Announcing the Advanced Encryption Standard(AES)," FIPS PUB ZZZ, 2001, available at http://www.nist.gov/aes.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Advances in Cryptology, Crypto'84, Springer-Verlag, LNCS 196, pp.47-53, 1985.

[10] V. Miller, "Use of elliptic curves in cryptography," Proc. Advances in ryptology, CRYPTO'85, Springer-Verlag, LNCS 218, pp. 417-7426, 1986.

[11] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol.48, No.177, pp.203~209, Jan. 1987.

[12] D. Bonech, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Advances in Cryptology, Asiacrypt 2001, Springer-Verlag, LNCS 2248, pp.514~532, Dec. 2001.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology, Crypto 2001, Springer-Verlag, LNCS 2139, pp.213-229, Aug. 2001.

[14] M. C. Gorantla, R. Gangishetti, and A. Saxena, "A Survey on ID-Based Cryptographic Primitives," Cryptology ePrint Archive, Report 2004/131, available at iacr.org/2005/094/.

[15] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol.22, No.6, pp.644-654, Nov. 1976.

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method of obtaining digital signature and public key cryptosystem," ACM Communication, Vol.21, No.2, pp.120-126, Feb. 1978.

[17] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inform. Theory, Vol.IT-31, No.4, pp.469-472, July 1985.

[18] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," Proc. Cryptographic Hardware and Embedded Systems (CHES 2004), Springer-Verlag, LNCS 3156, pp.119-132, Aug. 2004.

[19] R. Hamming. Coding and Information Theory. Prentice-Hall, 1980.

[20] Brent Hodges, Craig Rodine, Craig Tinder, and Ivan O'Neill, "Smart Energy Profile Marketing Requirements" Document Draft Revision 1.0, ZigBee+HomePlug Joint Working Group, Mar. 2009.

[21] Y. Frankel, P. Gemmell, P.-D. MacKenzie, and M. Yung, "Optimal-Resilience Proactive Public-Key Cryptosystems", IEEE Symp. on Foundations of Computer Science, 1997.

[22] S. Capkun, L. Buttyan and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE Trans. on mobile computing, Vol.2, No.1, Jan./Mar. 2003.

[23] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF RFC3280, April 2002.

[24] C. C. Shen, C. Srisathapornphat, R. L. Z. Huang, C. Jaikaeo, and E. L. Lloyd, "CLTC: A cluseter-based topology control framework for ad hoc networks," IEEE Trans. Mobile Computing, Vol.3, No.1, pp.18-32, Jan.~Mar. 2004.

[25] ZigBee Smart Energy Profile Specification : Document 075356r15

임 송 빈 (Song-Bin Im) 정회원

2002년 2월 광운대학교 전자통신공학과 석사

2008년 3월~현재 신흥대학 전자통신과 겸임교수

2007년 3월~현재 광운대학교 전자통신공학과 박사과정

<관심분야> SmartGrid, ZigBee, Security

오 영 환 (Young-Hwan Oh) 정회원

현재 광운대학교 전자통신공학과 정교수