주 제

이종 무선 홈네트워크 Co-Existence 기술

아주대학교 이주아, 김재현

차례

I. 서 론

홈네트워크는 다양한 통신기술들을 집약하여 사용자들에게 더욱 편리한 생활을 제공하기 위한 통합 기술 형 서비스이다. 무선 홈네트워킹 기술은 유선 홈네트워킹 기술에 비하여 상대적으로 장치 가격이 고가이고 대역폭에 제한이 있으나 배선 작업이 필요 없는 장점과 전송 거리 범위 내에서 자유롭게 움직일 수 있는 편리함을 가지고 있다. 또한 유선에 비하여 네트워크 구조 변경이 쉽고, 설치와 유지 보수가 용이하다. 집안 전체에 무선 네트워킹을 제공하기 위해서는 무선 백본 망이 구성되어야 하며, 이러한 백본 망은 적어도 전송거리가 최소한 30m 이상을 지원하는 홈네트워킹 기술이어야 한다. 무선 전송기술로는 IEEE 802.11이나 IEEE 802.15.3 등을 고려할 수 있다. 이러한 무선 백본 망의 인터페이스를 가지는 기기는 프로토콜 변환 기능을 할 수 있는 브릿지 역할을 해야 하며, 이기종 네트워크간의 QoS 연동도 지원할 수 있어야 한다. 또한 개인 정보와 밀접하게 관련이 있는 홈네트워크의 특성상 보안이 중요한 문제이며 사용자의 미숙한 보안 지식으로 인해 보안에 틈이 생기지 않도록 사용자가 쉽게 사용할 수 있도록 연구되어야 한다.

본 고에서는 무선 접속 기술로서 급속하게 시장이 커지고 있는 IEEE 802.11 계열 프로토콜과 좁은 범위에서 다양한 통신 기기들의 접속을 가능하게 하는 IEEE 802.15 계열의 특성을 기술하였으며 각각의 기술에서 QoS를 제공하기 위한 방안과 보안 기법을 소개하고자 한다.

II. 무선 홈네트워킹 기술

1. IEEE 802. 11 무선 LAN 기술

IEEE 802.11의 무선 LAN 기술은 1990년대 초

〈표 1〉 IEEE 802.11 PHY 특성

Frequency		802.11a 5.2 GHz		802.11b 2.4GHz		802.11g 2.4GHz	
Data Rate (Mbps)	Carrier	PHY Modulation Scheme					
		Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	Single			DS/SS		DS/SS	
2	Single			DS/SS		DS/SS	
5.5	Single			CCK	PBCC	CCK	PBCC
6	Multi	OFDM				OFDM	CC-OFDM
9	Multi		OFDM				OFDM, CCK-OFDM
11	Single			CCK	PBCC	CCK	PBCC
12	Multi	OFDM				OFDM	CC-OFDM
18	Multi		OFDM				OFDM, CCK-OFDM
22	Single						PBCC
24	Multi	OFDM				OFDM	CC-OFDM
33	Multi						PBCC
36	Multi		OFDM				OFDM, CCK-OFDM
48	Multi		OFDM				OFDM, CCK-OFDM
54	Multi		OFDM				OFDM, CCK-OFDM

NCR 사가 Ethernet 칩을 사용하여 무선 전송을 시작한 제품을 선보이면서 시작되었다. 현재 IEEE 802.11 표준화 그룹은 2.4GHz 대역에서 최대 11 Mbps 전송 속도를 갖는 IEEE 802.11b, 5.7GHz 대역을 사용하여 최대 전송 속도 54Mbps를 제공하는 IEEE 802.11a와 2.4GHz 대역에서 OFDMA (Orthogonal Frequency Division Multiple Access)를 사용하여 최대 54Mbps를 제공하는 IEEE 802.11g로 나누어 볼 수 있다[1]-[3]. 그리고 무선 LAN에 QoS를 제공할 수 있도록 IEEE 802.11e에서 표준화 작업 중이며, IEEE 802.11n은 기존 무선 랜 주파수 대역인 2.4 GHz, 5 GHz에서 100~600Mbps을 지원하는 차세대 무선 LAN 기술이 연구중이다. 802.11a/b/g의 각각의 물리계층의 특성과 변복조방식에 따른 전송속도의 관계를 비교하면 <표 1>과 같다. 이때 <표 1>에서 CCK는 Comple-mentary Code Keying을 의미하며, PBCC는 Packet Binary Convolution Code를 의미한다.

기본적인 데이터 처리의 구조로 IEEE 802.11b의 MAC 프로토콜을 살펴보면 contention 서비스와 contention free 서비스로 구분하고 있다. Contention 서비스는 일반적인 인터넷 서비스로 파일의 전송과 같은 비동기성 데이터의 서비스를 담당하고 CSMA/CA 방식을 기본으로 하는 DCF (Distributed Coordination Function)에 의하여 처리된다[2]. Contention free 서비스는 음성이나 화상과 같은 지연에 민감한 전송에 대한 동기성 서비스로서 PCF (Point Coordination Function)에 의하여 처리된다. IEEE 802.11의 MAC 프로토콜에서는 CP (Contention Period) 서비스와 CFP (Contention Free Period) 서비스를 함께 처리할 수 있도록 설계되었다.

2. IEEE 802.15 무선 PAN 기술

무선 PAN 이란 무선으로 사람에게 인접해 있는 PC, PDA, 주변기기, 무선 전화기, 호출기, 가전제품 등이 상호 통신을 하여 적절한 환경을 구축하는 것을 목표로 하는 용어이다. 이에 IEEE 802.15 WG (Working Group)은 휴대형 및 모바일 컴퓨팅 기기를 위한 무선 PAN의 표준화를 위해 만들어 졌으며, 여러개의 TG(Task Group)로 나누어 각각 용도에 따라 표준화를 진행 중이다. 무선 PAN의 표준화를 담당하고 있는 TG 의 기술적 특성을 <표 2>에 비교하여 보았다.

〈표 2〉 IEEE 802.15의 TG의 기술적 특성

	802.15.1	802.15.3	802.15.3a	802.15.4	802.15.4a
Objectives	Bluetooth	High Rate	UWB	Low Rate/ Zigbee	위치인식 지전력 센서 네트워크
Frequency band	2.4~2.4835Ghz	2.4GHz	3.1GHz~10.6GHz	868/915MHz 2.4GHz	2.4 GHz
MAC	FH/TDD 79 Ch, 1600hop/sec	CSMA/CA, S-Aloha, TDMA		CSMA/CA TDMA	CSMA/CA TDMA
Topology	Piconet, Scatternet	Piconet, Child piconet, Neighbor piconet		Star, Peer2peer	Star, Peer2peer
Data Rate	< 1Mbps(sync.) < 723Kbps(Async.)	< 55Mbps	100Mbps at 10m 200Mbps at 4m path to 400Mbps	20k~250kbps	250kbps 1Mbps
Modulation	GFSK	QPSK, DQPSK, 16/32/64-QAM (11,22,33,44,55 Mbps)	QAM (if Multi -band OFDM)	BPSK (868/915MHz) O-QPSK(2.4GHz)	DBO-CSS
Range	10m(1mW) 100m(100mW)	5~10m		10~20m	100m+
Major Vender	Nokia, Sony, Ericsson	Xtreme spectrum, Timedomain		Philips, Motorola	Multispectral 삼성전기

IEEE 802.15.1은 10m 이내의 단거리에 놓여 있

는 컴퓨터 주변기기, 이동단말기, 가전제품 등을 상호 무선 네트워크로 연결하여 양방향 통신을 지원하는 기술인 Bluetooth의 표준화를 위하여 만들어졌으며, Bluetooth SIG (Special Interest Group)와 상호협력 하에 표준화가 진행되었다[4]. Radio 계층을 보면 2.4~2.4835GHz 대역의 ISM 밴드를 사용하고 1MHz 대역폭을 가진 79개의 채널로 이루어져 있으며, 초당 1600회의 주파수 호핑으로 전송한다. 변조방식은 G-FSK (Gaussian Frequency Shift Keying)를 사용하며 duplex 통신을 위하여 TDD (Time Division Duplex) 방식을 사용하여 무선 디지털 데이터 통신을 한다. 그러나 통상적인 데이터뿐만 아니라 음성 신호도 디지털 변조를 하여 전송할 수 있다. 송신 전력이 1mW 일 때 전송 거리가 10m 정도로 짧으나 출력에 여유가 있는 기기의 경우 전송 거리를 확장하기 위하여 전송 출력을 늘리는 것을 허가하여 100mW의 출력을 사용하는 경우 100m까지 전송 거리를 연장할 수 있다. Bluetooth 2.0의 경우는 1~2Mbps까지 구현 가능하다.

IEEE 802.15.3a는 UWB(Ultra Wide Band)를 사용하여 전송 속도를 크게 증가시키는 표준화 작업을 하고 있다. UWB란 중심 주파수 대비 대역폭이 20% 이상이거나 500MHz 이상의 주파수 대역폭을 차지하는 통신 방식을 의미한다. 현재 FCC에서는 UWB를 사용하는 경우 다른 무선 서비스와 간섭을 일으키는 것을 방지하기 위하여 매우 낮은 방사잡음 제한(EIRP)을 두고 있는데, 통신/측정 시스템에서 사용하는 3.1GHz~10.6GHz 대역의 경우 -41.3dBm/MHz을 준수하도록 엄격히 제한하고 있다. UWB 기술은 광대역에 넓게 퍼진 에너지를 수신하여 신호를 검출하므로 협대역 통신 신호에 의한 간섭 특성이 우수하고 보안 통신에도 적합하며 펄스폭이 매우 좁고 duty cycle이 작아 다중경로 페이딩에 의한 영향이 적다. 또한 반송파 발진기가 필요 없고, 고출력 통신을 행하지 않을 경우에는 선형 증폭기도 필요 없으며, 중간 주파수단도 사용하지 않으므로 시스템이 간단하다.

IEEE 802.15.4 LR-WPAN은 Bluetooth보다 낮은 20-250Kbps의 낮은 전송 속도와 매우 저렴한 가격, 매우 긴 배터리 수명, 간단한 구조 및 연결성을 제공하여 10m 이내의 작은 범위 내에서의 무선 연결을 요구하는 분야에 적합한 표준으로 개발되고 있다[5]-[7]. IEEE 802.15.4 프로토콜 계층구조는 기존 IEEE 802 표준과 동일하며, 물리계층과 데이터 링크 계층에 대해 관해서만 표준화되고 상위 계층의 프로토콜은 각각의 응용 환경에 따르도록 하고 있다. 이에 상위의 네트워크 계층에 관련된 사항으로 IEEE 802.15.4 표준안은 네트워크 계층에서의 소모 에너지 관리의 중요성을 감안하였다.

IEEE 802.15.4에서는 두 가지 물리계층(multi band, multi rate)을 지원하며 이들 물리계층은 low duty cycle과 저 전력 동작을 위하여 동일한 패킷 구조를 갖는다. 두 물리계층 사이의 근본적인 차이는 주파수 대역이며, 일반적으로 널리 활용되는 ISM 밴드인 2.4GHz와 유럽과 미국의 868/915MHz 대역으로 유럽에서는 868MHz 대역을, 미국에서는 915MHz 대역을 사용한다. 그리고 물리계층의 사용 대역에 따라 전송속도가 다르며 2.4GHz대역에서는 O-QPSK 변조방식에 의해 250Kbps의 전송속도를 제공하고, 868/915MHz 대역은 BPSK변조방식에 의해 각각 20Kbps와 40Kbps 전송속도를 제공한다. IEEE 802.15.4에서는 3개의 주파수 대역에서 27개의 채널을 갖는다. 868/915 MHz에서는 868.0MHz와 868.6 MHz 사이의 대역에서 하나의 채널을 902.0MHz와 928.0MHz 대역에서 10개의 채널을 제공한다. 2.4GHz에서는 2.4GHz와 2.4835GHz 사이의 대역에서 5MHz 간격으로 16개의 채널을 제공한다. 또한 근래에는 레이더에서 사용하고 있는 첩

(Chirp) 신호를 이용하여 위치정보를 이용하는 물리 계층 표준을 IEEE 802.15.4a에서 연구중이다. 그러나 현재까지 국내에서는 이러한 ISM 밴드대역의 중 900MHz 대역이 배정되어 있지 않기 때문에, 무선 PAN 및 RFID 등과 기술들의 주파수 배정 및 사용 문제가 대두되고 있다.

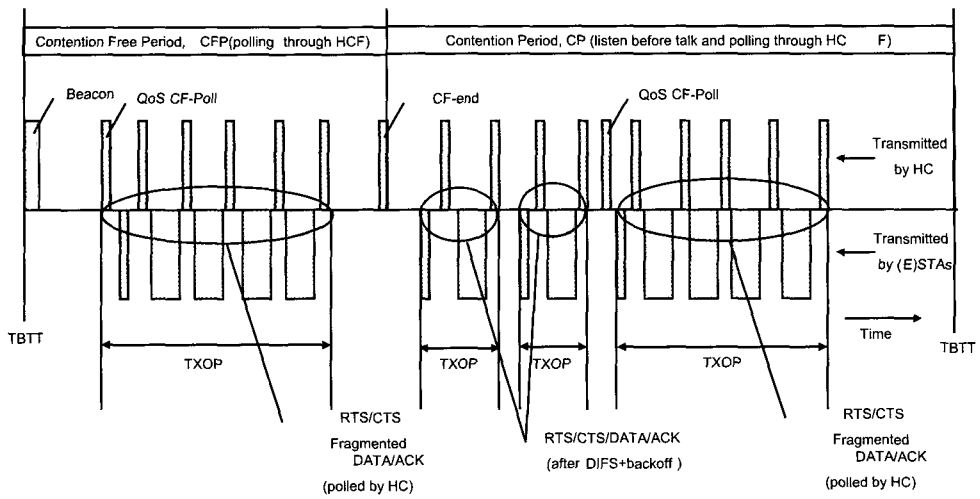
III. 무선 홈네트워킹 기술 QoS

1. IEEE 802.11 무선 LAN의 QoS 기술

IEEE 802.11 기반의 무선 LAN의 초기 시스템에서는 QoS에 대한 고려가 반영되어 있지 않았기 때문에 이를 위하여 IEEE 802.11e라는 새로운 WG을 결성하여 QoS 보장을 위한 연구를 진행하고 있다. 이 새로운 MAC 프로토콜은 크게 두 개의 기능으로 구분될 수 있다. 하나는 경쟁에 기반한 EDCA (Enhanced Distributed Channel Access) 방식이며 다른 하나는 polling에 의한 채널 제어 방식인 HCCA (HCF Controlled Channel Access) 방식이다.

EDCA는 기존의 DCF를 강화해 8가지 종류의 사용자 우선 순위를 가지는 프레임에 대해서 차별화된 매체 접근을 허용하고 있다. 상위 계층으로부터 MAC 계층에 수신된 각 프레임은 특정 사용자 우선 순위 값을 갖게되며, 각각의 QoS 데이터 프레임 MAC 헤더에는 사용자 우선 순위 값을 포함한다. 이들 우선 순위를 포함하는 QoS 데이터 프레임의 전송을 위해 802.11e 에서는 4개의 AC(Access Category)를 구성하고, 모든 AC는 각각의 전송 큐와 AC 파라미터를 가지며 각 AC마다 AIFS(Arbitration Inter Frame Space)에 의하여 전송 순위를 결정한다.

HCCA에서는 DLP(Direct Link Protocol)를 사용하여 HC(Hybrid Coordinator)의 도움 없이 QSTA(QoS STAtion) 사이에서 직접 데이터를 전송할 수 있도록 하였으며 두 번째로 다음 비콘 전에 MSDU(MAC Service Data Unit)의 전송을 끝낼

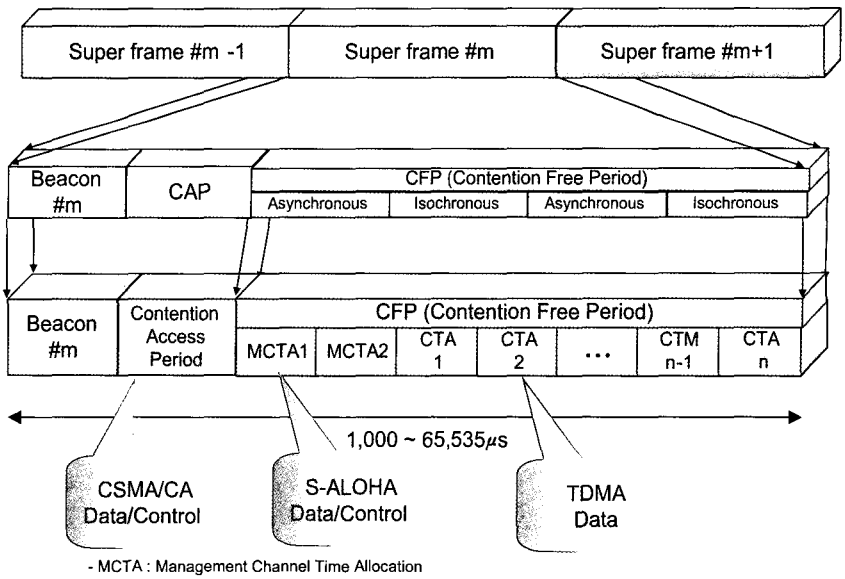


(그림 1) IEEE 802.11e의 HCCA 사용 예

수 없다면 전송을 하지 않고 잠시 연기하도록 하였다. 또한, IEEE802.11e에서는 기존의 성능 이상현상(performance anomaly)을 없애기 위하여, 서비스 종류에 따라 TxOP(Transmission Opportunity) Limit를 정하여 전송시간을 정확히 결정하도록 하였다. 또한 CFP 구간에서만 PCF를 사용할 수 있었던 것과는 달리 HCCA는 CFP구간뿐만 아니라 CP구간에서 PIFS(PCF Inter Frame Space) 시간 뒤에 CF-poll이 전송되면 CP 구간 동안 MSDU를 전송할 수 있는 장점을 가지고 있다. (그림 1)은 IEEE 802.11e에서 사용하는 HCCA 방식의 서비스 예를 나타내고 있다.

2. IEEE 802.15 무선 PAN의 QoS 기술

(그림 2)는 IEEE 802.15.3의 슈퍼프레임의 구조를 나타낸 것으로 크게 비콘, CAP (Contention Access Period), CFP (Contention Free Period)의 세 종류 블록으로 구성되어 있다. 이 중 CAP와 MCTA (Management CTA)는 모두 선택적으로 사용가능하며, 데이터 전송이나 시그널링 전송에 사용될 수 있다. CAP 영역은 IEEE802.11의 CSMA/CA (DCF) 방식을 토대로 랜덤 액세스 제어가 이루어지는데 반하여 MCTA는 Slotted Aloha방식을 이용하게 된다. CAP에서는 랜덤 액세스 제어를 통하여 선택된 서비스에 해당하는 페이로드(사용자 데이터)를 보낼 수 있는 시간 구간을 CFP에 할당한다. 스트리밍과 같은 동기 데이터도 CFP안에서 슬롯을 얻어 전송할 수 있고, 비동기 데이터의 경우 패킷의 크기에 따라 적절한 크기의 슬롯을 할당하여 전송할 수 있다. 데이터를 송신하는 시간 슬롯의 설정으로는 CTA (Channel Time Allocation)와 pseudo-static CTA가 사용된다. CTA의 경우 CTA의 위치를 슈퍼

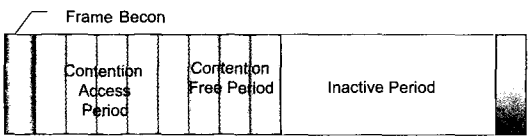


(그림 2) IEEE 802.15.3의 슈퍼프레임 구조

프레임마다 바꾸는 것이 가능하며, 비콘을 수신하지 못하면, 데이터 송수신을 하지 못한다. 반면 pseudo-static CTA의 경우 슈퍼프레임 마다 절대적인 전송 타이밍이 변하지 않으며 비콘을 몇 개 수신하지 못해도 계속 정해진 타이밍에 데이터를 송수신할 수 있다.

IEEE 802.15.4에서 coordinator는 기기들에게 비콘을 주기적으로 전송한다. 이때 연속된 2개의 비콘 사이의 시간을 활성(active) 구간과 비활성(inactive) 구간으로 분할하여 사용하는 슈퍼프레임 구조를 사용한다. 이 중에서 활성 구간의 시간에만 채널에의 접근이 허용되며, 비활성 구간에서는 모든 디바이스들이 수면 모드로 동작하기 때문에 기기의 저전력 소모가 가능해진다. 활성 구간은 real time 서비스를 제공하기 위하여 CAP 구간과 CFP 구간으로 구분할 수 있다. CAP 구간에서는 CSMA/CA 방식이 사용되며 다음 슈퍼프레임 비콘 전에 해당 데이터 송수신을 완료하여야 한다.

CFP 구간에서 coordinator는 요청을 받으면 기기에게 시간 슬롯을 할당해준다. 이같이 할당된 시간 슬롯을 GTS (Guaranteed Time Slot)라 하며 경쟁 없이 할당된다. 이러한 GTS의 수는 정해져 있지 않고 관련 네트워크 디바이스들의 요구에 따라 가변이다. (그림 3)은 GTS를 사용한 슈퍼프레임 구조를 나타내고 있다.



(그림 3) IEEE 802.15.4에서 GTS를 사용한 슈퍼프레임 구조

IV. 무선 홈네트워킹 보안 기술

1. IEEE 802.11 무선 LAN의 보안 기술

IEEE 802.11i TG는 무선랜 보안을 위한 표준 단체이며 RSN(Robust Security Network) 을 정의하고 있다[9]. RSN은 IEEE 802.11과 IEEE 802.11i를 지원하는 AP들이 공존하는 환경에서 IEEE 802.1X를 이용한 가입자 인증 및 키 관리 메커니즘, 무선구간 암호 알고리즘, 빠르고 안전한 핸드오프 보안 프레임워크를 제시한 새로운 형태의 보안 구조이다. RSN의 주요 보안 요소는 IEEE 802.1X 인증 메커니즘, 데이터 프라이버시 메커니즘, 그리고 보안 association 관리이다.

IEEE 802.1X는 논리적 포트 개념을 도입하여 링크 계층에서 IEEE 802 LAN을 인증하는 메커니즘을 제공한다[10]. 인증이 완료되기 이전에는 인증서버와 연결되어 있는 제어 포트(controlled port)를 통해서만 패킷이 전송될 수 있고, 인증이 완료된 이후에는 비제어 포트(uncontrolled port)를 통해서 외부 망과의 연결이 가능하다. IEEE 802.1X 표준안에서는 접근 제어를 위하여 요구자 (Supplicant), 인증자 (Authenticator) 및 인증서버 (Authentication Server)의 세 가지 개체가 정의된다. 요구자와 인증자 사이에서는 다양한 인증 방식을 수용할 수 있는 인증 프로토콜인 EAP (Extensible Authentication Protocol) 프로토콜을 통해서 인증을 수행하고, 인증자와 인증서버간 통신 프로토콜은 별도로 규정하고 있지 않지만 RADIUS (Remote Access Dial-In User Service) 프로토콜에 대한 기본적인 참조 모델을 제시하고 있다.

IETF EAP WG에서 표준화를 진행하고 있는 EAP 프로토콜은 사용자 인증을 위하여 특정 인증 방

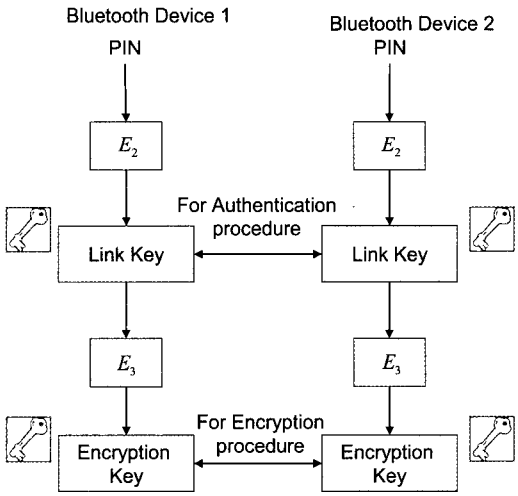
식을 지정하지 않고, 여러 인증 방식을 지원하는 프로토콜이다[11]. 즉, EAP 자체로는 실제 사용되는 인증 프로토콜을 지정하지 않고, 단지 인증 프로토콜을 사용하기 위한 기 본 절차만을 제공한다. 현재 표준화 중인 EAP 인증 방식은 EAP-MD5 (Message Digest 5), EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS) 등 여러 가지가 있으며 그 중 EAP-MD5 방식은 가장 초기의 인증 유형으로 패스워드를 기반으로 하는 인증 방식이다. EAP-TLS[12]는 단말기와 인증서버가 인증서를 이용하여 상호 인증하는 방식이고, EAP-TTLS[13]는 EAP-TLS의 확장 형태로 서버는 인증서를 이용하여, 단말기는 패스워드를 이용하여 인증하는 방식이다.

데이터 프라이버시를 제공하기 위해 IEEE 802.11i에서 사용하고 있는 암호화 알고리즘은 WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol), AES-OCB (Advanced Encryption Standard-Offset Codebook)가 있다.

2. IEEE 802.15 무선 PAN의 보안 기술

IEEE 802.15.1은 다음과 같이 세가지 보안 모드 중 한가지로 운영될 수 있다[14].

- Security Mode 0 (non-secure): 암호화나 인증이 사용되지 않는다.
- Security Mode 1 (service level enforced security): 보안 관리자가 인증을 수행한다.
- Security Mode 2 (link level enforced security): 기기가 네트워크에 참여하기 위해서는 인증을 수행하여야 하며 데이터가 암호화되어 전송된다.



(그림 4) Bluetooth 키 생성

IEEE 802.15.1에서 암호화를 위한 키는 1~6 바이트 정도의 PIN (Personal Identification Number) 코드를 사용하여 생성되며 PIN 코드는 사용자가 직접 입력한다. 또한 IEEE 802.15.1에서는 키를 생성하기 위해 E 알고리즘을 사용하는데, (그림 4)와 같이 E2는 인증키 생성을 위한 알고리즘이며, E3은 암호화 키 생성을 위한 알고리즘이다. E2 알고리즘은 PIN 코드를 기반으로 하여 16 바이트의 링크 키를 생성한다. 이렇게 생성된 링크키는 인증을 위해 사용되며 E3 알고리즘의 입력값으로도 사용되어 암호화를 위한 키를 생성한다.

링크키를 사용하는 인증 과정은 다음과 같으며 A 기기가 B 기기로부터 인증 받는다고 가정하였다.

1. A기기는 B기기와의 접속을 위하여 48 비트의 주소를 전송한다. 이 주소는 MAC 주소와 유사하며 기기 제조사를 이 주소로 알 수 있다.
2. B기기는 128 비트의 랜덤한 수를 생성하여 A 기기에게 전송한다.
3. A기기와 B기기는 48 비트의 주소와 랜덤한 수,

링크키 값을 이용하여 SRES (Signed Response)라는 인증 응답 스트링을 생성한다.

4. A기기는 SRES를 B기기에게 전송하며 B기기는 자신이 생성한 SRES와 동일한 값이면 A기기의 접속을 허락한다.

IEEE 802.15.1 보안에서 PIN 코드는 공개적으로 전송되지 않지만 중간에서 해커가 48 비트의 주소와 랜덤한 수, SRES를 가로채면 해킹이 가능하다. 또한 링크키를 생성하기 위하여 사용자가 각각의 기기에게 PIN 코드를 직접 입력해야하는 불편함이 있으며 사용자가 입력하는 PIN 코드의 길이가 짧을수록 쉽게 공격받을 수 있다. 마지막으로 Dos와 DDos 공격은 네트워크와 기기에 대한 가용성을 손실시키며 기기의 배터리를 빠르게 소모시킬 것이다. 따라서 이러한 위험을 감소시키기 위해서는 다차원적인 부분에서 위협 요소에 대한 대책을 고려해야 한다[15].

IEEE 802.15.3 보안서비스는 신뢰성 성립, 기기 인증, 키 관리, 적시성 (Freshness) 보호, 무결성, 암호화의 항목을 지원하도록 하고 있다[16]. PNC (Piconet coordinator)는 피코넷 자원의 사용을 제어하며 보안 관리자의 역할을 하고, 상위 계층에서 다른 기기와의 신뢰성을 확인하기 위하여 공개키 같은 신뢰 관계를 정의하며 피코넷 내에서 사용될 보안 정책을 정의한다. MAC/PHY 계층에서는 인증을 하며 대칭키를 관리하고 명령과 데이터 메시지의 암호화를 담당한다.

(그림 5)에서 보는 바와 같이 PNC와 각 기기간에 보안 관계를 성립하는 과정을 보면 다음과 같다.

① 기기들은 어떤 기기가 PNC로 적당한지 결정하고 동의한다.

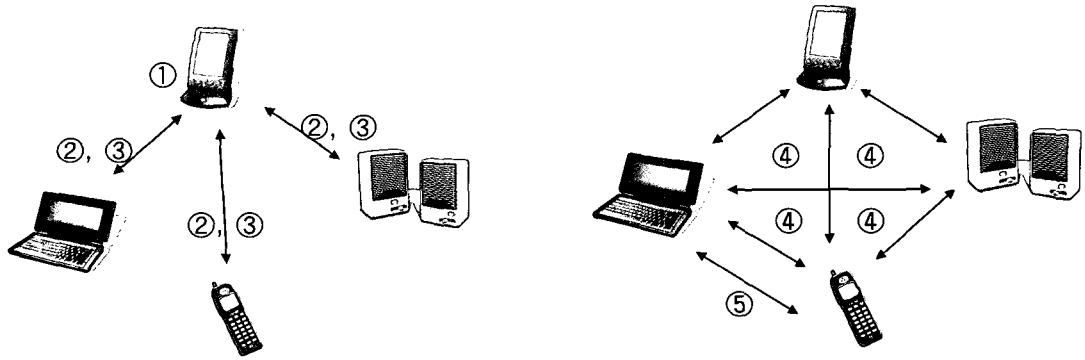
② 각 기기들은 피코넷에 참여하기 위한 요청 메시지를 전송하고 PNC와 상호 인증을 수행한다.

③ PNC는 각 기기들을 위해 시간 슬롯을 결정하고 피코넷에서 전송되는 데이터를 암호화하기 위한 키를 분배한다.

④ 기기들은 다른 기기와의 통신을 위하여 정해진 시간 슬롯 동안 암호화된 데이터를 전송한다.

⑤ 두 기기간은 자신들만의 안전한 subnet을 형성할 수 있다.

기기들과 PNC간의 상호 인증은 공개키를 이용하며, TLS 핸드쉐이크 방식과 비슷한 절차로 수행된다. 이러한 인증 프로토콜을 통하여 secure association이 수립되면 PNC는 그룹키를 각 기기들



(그림 5) UWB 인증 과정

에게 암호화하여 전송한다. 그룹키는 기기가 네트워크에 참여하거나 네트워크를 떠날 때마다 변경이 된다. 만일 PNC의 역할이 변경되면 각 기기들은 새로운 PNC와 인증 과정을 다시 거쳐야 한다.

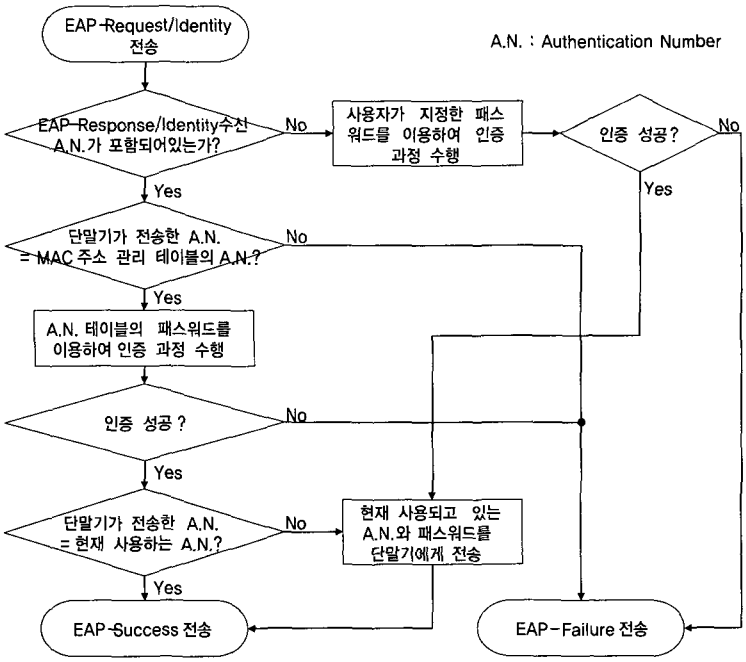
IEEE 802.15.4 에서 지원하는 보안의 종류는 다음과 같다[17].

- 적시성 – replay 공격을 방지하기 위하여 incoming and outgoing freshness counter를 사용하며 counter는 새로운 키가 생성되면 다시 시작한다.
- 메시지 무결성 – 공격자가 전송되는 메시지의 변조를 방지하기 위하여 패킷의 마지막에 MIC (Message Integrity Code)를 붙여 패킷의 무결성을 체크한다. 0, 32, 64, 128 비트의 MIC를 제공하며 메시지 보호와 메시지 오버헤드 간에 tradeoff가 있다.
- 인증 – 메시지를 만들어 보낸 기기 또는 사용자가 네트워크를 이용할 자격이 있는지를 판단하기 위해 인증이 필요하다. 인증은 네트워크 레벨이나 디바이스 레벨에서 가능하다. 네트워크 레벨에서의 인증은 네트워크 키를 이용하며 디바이스 레벨에서의 인증은 서로 통신을 하는 두 기기간의 유일한 링크 키를 이용하여 이루어진다.
- 암호화 – 중간에서 메시지가 도청당하는 것을 방지하기 위하여 128 비트의 AES 암호화 기법을 사용한다. 네트워크 키와 링크 키를 이용하여 네트워크 레벨고 디바이스 레벨로 데이터를 암호화하여 패킷을 전송할 수 있다.

IEEE 802.15.4 에서는 coordinator를 trust center로 가정하고 있으며 이를 이용하여 네트워크에 참여하려는 기기를 인증하며 키를 관리하며 분배한다

3. 홈네트워크의 보안 기술

홈네트워크 보안에서 가장 중요한 것은 사용자와 디바이스를 인증하는 것과 그 사용자의 권한을 제한하는 접근제어라 할 수 있다. 사용자와 디바이스를 인증하는 방식은 ID/패스워드, 인증서, 생체인식 등이 있지만 현재는 ID/패스워드와 인증서 방식만이 제한적으로 구현 가능한 수준이다. 그러나 홈네트워크의 다양한 무선 기술을 적용하기 위해서는 경량화된 인증 방법이 필요하며 사용자가 편리하게 이용할 수 있는 방법도 제시되어야 한다. 인증서를 이용한 방식은 무선 LAN에서는 사용 될 수 있겠지만 무선 PAN 기술에 적용하기에는 무리가 있으며 사용자의 개입을 최소화하는 인증서 분배 방식이 제안되어야 한다. 반면에 ID/패스워드 방식은 무선 PAN 기술에도 적용될 수 있지만 인증을 할 때마다 사용자가 ID/패스워드를 입력해야하는 불편함과 인증서 방식보다 보안에 취약하다는 단점이 있다. 이를 해결 하기 위해서는 사용자가 처음 기기 설치 과정에서 한 번만 패스워드를 입력하면 그 이후에 패스워드가 인증서버에 의하여 자동적이고 주기적으로 변경되는 방식을 생각해 볼 수 있다. (그림 6)은 무선 LAN에서 변경되는 패스워드 방식을 적용한 예를 보여준다. 인증서버에서는 인증을 위한 패스워드를 주기적으로 변경시키며 패스워드가 변경 될 때 마다 랜덤한 숫자를 할당하고 이를 authentication number라고 한다. 그리고 인증서버에서는 두 개의 테이블을 관리하며 하나는 MAC 주소 관리 테이블로 인증된 단말기의 MAC 주소와 사용하고 있는 패스워드의 authentication number를 기록해 놓는다. 다른 하나는 authentication number 관리 테이블이다. 패스워드가 변경 될 때마다 변경된 패스워드와 함께 랜덤한 authentication number를 저장한다. 제안하는 인증 방식은 사용자에게 전문적인 지식을 요구하지 않고, 자동적으로 패



(그림 6) 제안하는 인증 프로토콜

스워드 변경이 이루어지기 때문에 처음 인증 이후에는 사용자의 개입을 요구하지 않는다. 또한 이러한 방식은 사용자의 편의성뿐만 아니라 홈네트워크의 보안을 강화시킬 수 있다[18].

V. 결 론

본 고에서는 홈네트워크에서 적용 가능한 다양한 무선접속기술에 대하여 기술하였다. 그 중 현재 널리 사용되고 이는 IEEE 802.11 무선 LAN 계열의 특성을 알아보았으며, IEEE 802.15 무선 PAN 계열의 표준화 프로토콜의 특성을 정리하였다. 이러한 무선 홈네트워킹 기술은 근래에들어 홈네트워크 환경에서 멀티미디어 서비스를 제공할 수 있도록 해주는 QoS도 중요한 이슈로 떠오르고 있다. 무선 LAN의 경우 어느 정도의 QoS는 보장하지만 아직 IEEE 802.11e의 표준화 작업이 완료되지 않아 보장된 QoS의 제공이 어려우며, 무선 PAN의 경우 저속이거나 또는 고속의 전송이 가능하지만 프로토콜의 복잡성과 망 구성의 연결 등이 보장되지 않을 수 있다는 단점이 있다. 이러한 홈네트워킹 무선 기술이 효율적으로 연동하기 위해서는 각 접속 기술별로 정의된 QoS 파라미터 맵핑 기술과 접속 기술별로 상이한 전송률에 따른 자원을 효율적으로 관리할 수 있는 자원 관리 기술이 필요하다. 또한 무선 기술은 태생적으로 보안에 한계가 있으며 특히 홈네트워크 서비스는 개인의 신상 정보와 밀접하게 관련이 있기 때문에 홈네트워크에서의 보안은 중요한 문제이다. 그러나 아직까지 홈네트워크를 위한 보안은 초기 단계이며 뚜렷한 통합 보안 솔루션이 미비한 실정으로 홈네트워크 사용자의 편의를 고려한 안전한 보안 기술에 대한 연

구는 계속될 것으로 전망된다. 결론적으로 홈네트워크에서 사용될 여러가지 무선 기술들의 원활한 사용을 위해서는 각 기술의 특성을 고려한 QoS의 연동 및 보안 기술이 고려되어야 하며 이를 기반으로 하는 홈 네트워킹 기술의 표준화가 이루어져야 한다.

감사의 글

본고는 2006년에 시행된 2 단계 BK21(Brain Korea 21)과 전자통신연구원의 지원에 의하여 작성되었습니다.

[참 고 문 헌]

[1] IEEE 802.11a-1999(R2003) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 1: High-speed Physical Layer in the 5 GHz band.

[2] IEEE 802.11b-1999(R2003) Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.

[3] IEEE 802.11g-2003 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[4] IEEE 802.15.1(tm)-2002 Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs(TM)) Gemma Paulo Wireless Cribs, "Living Large with a Wireless Home Network,: 10. 2002.5. Specification of the Bluetooth System v1.1, 2.2001.

[5] IEEE P802.15.4-2003 Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) pecifications for Low Rate Wireless Personal Area Networks (LR-WPANs), 2.2003.

[6] Venkat Bahl, "Zigbee Overview," The ZigBee Alliance, September 2002.

[7] Venkat Bahl, "ZigBee and Bluetooth-Competitive or Complementary?," The ZigBee Alliance, September 2002.

[8] S. Chung and K. Piechota, "Understanding the MAC impact of 802.11e: Part 2" http://www.commsdesign.com/showArticle.jhtml articleID=16502136.

[9] IEEE, LAN/MAN Specific Requirements ? Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i, Jul. 2004.

[10] IEEE, Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control, IEEE Std 802.1X, Jun. 2001.

[11] B. Aboba et al., "Extensible Authentication Protocol," IETF RFC 3748, Jun. 2004.

[12] B. Aboba, "PPP EAP TLS Authentication Protocol," IETF RFC 2716, Aug. 1999.

[13] P. Funk, "EAP Tunneled TLS Authentication Protocol," internet draft, Jul. 2004.
[14] ARGUS Advanced Remote Ground Unattended Sensor System, Department of Defense, U.S. Air Force, http://www.globalsecrurity.org/intell/systems/arguss.htm
[15] http://www.cqcom.com/document.html
[16] http://www.ieee802.org/15/pub/TG3.html
[17] http://www.ieee802.org/15/pub/TG4.html
[18] J. A. Lee, J. H. Kim, J. H. Park and K. D. Moon, "A Secure Wireless LAN Access Technique for Home Network," in Proc. IEEE VTC' 06-Spring, Melbourne, Australia, May. 7-10, 2006.

이주아

2005년 아주대학교 전자공학부 학사
2005년 ~ 현재 아주대학교 대학원 전자공학과
관심분야 : 무선 LAN 보안, 센서 네트워크

김재현

1991년 한양대학교 전산과 학사
1993년 한양대학교 전산과 석사
1996년 한양대학교 전산과 박사
1997년 ~ 1998년 미국 UCLA 전기전자과 박사후 연수
1998년 ~ 2003년 Bell Labs, Performance Modeling and QoS Management Group, 연구원
2003년 ~ 현재 아주대학교 전자공학부 조교수
관심분야 : 무선 인터넷 QoS, MAC 프로토콜, IEEE 802.11/15/16/20