情 報 保 護 學 會 誌
第17卷 第1號, 2007. 2

유비쿼터스 환경에서의 ZigBee 기술과 보안요구사항

김 학 범*

요 약

저전력·초소형·저비용 장점과 함께 10~20m 내에서 250Kbps의 속도로 데이터를 전송하고 6만 5000개 이상의 노드를 연결할 수 있는 ZigBee는 이제 막 상용화 단계에 접어들었으며, 유비쿼터스 센서 네트워크(USN)를 구현하는 최적의 기술로 주목받고 있다. 본 고에서는 다양한 분야에 응용될 것으로 예상되는 ZigBee 관련하여 표준화 현황, 기술 현황 및 보안 요구사항에 대해서 고찰한다.

Ⅰ. 서 론

ZigBee는 저속의 전송 속도를 갖는 홈 오토메이션 및 데이터 네트워크를 위한 표준 기술로서 버튼 하나로 하나의 동작을 잡아 집안 어느 곳에서나 전등 제어 및 홈보안 시스템 VCR on/off 등을 할 수 있고, 인터넷을 통한 전화 접속으로 홈 오토메이션을 더욱 편리하게 이용하려는 욕구에서부터 출발한 기술이다. IEEE 802.15.4에서 표준화가 진행되고 있으며, 듀얼 PHY 형태로 주파수 대역은 2.4GHz, 868/915MHz를 사용하고, 모뎀 방식은 직접 시퀀스 확산 스펙트럼(DS-SS: Direct Sequence Spread Spectrum) 기술을 사용한다.

ZigBee의 시작은 Home Network의 무선 기술로 각광받았던 HomeRF의 Low Rate Version으로 1998년에 시작되었으며, Firefly, RF-Lite로 이름이 변경된 후 최종적으로 ZigBee로 명명되었다[1].

과학적으로도 꿀벌의 지그재그 춤은 상당히 정확하고 경제적인 통신수단으로 인정받고 있다. 이런 혁신적인 통신기술을 표방하며 'Zig'와 'Bee'의 합성어로 만들어진 차세대 무선네트워크 기술이 '지그비'(ZigBee)다. 저전력·초소형·저비용 장점과 함께 10~20m 내에서 250Kbps의 속도로 데이터를 전송하고 6만 5000개 이상의 노드를 연결할 수 있는 ZigBee는 이제 막 상용화 단계에 접어들었으며 유비쿼터스 센서 네트워크(USN)를 구현하는 최적의 기술로 주목받고 있다[2].

ZigBee의 첫 번째 시장은 사업분야로 예상되며, 초기 투자 대비 막대한 효과를 발휘할 수 있는 시점으로 평가되고 있으며, 두 번째 시장으로는 빌딩 제어 및 자동화 분야, 그 다음이 무선 리모콘 및 게임용 콘솔기 등의 가전 분야, 자동차용 센서 및 홈 네트워크 분야로 이어질 전망이다[3].

본 고에서는 ZigBee 관련하여 표준화 현황, 기술 현황 및 보안 요구사항에 대해서 고찰한다.

Ⅱ. ZIgBee 관련 표준화 동향

2.1 IEEE 1451 워킹 그룹

IEEE 1451 워킹 그룹은 '93년 9월 NIST와 IEEE의 기술 위원회를 중심으로 하여 스마트 센서 통신 인터페이스의 표준에 대한 논의를 시작으로 각 5개의 워킹 그룹을 통해 표준화가 진행되었으며, 현재 7개의 워킹 그룹이 활동하고 있다.

IEEE P1451.5 무선 표준은 변환기들의 무선 통신 방식과 데이터 형식을 정의한 표준이다. 이 표준은 여러 MAC/PHY 조합을 포함하며 하나의 모델로써 IEEE 802로의 접근을 시도하여 블루투스(IEEE 802.15.1), Zigbee (IEEE 802.15.4), IEEE 802.11의 모든 무선 표준들과 개인의 무선 링크를 포함한다[4].

IEEE 1451.5 무선 인터페이스 표준은 다른 1451 프로젝트로부터 센서 네트워킹 특성을 영향 받았다. 1451.1로부터 지능형 변환기 오브젝트 모델을, 1451.2

* 순천향대학교 정보보호학과(khb0305@sch.ac.kr)

로부터 TEDS 컨셉을, 1451.3으로부터 동기화 및 XML TEDS를, 1451.4로부터 콤팩트 TEDS와 변환기 인터페이스를 받아들였다. 또한 계층 구조를 가짐으로써 현존하는 제품들의 사용을 크게 증가시킬 수 있으며 차후 확장도 가능하게 하였다. [그림 1]은 P1451.5 프로토콜 구조를 보여준다[5].

[그림 1]에서 1451.1 관리 영역은 1451 어플리케이션과 QoS 제어 사이의 정보 교환을 하는 능력과 관리 함수들을 제공한다. 1451.5 어플리케이션 영역은 센서 응용 프로그램 정보의 전송을 담당하며, QoS 제어 영역은 QoS 보장을 위해 필요한 연결 성립과 해지, 다른 제어 기능 등을 다룬다.

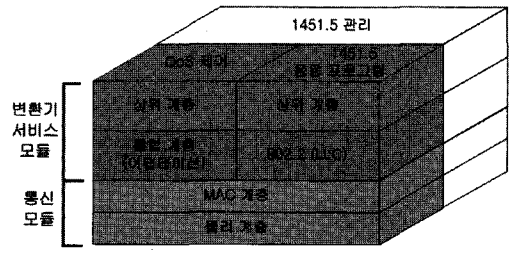
IEEE P1451.5의 프레임 구조는 NCAP(Network Capable Application Processor)와 변환기들, 변환기 서비스와 인터페이스, 변환기 전자 데이터 시트와 인터페이스 사이의 무선통신과 인터페이스를 포함한다.

[그림 2]에서 보면 U 지점은 통신 모듈 사이의 논리적, 물리적 인터페이스의 성격을 포함한다. 무선 브리지 같은 점대점 연결은 하나의 통신 케이블을 대체할 수 있으며, IEEE 802.11과 블루투스 같은 점대다 연결 링크는 네트워크 내에 모든 다른 무선 노드들과의 통신이 하나의 액세스 포인트를 통해서 이루어질 수 있다. 감지와 산업적인 제어를 위한 무선 그물형망 토폴로지는 ad hoc이나 멀티 홉 네트워크라고 불리는 시스템이나 점대점, peer-to-peer로 이루어진다. 한 노드는 그물형망 내에서 메시지를 보내고 받을 수 있다. 각 노드는 또한 라우터의 역할을 하며 그 이웃에게 데이터를 전달할 수 있다. 이러한 전달 과정을 통해 무선 데이터 패킷은 신뢰할만한 통신 링크를 가진 중간 노드들을 거쳐 그것의 목적지로 가는 길을 찾게 된다.

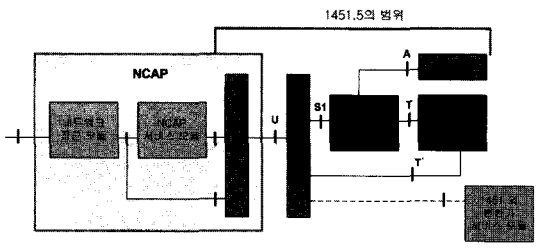
S1 지점은 통신 모듈과 변환기 서비스 모듈사이 인터페이스의 논리적, 물리적 특성을 가지고 있다. SAP (Service Access Point)를 가지며 직렬의 점대점 연결로 물리적 인터페이스가 구성되어 있다.

T 지점은 변환기 서비스 모듈과 변환기의 전기적 데이터 시트 사이 인터페이스의 논리적, 물리적 특성을 나타내는 부분이다.

A 지점은 변환기 서비스 모듈과 아날로그에 기초한 변환기 사이 인터페이스의 논리적, 물리적 특성을 갖는다[5].



[그림 1] 프로토콜 구조



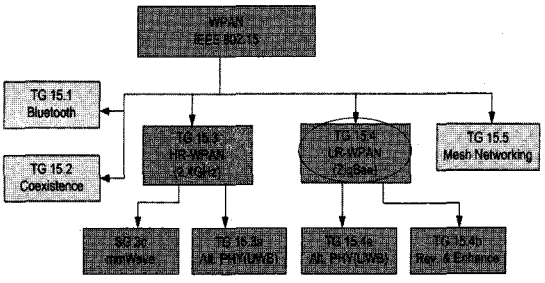
[그림 2] IEEE 1451.5 프레임 구조

2.2 IEEE 802.15 워킹 그룹

IEEE 802.15 워킹 그룹은 무선 개인 영역 네트워크(Wireless Personal Area Networks, WPAN) 또는 단거리 무선 네트워크를 위한 표준을 제정하는 것을 목표로 한다. WPAN은 PC, PDA, 셀룰러 폰 등의 무선 이동 기기간의 통신을 가능하게 하며, 다른 무선 통신 기술에 비해 에너지 소비가 낮고 저가이기 때문에 센서네트워크에 도입되기에 적합한 통신 기술로 부각되고 있다. 특히, IEEE 802.15.4 표준은 센서네트워크에서 가장 적합한 통신 기술로 인정받고 있으며, 현재 ZigBee와 6LoWPAN의 MAC(Medium Access Control)/PHY (Physical layer) 표준으로 사용되고 있다.

[그림 3]은 IEEE 802.15 워킹 그룹의 구성을 보여준다.

IEEE 802.15 TG3는 고속의 WPAN에 대한 연구를



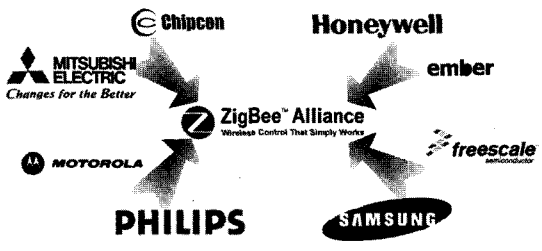
[그림 3] IEEE 802.15 워킹 그룹 구성

진행한다. TG3에서는 MAC과 PHY를 정의하며, 데이터 전송 속도는 11~55Mbps 정도이고 이동 기기에서 이미지 및 멀티미디어 응용 서비스 제공에 초점을 맞추고 있다.

IEEE 802.15 TG4는 데이터 전송률이 낮고 수개월 또는 수년간 지속되는 배터리를 이용하는 저가의 장비를 위한 데이터 표준을 제정한다. TG4에서 정의한 MAC과 PHY는 ISM(industrial, scientific and medical) 밴드에서 동작하며 센서, 장난감, 스마트 뱃지, 무선 컨트롤러 등에 사용 가능할 것으로 예상된다. 2003년에 발표된 'IEEE Std 802.15.4-2003' 표준에 따르면 TG4의 MAC과 PHY는 250kbps 이하의 데이터 전송률을 지원하며, 2개의 주소 모드, 네트워크 설정 자동화, 낮은 에너지 소비 등의 특징을 갖는다. TG4의 표준 제정 이후, TG4는 TG4a와 TG4b로 분리되어 운영되고 있다. TG4a에서는 TG4의 표준을 기반으로, 통신 능력 뿐만 아니라 1미터 혹은 그 이상의 정확성을 갖는 위치 인식 능력, 높은 전송 효율, 다양한 데이터 전송률을 제공하는 저가 및 저전력 PHY를 제정하는 것을 목적으로 한다. 또한, TG4b는 TG4에서 제정한 표준을 더욱 명확하게 하고, 불필요한 복잡성을 줄이는 등 좀더 명확한 IEEE 802.15.4 표준을 제공하는 것을 목적으로 한다[6].

2.3 ZigBee Alliance

ZigBee Alliance의 프로모터는 Chipcon, 필립스(Philips), 미쓰비시(Mitsubishi), 모토로라(Motorola), Honeywell, Freescale, Ember, 삼성으로 구성되어 있으며, 100개 이상의 참여 기업이 존재한다. 국내에서도 LG, TTA, 한국무선네트워크(korwin), 한국전자통신연구원(ETRI) 등 다수의 기업 및 연구단체가 참여 기업으로 활동하고 있다. [그림 4]는 ZigBee Alliance의 프로모터(promoter) 기업들을 보여준다.

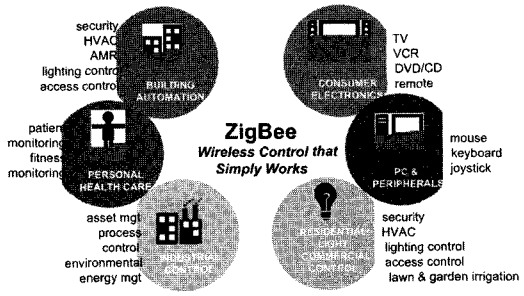


[그림 4] ZigBee Alliance 프로모터

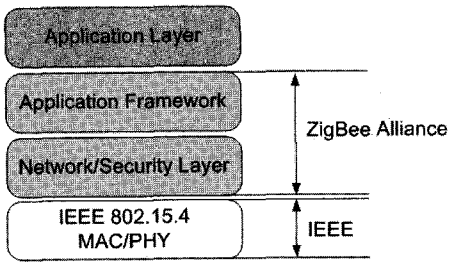
ZigBee Alliance는 2003년 완성된 IEEE 802.15.4 표준을 기반으로 저전력 무선 네트워킹이 가능한 모니터링 및 제어(control) 제품을 위해 상위 프로토콜 표준을 정의하는 것을 목표로 한다. ZigBee는 단순 기능이 요구되는 초소형, 저전력, 저가격 시장에 적합한 기술로 우선 홈오토메이션(Home automation)과 같은 홈네트워크 분야에 적용에 초점을 맞추고 있으나 궁극적으로 [그림 5]와 같이 다양한 분야에 적용시키는 것을 목적으로 하고 있다.

ZigBee Alliance는 ZigBee 네트워크를 구성하기 위해 [그림 6]과 같이 네트워크 계층, 응용프로그램을 지원하기 위한 응용 지원 부계층(Application support sublayer), 응용 프레임워크(Application Framework), 보안 계층, ZDO(ZigBee Device Object)등에 대한 표준화를 진행하여, 2005년 6월에 ZigBee 표준 1.0 버전을 완성하여 공개하였다[8]. ZigBee는 IEEE 802.15.4 표준을 기반으로 하며 네트워크 계층에서 응용 계층까지 모든 계층을 정의하고 있다. ZigBee 스택은 OSI (Open Systems Interconnection) 7계층 모델을 기반으로 한 계층적 구조를 가지고 있다. [그림 7]은 ZigBee 스택의 계층적 구조에 대해 보여준다.

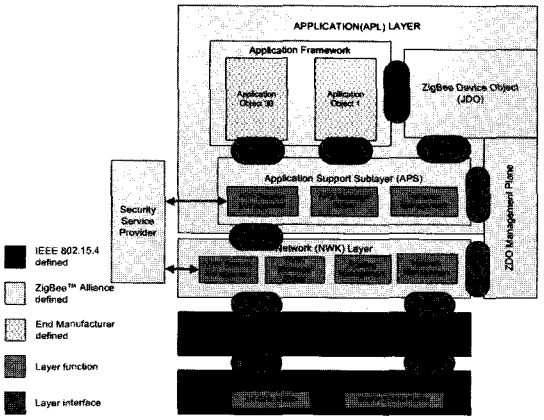
ZigBee 네트워크 계층에서는 노드들이 네트워크에 접속하고 접속을 끊는 메커니즘과 보안이 적용된 데이



[그림 5] ZigBee 응용 분야[7]



[그림 6] ZigBee Alliance 표준화 작업 범위



〔그림 7〕 ZigBee 스택 구조[8]

터 프레임, 그리고 원하는 목적지까지 데이터 프레임을 전송하기 위해 경로를 찾는 라우팅 알고리즘과 프레임 전달 메커니즘 등이 정의되어 있다.

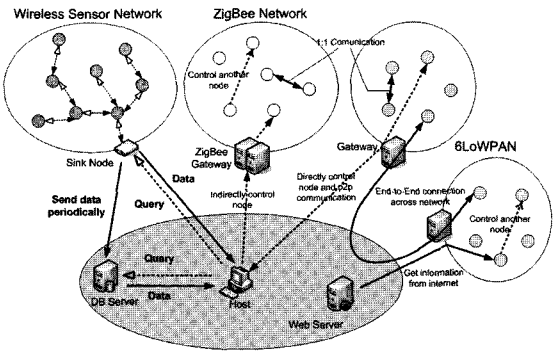
응용 지원 부계층에서는 두개의 서로간의 장치를 연결하기 위한 바인딩 테이블 관리와 바인딩된 장치 간에 메시지를 전송하기 위한 메커니즘이 정의 되어 있다.

ZDO에는 네트워크에서 각 장치의 역할에 대한 정의와 바인딩에 대한 초기화와 바인딩이 되는 과정, 네트워크 장치간의 보안과 장치들이 제공하는 서비스를 발견하는 방법 등이 정의되어 있다.

ZigBee Alliance는 기업들이 주축이 된 만큼, 표준 제정과 동시에 참여 기업들에 의한 제품생산이 이루어지고 있다.

Ⅲ. ZigBee 네트워크(NWK) 계층

ZigBee Alliance의 ZigBee[9]는 IEEE 802.15.4 표준[10]을 기반으로 하고 있으며 각 노드들은 네트워크 내에서 유일한 주소를 부여받는다. 자신만의 주소를 부여받은 노드들은 이 주소를 통해 네트워크 내에서 독립적인 개체로 존재한다. 〔그림 8〕과 같이 ZigBee 네트워크의 각 노드들은 네트워크 내의 다른 노드들과 1대1 통신이 가능하며, 싱크 노드 혹은 게이트웨이의 추가적인 기능이 갖추어 진다면 다른 네트워크의 기기들과 1대1 통신도 가능해진다. 그러나 ZigBee의 주소는 ZigBee 네트워크 단위로 부여되기 때문에 다른 ZigBee네트워크의 주소와 겹칠 가능성이 있고 같은 PAN(Personal Area Network) ID를 부여받는 ZigBee 네트워크가 여러 개 존재할 가능성도 있다.

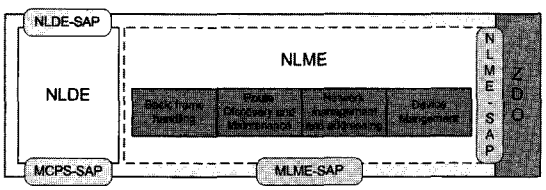


〔그림 8〕 센서네트워크, ZigBee 네트워크, 6LoWPAN 네트워크의 특징

ZigBee 네트워크(NWK) 계층은 ZigBee Specification v1.0[8]을 기반으로 작성되었다.

ZigBee 네트워크 계층은 데이터 프레임을 전송하거나 수신하고 네트워크 헤더를 조작하는 NLDE (Network Layer Data Entity)와 관리를 목적으로 하는 NLME(Network Layer Management Entity)로 구분된다. 또한 계층 간의 상호통신을 위해 인터페이스를 정의하고 있다. 각 계층들은 데이터 프레임과 관련된 데이터 인터페이스와 관리를 위한 관리 인터페이스를 가지고 있으며 네트워크 계층에서도 NLDE-SAP(Service Access Point)라고 이름 붙여진 데이터 인터페이스를 통해 응용지원(Application Support) 부계층의 데이터 관리부와 통신을 하며 IEEE 802.15.4 표준의 MCPS-SAP 데이터 인터페이스를 통해 MAC 계층의 데티어 관리부와 통신한다. 애플리케이션들은 APS 부분계층이 아닌 ZDO (ZigBee Device Object)를 통해 네트워크 계층을 관리할 수 있다. 이 때 ZDO와 네트워크 계층은 NLME-SAP 관리 인터페이스를 사용해 통신한다. 그리고 MAC 계층의 관리를 위해 MLME-SAP 관리 인터페이스를 통해 MAC 계층과 직접적으로 통신한다. 〔그림 9〕는 ZigBee 네트워크 계층의 인터페이스와 기능에 대해 보여준다.

ZigBee의 네트워크 계층에서는 그림에서처럼 크게



〔그림 9〕 ZigBee 네트워크 계층 구조

다음의 4가지 기능을 제공한다.

- 기본 프레임 핸들링
- 경로 탐색 및 유지 보수
- 네트워크 관리 및 주소 할당
- 장치 관리

3.1 ZigBee 네트워크 계층의 장치 분류

IEEE 802.15.4 표준의 장치 분류가 FFD와 RFD의 두개로 분류되는데 비해 ZigBee 네트워크 계층에서는 이를 세분화 하여 총 3개의 장치로 구분하고 있다. 다음은 ZigBee 네트워크 계층에서의 각 장치별 분류와 그 특징에 대한 설명이다.

3.1.1 ZigBee 코디네이터

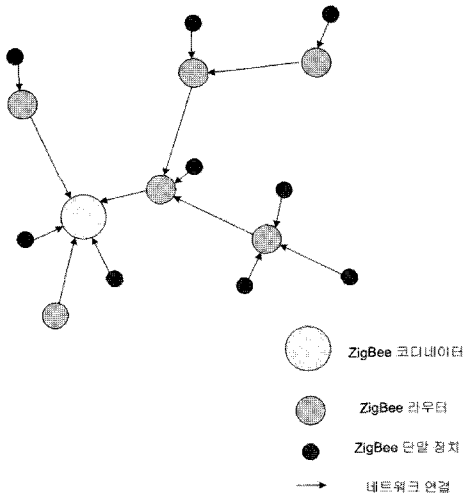
- 각각의 ZigBee 네트워크 내에서 하나의 ZigBee 코디네이터가 필요하다.
- 네트워크 정보를 초기화한다.
- IEEE 802.15.4 표준의 PAN 코디네이터와 같은 역할을 한다.
- FFD(Full Function Device)만이 될 수 있다.

3.1.2 ZigBee 라우터(Router)

- 선택사항인 네트워크 컴포넌트로써 멀티 홉 라우팅을 하기 위해서 필요하다.
- 하나의 네트워크 내에는 여러 개의 ZigBee 라우터가 존재한다.
- ZigBee 코디네이터 혹은 이미 네트워크에 접속중인 ZigBee 라우터를 통해 네트워크에 참여한다.
- IEEE 802.15.4 표준의 코디네이터와 같은 역할을 한다
- FFD만이 될 수 있다.

3.1.3 ZigBee 단말장치(End Device)

- 선택사항인 네트워크 컴포넌트이며 라우팅에는 참여하지 않는다.
- 하나의 네트워크 내에는 여러 개의 ZigBee 단말장치가 존재한다.
- ZigBee 코디네이터 혹은 이미 네트워크에 접속중인 ZigBee 라우터를 통해 네트워크에 참여한다.
- ZED는 가장 하위 장치로 네트워크 참여를 허락하지 않는다.



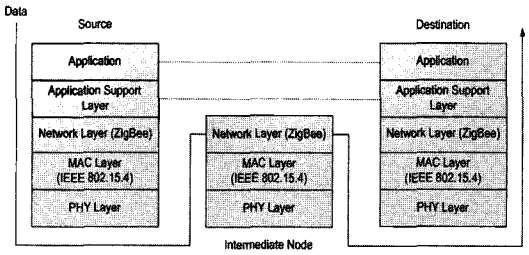
〔그림 10〕 ZigBee 네트워크 토폴로지

ZigBee 네트워크는 위의 세 개의 장치에 의해 구성된다. 〔그림 10〕은 위의 세 장치들로 구성된 ZigBee 네트워크를 보여준다.

3.2 네트워크 내에서의 데이터 전송

네트워크 내에서의 데이터 전송 시간에 가장 큰 영향을 미치는 것은 라우팅(Routing)을 어떤 계층에서 하는가이다. 소스에서 목적지까지 데이터가 전송될 때 거치게 되는 중간 노드들에서는 목적지를 찾기 위해서 경로를 탐색한다. 그러나 라우팅을 보다 상위 계층에서 하게 될수록 중간 노드를 거칠 때마다 거쳐야 하는 계층의 수가 많아지고 그에 따라 프로세싱 처리 시간이 커지게 된다. 프로세싱 처리 시간의 증가는 데이터 전송 시 지연(delay) 시간이 길어짐을 의미하기 때문에 라우팅과 같이 네트워크 연결에 관련된 기능은 최대한 하위 계층에 있는 편이 좋다.

ZigBee 네트워크 내에서 데이터 흐름은 〔그림 11〕과 같다. ZigBee에서는 라우팅 기능을 ZigBee 네트워크 계층이 가지고 있다. 응용(application) 계층과 응용 프레임워크(framework)는 소스와 목적지에서 단대단 연결이 된다. 중간노드에서의 메시지는 ZigBee 네트워크 계층까지만 올라가게 된다. 라우팅 기능을 통해 목적지로 가기위한 경로를 찾은 메시지는 다시 새로운 MAC 헤더와 PHY헤더를 추가하는 작업을 거치고서 다음 노드로 전송된다.



〔그림 11〕 ZigBee 네트워크에서의 데이터 전송

3.3 네트워크 주소 및 주소 할당

ZigBee의 각 노드들은 처음 네트워크에서 참여할 때 ZigBee 코디네이터와 통신하며 참여하려는 네트워크의 정보와 자신이 사용할 16bit 주소를 할당받는다. 이 과정에서 16bit 주소를 할당받지 못한 노드는 자신이 가지고 있는 64bit 주소를 이용해 주위 노드들과 통신한다. 이 때 할당받은 16bit 주소는 하나의 PAN(Personal Area Network)내에서는 유일한 주소값이다. 그러나 다른 PAN의 노드와는 주소가 충돌할 가능성이 있으며 이는 ZigBee가 외부 네트워크와의 연결할 때 하나의 ZigBee 장치를 식별하기 위해서는 추가적인 기능을 제공해야 한다.

3.4 라우팅 및 토폴로지의 확장성

ZigBee 네트워크에서는 새로운 장치가 네트워크에 참여할 때 클러스터 트리 기반의 토폴로지를 형성한다. 이는 ZigBee에서 제공하는 계층적 라우팅(Hierarchical routing)을 이용하고, 16bit 주소를 할당할 때 분산 처리를 하기 위해서이다. 분산 주소 할당 기법 덕분에 ZigBee에서는 주소의 충돌을 검사하기 위한 부가적인 기능이 필요하지 않다. 그러나 이 방법은 클러스터 트리 구조를 가지고 있기 때문에 하나의 부모가 가질 수 있는 자식의 수는 네트워크 설정에 따라 제한이 생기고, 그로 인해 트리구조에 참여하지 못한 노드가 생길 가능성도 존재한다. 이러한 노드들은 네트워크 주소 할당 부분의 설명에서처럼 64bit 주소를 이용해 다른 노드들과 통신하지만, 정상적으로 네트워크에 참여하는 노드에 비해 경로 탐색(route discovery) 알고리즘을 이용하지 못하는 등, 몇가지 기능을 제약 받게 된다.

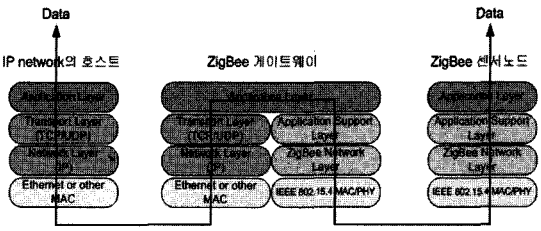
ZigBee에서는 계층적 라우팅과 경로 탐색 알고리즘 이라는 두 가지 라우팅 알고리즘을 제공하며 데이터를 전송할 때 둘 중 하나를 선택하여 사용할 수 있다.

3.5 외부 네트워크와의 호환성 및 게이트웨이 구조

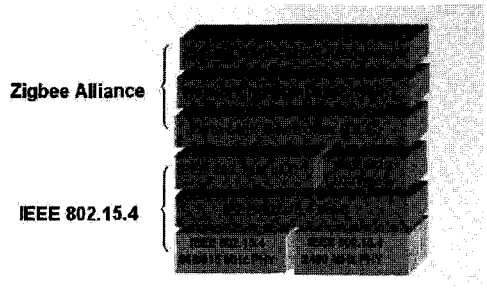
ZigBee는 ZigBee 네트워크 내에서의 통신에 중점으로 두고 있으며 ZigBee specification v1.0에서도 외부 네트워크와의 호환에 대해서는 정의 되어 있지 않다. 현재 가장 많이 사용되는 IP네트워크와 통신하기 위한 ZigBee 게이트웨이는 〔그림 12〕와 같은 구조를 지녀야 한다. ZigBee는 모든 계층이 기존의 IP와 다른 ZigBee만의 프로토콜 구조를 가지고 있기 때문에 응용 계층 수준의 게이트웨이가 필요하다. 그러나 IPv6가 주류가 되는 시대에는 네트워크 트래픽이 급증할 것이다. 엄청난 트래픽이 발생 할 것을 예상한다면 응용 계층 수준의 게이트웨이는 프로세싱 딜레이가 크다는 점에서 데이터 전송의 지연, 패킷 손실과 같은 문제점을 예상할 수 있다[5].

Ⅳ. 보안요구사항 분석

ZigBee의 보안 서비스는 대칭키 암호 방식을 이용하여 두 노드 간의 비밀키 설정과 상호 인증 과정을 수행하고, 이 키를 이용하여 MAC 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 보안 기능을 제공한다[10].



〔그림 12〕 ZigBee 게이트웨이의 구조



〔그림 13〕 ZigBee와 IEEE 802.15.4와의 관계

4.1 IEEE 802.15.4에서의 보안 요구사항

IEEE 802.15.4 표준에서 제공하는 security suite은 장치들이 안전 모드로 운영될 때 사용 가능하다. security suite들은 보안 서비스를 제공하는 MAC 프레임을 수행하기 위한 오퍼레이션들로 구성된다. security suite들의 명칭은 대칭키 암호 알고리즘, 운용모드 및 무결성 코드의 비트 길이를 표시한다. 무결성 코드의 길이는 대칭암호의 블록 크기보다는 작거나 같아야 한다.

이 표준에서 알고리즘들은 AES(Advanced Encryption Algorithm)을 사용되어야 하며, 각 장치들은 AES-CCM-64 security suite을 지원하여야 한다. 각 security suite에 대한 목록은 〔표 1〕과 같다[10].

4.1.1 보안요구사항 빌딩 블록

security suite에 사용하기 위하여 다음과 같은 방법들을 정의한다.

① 비트 순서(Bit ordering) : {0, 1}의 집합을 가지는 8비트의 octet이 정의되는데 bit 7이 처음 비트이며 bit 0이 마지막 비트이다.

② 연접(Concatenation) : 두 옥텟 스트링 a(n 길이)와 b(m 길이)의 연접은 a||b로 표시되며 길이는 n+m이 된다.

③ 정수 인코딩 및 카운터 증가(Integer encoding and counter incrementing)

④ CTR 암호화 : CTR(counter mode) 대칭키 암호화 알고리즘이 사용되는데 이는 주어진 키와 난수를 가지고 블록 암호를 사용하여 키 스트림을 생성하고 평문과 무결성 코드를 키 스트림과 XOR하여 구성한다.

〔표 1〕 Security-suite 목록

식별자	security suite name	보안 서비스			
		접근통제	데이터 암호화	프레임 무결성	Sequencial freshness (선택)
0x00	None				
0x01	AES-CTR	x	x		x
0x02	AES-CCM-128	x	x	x	x
0x03	AES-CCM-64	x	x	x	x
0x04	AES-CCM-32	x	x	x	x
0x05	AES-CBC-MAC-128	x		x	
0x06	AES-CBC-MAC-128	x		x	
0x07	AES-CBC-MAC-128	x		x	

⑤ CBC-MAC 인증 : cipher block chaining message authentication code는 대칭형 인증 알고리즘으로 데이터 초기부분에서 인증데이터의 길이를 포함하는 메시지 상에서 계산된 CBC 모드의 블록 암호를 사용하여 무결성 코드를 생성한다.

⑥ CCM combined 암호화 및 인증 : CTR 암호화와 CBC-MAC이 결합된(CCM) 암호화 및 인증 메커니즘은 암호화된 데이터와 암호화된 무결성 코드를 만드는 것이다.

⑦ AES 암호화 : NIST FIPS Pub 197[12]에 정의된 대로 수행하여야 하며, 128비트의 키 크기와 블록 크기를 사용하여야 한다.

⑧ PIB security material : 이는 MAC PIB에 저장되는 보안정보에 대한 포맷을 설명하는데, 이들 정보는 각각의 security suite에 독립적이다.

4.1.2 AES-CTR security suite

AES-CTR security suite은 장치가 안전 모드로 동작할 때 사용되는데, 공유된 데이터, 프레임 카운터 및 키 순서 카운터를 사용하는 MAC 페이로드 내의 페이로드 필드 상에서 AES-CTR 암호화를 수행한다.

AES-CTR security suite에서는 접근통제, 데이터 암호화 및 sequential freshness 서비스(선택사항)를 제공한다.

4.1.3 AES-CCM security suite

AES-CCM security suite은 장치가 안전 모드로 동작할 때 사용되는데, MAC 페이로드와 함께 연접된 MHR 상에서 AES-CCM 인증(또는 검증)을 수행하고, 공유된 데이터, 프레임 카운터 및 키 순서 카운터를 사용하는 MHR 내의 페이로드 필드 상에서 암호화(또는 복호화)를 수행한다. AES-CCM security suite는 32비트, 64비트, 128비트의 무결성 코드를 사용하여 구현하여야 한다.

AES-CCM security suite에서는 접근통제, 데이터 암호화, 프레임 무결성 및 sequential freshness 서비스(선택사항)를 제공한다.

4.1.4 AES-CBC-MAC security suite

AES-CBC-MAC security suite은 장치가 안전 모드로 동작할 때 사용되는데, MHR과 MAC 페이로드 상에서 AES-CBC-MAC 인증을 수행한다. AES-CBC-

MAC security suite는 32비트, 64비트, 128비트의 무결성 코드를 사용하여 구현되어야 한다.

AES-CCM security suite에서는 접근통제와 프레임 무결성 서비스를 제공한다.

4.2 ZigBee 스펙에서의 보안 요구사항

ZigBee가 128비트 AES 알고리즘에 기반하여 보안 스펙 및 소프트웨어의 표준화된 툴박스를 제공하며 802.15.4의 보안 요소를 통합했다. ZigBee 스택 프로파일이 MAC, 네트워크, 어플리케이션 층을 위한 보안을 정의한다. 이 보안 서비스가 주요 구축 및 전송, 장치 관리, 프레임 보호를 위한 기법을 포함한다[8].

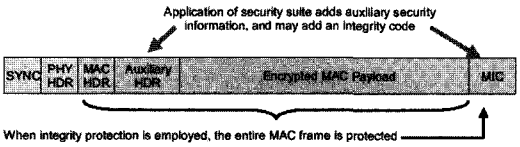
개발자가 공개 ZigBee 프로파일을 이용하기로 한다면 어플리케이션의 보안 결정이 이미 이루어진 것이다. 프로파일로 사전에 정의되었기 때문이다. 개발자가 고유의 프로파일 어플리케이션을 구축하고자 하더라도 ZigBee의 사전정의 스택 프로파일의 보안 모드를 선택할 수 있다.

이 단계(level)에서는 개발자가 데이터 프레임 페이로드를 암호화할지 또는 프레임 끝에 태그되는 승인 코드를 어느 길이로 할지 등의 문제를 결정해야 한다. 기본 어플리케이션은 승인을 필요로 하지 않을 수 있으므로 더 작은 패킷 페이로드를 이용할 수 있다. 이러한 데이터 무결성 옵션을 이용해 개발자가 메시지 보호와 오버헤드를 절충할 수 있다.

개발자는 또한 MAC, 네트워크, 아니면 어플리케이션 층에서 보안을 적용할지를 결정해야 한다. 어플리케이션이 가장 강력한 보안을 필요로 할 때는 어플리케이션 층에서 적용해야 한다. 이 층에서 구현되는 보안은 세션 키를 이용해서 이 키를 소유한 장치만이 이를 승인하고 해독할 수 있다. 이 기법은 내부적 및 외부적 공격을 방어하기는 하지만 이의 구현을 위해 더 많은 메모리를 필요로 한다.

4.2.1 MAC 계층 보안

ZigBee에서는 MAC 계층에서 프레임이 시작되면, 802.15.4 규격에서 정의된 대로 MAC 계층 보안을 사용해야 한다. 입력과 출력 프레임 중 적어도 하나는 막을 수 있도록 CCM*에 기반한 보안 레벨을 사용해야 한다. CCM*는 CCM에 대한 약간의 변경으로서 CCM의 기능에 encryption-only 또는 integrity-only 기능을 추가로 제공한다. 이러한 기능은 CTR 모드와 CBC-MAC 모드의 필요성을 없앰으로서 보안을 단순화시킨다. 또한 각 보안 수준마다 다른 키를 요구하는 다른 MAC 계층 보안 모드와는 달리 CCM*을 사용하므로서 모든 CCM* 보안 수준에서 단일 키 사용을 가능하게 하였다. ZigBee 스택 전체에 걸쳐서 CCM*를 사용하므로서 MAC, NWK 및 APS 계층에서 같은 키를 재사용할 수 있다.



〔그림 14〕 MAC 레벨에서 보안을 처리하는 ZigBee 프레임

〔그림 14〕에서는 MAC 계층에서 보안이 적용된 출력 프레임을 포함할 수 있는 보안 필드의 예를 보여준다.

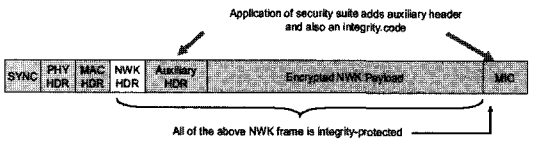
4.2.2 NWK 계층 보안

NWK 계층에서 안전하게 처리해야 할 프레임이 시작되거나, 높은 계층에서 프레임이 시작되고 NIB 내의 nwkSecureAllFrames 속성이 TRUE일 경우에, NLDE-DATA 요청 프리미티브의 SecurityEnable 파라미터가 FALSE가 아닌 이상 ZigBee는 규격 3.4.1절(Frame Security)에 규정된 프레임 보호 메커니즘을 사용하여야 한다.

MAC 계층과 비슷하게 NWK 계층의 프레임 보호 메커니즘은 AES를 사용하여야 하며 CCM*를 사용하여야 한다. NWK 프레임에 적용된 보안 레벨에서는 NIB 내에 nwkSecurityLevel 속성에 의해 주어져야 한다.

NWK 계층에서는 멀티 홉 연결에 따른 메시지 라우팅에 대한 기능이 있는데, 그 중 하나로 NWK 계층에서 라우트 요청 메시지를 브로드캐스트 하고 수신한 라우트 응답 메시지를 처리한다.

만일 적절한 링크 키가 가용하면 NWK 계층에서는 NWK 프레임을 안전하게 내보내기 위하여 링크 키를 사용하여야 한다. 만일 적절한 링크 키가 가용하지 않으



〔그림 15〕 NWK 레벨에서 보안을 처리하는 ZigBee 프레임

면, NWK 계층의 외부에 대하여 안전한 메시지를 위하여 active 네트워크 키를 사용하여야 한다.

〔그림 15〕는 NWK 프레임에 포함될 수 있는 보안 필드의 예를 보여준다.

4.2.3 APL 계층 보안

APL 계층에서 보안이 필요한 프레임이 시작되면 APS 부계층에서 보안을 처리해야 한다. APS 계층의 프레임 보호 메커니즘에서는 링크 키나 네트워크 키에 기반하여 프레임 보안을 허용한다.

〔그림 16〕은 APL 프레임에 포함될 수 있는 보안 필드의 예를 보여준다.

APS 계층의 또 다른 기능은 키 설정, 키 전송 및 장치 관리 서비스를 갖춘 ZDO를 제공하는 것이다.

① 키 설정 : 공유된 비밀키(즉, 다른 ZigBee 장치와의 링크 키)를 유도한다.

② 키 전송 : 다른 장치들에게 안전한 방법 또는 안전하지 않은 방법으로 키를 전송하는 기능을 제공한다.

③ 장치 업데이트 : 라우터 같은 장치가 신뢰 센터에게 다른 장치의 상태 변경 내용을 알려주는 안전한 수단을 제공한다.

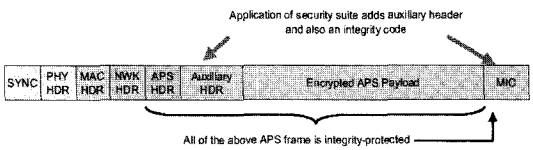
④ 장치 제거 : 신뢰 센터 같은 장치가 라우터와 같은 장치에게 네트워크로부터 장치가 제거되었다는 정보를 알려주는 안전한 수단을 제공한다.

⑤ 키 요청 : 다른 장치로부터 현재의 네트워크 키나 end-to-end 응용 마스터 키를 요청하는 안전한 수단을 제공한다.

⑥ 키 스위치 : 신뢰 센터와 같은 장치가 다른 active 네트워크 키로 스위치 되었다는 사실을 다른 장치에게 안전하게 알려주는 수단을 제공한다.

4.2.4 신뢰 센터 역할(Trust Center Role)

Zigbee 보안은 또한 "신뢰 센터" 개념을 이용한다. 이는 네트워크 상의 장치가 키를 분배하고 장치 간에 1대1 보안을 가능하게 하는 것이다. 이를 위해서는 개발자가 어플리케이션에 따라 주거용 및 상업용의 두 가지 신뢰 센터 모드 중에서 하나를 선택해야 한다. 주거용 모드는 경량이지만 키를 구축하거나 네트워크 크기에 따른 확장이 불가능하다. 상업용 모드는 키를 구축 및 유지하고 네트워크에 따라 확장이 가능하지만 훨씬 더 많은 메모리를 필요로 한다.



〔그림 16〕 APS 레벨에서 보안을 처리하는 ZigBee 프레임

V. 결 론

본 고에서는 다양한 분야에 응용될 것으로 예상되는 ZigBee 관련하여 IEEE 1451, IEEE 802.15 및 ZigBee Alliance 등의 표준화 현황과 관련 기술 현황 및 보안 요구사항에 대해서 고찰하였다.

저전력·초소형·저비용 장점과 함께 10~20m 내에서 250Kbps의 속도로 데이터를 전송하고 6만 5000개 이상의 노드를 연결할 수 있는 ZigBee는 이제 막 상용화 단계에 접어들었으며 블루투스, UWB 보다는 현재 관심을 덜 받고 있지만 센서 네트워크와 같은 버티컬 응용 영역에서 경쟁력 있는 단거리 무선 통신 기술로 각광받을 것으로 예상된다.

참고문헌

〔1〕 한국전자부품연구원, *Zigbee*, 2005. 7.

〔2〕 주상돈, "차세대 무선 네트워크 기술, 이름 값 한다", 전자신문 기사, 2006.10.26.

〔3〕 박재성, 천성일, "ZigBee 기술 및 시장 동향", 한국전자부품연구원, 2005.12.

〔4〕 Michael R. Moore, "Wireless Interface Options for 1451", Wireless Sensing Workshop Sensors Expo/2001, June 4, 2001.

〔5〕 NCA V-RER-05022, *USN 기술 동향 분석 연구*, 한국전산원, 2005.11.

〔6〕 NCA II-RER-05075, RFID 및 USN에 IPv6 적용 방안 및 활용 분야에 관한 연구, 한국전산원, 2005.11.

〔7〕 Bob Heile, "Emerging Standards: Where does ZigBee fit", ZigBee Alliance, 10. 2004.

〔8〕 ZigBee Alliance, "ZigBee Specification v1.0", 2005. 6.

〔9〕 ZigBee Alliance 홈페이지, http://www.zigbee.org

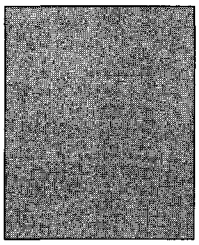
〔10〕 IEEE 802.15.4, *Wireless Medium Access Control*

(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society, 2003. 10.

[11] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향", 전자통신동향분석 제20권 제1호, 2005. 2.

[12] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/ NIST, Springfield, Virginia, 2001.11. Available from http://csrc.nist.gov/.

〈著者紹介〉



김 학 범 (Hak-Beom Kim) 종신회원

1990년 8월 : 중앙대학교 대학원 컴퓨터공학과 졸업(석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 (주)장미디어인터렉티브 상무이사
2005년 4월~현재 정보보호연구소 부소장
2001년 3월~현재 순천향대학교 공과대학 정보보호학과 겸임교수
관심분야 : 컴퓨터보안, 공개키 기반구조(PKI), 정보보호 표준화/평가, 스마트카드 보안, 유비쿼터스 보안