무선 LAN 통신망의 기술 동향

강영진* 김성남* 강신일* 이영실* 이훈재**

*동서대학교

**동서대학교 컴퓨터정보공학부

Technologies trend for Wireless LAN

Sung Nam Kim* · Sin Ill Kang** · Hoon Jae Lee***

*Computer Engineering, **Information and Communication Engineering, Dongseo University

***Div. Computer and Information Engineering, Dongseo University

E-mail : rkddudwls55@naver.com, wave88, ksiync, youngsil.lee0113@gmail.com, hjlee@dongseo.ac.kr

요 약

무선 LAN(Wi-Fi: Wireless Fidelity)은 스마트폰 대중화와 더불어 급속히 확대되는 통신망으로 컴퓨터, 노트북, 태블릿 PC 그리고 스마트폰 등 다양한 기기가 접속되어 유비쿼터스 기반의 핵심 네트워크로 자리 잡아 가고 있다. 현재 많은 무선 LAN 통신 기술이 개발되어 다양한 데이터 전송이 가능해졌으며, 표준인 IEEE 802.11n은 2.4GHz 대역과 5GHz 주파수 대역을 사용하고 있다. 2.4GHz 대역은 파장이 길고 회절 및 수신 거리가 좋아서 802.11b/g 방식으로 널리 보급되었다. 5GHz 주파수 대역은 2.4GHz보다 활용할 수 있는 더 많은 채널을 가지고 있어 블루투스, RFID 등 다른 무선 장치의 주파수 대역과 간섭이 없으며 주파수 사용자가 적어 채널 간섭이 적은 특징을 가지고 있다. 본 논문에서는 초기부터 사용된 802.11b/a/g과 현재 사용되고 있는 802.11n 기술 분석 및 동향 그리고 최근 차세대 무선 LAN 통신망으로 대두되고 있는 802.11ac와 802.11ad의 개발 현황 및 표준화 방향에 대하여 살펴본다. 또한, 무선 LAN 보안 취약점 및 이용 현황과 추가적인 대책 방안에 대하여 논하고자 한다.

ABSTRACT

Wi-Fi is a rapidly spreading communications network with Smart phone's publication, the technology has become Ubiquitous-based core network which is connected to personal computers, laptops, and tablet PC. Wi-Fi can send currently a variety of data standard due to developed wireless LAN communications network. One of Wi-Fi standard protocols, which is IEEE 802.11n, use 2.4GHz and 5GHz band. 2.4GHz band is used for 802.11b/g protocol because wavelength is long, diffraction and receiving distance is enough to connect other device. 5GHz band has more available channels to use than 2.4GHz band, so there is no frequency interference of other wireless device such as Bluetooth, RFID. Moreover, there is low interference between channels due to small users in each bandwidth level. In the thesis, we are going to analyze 802.11a/b/g protocol which has used since the beginning of Wi-Fi protocol and 802.11n protocol which is used lately. Furthermore, we look into development and direction for standardization of the next generation wireless LANs which are 802.11ac and 802.11ad. In addition, we will consider for the security, vulnerabilities and its countermeasure in Wireless LAN .

키워드

무선LAn 표준, 무선LAN 기술 동향, 차세대 무선LAN통신, 802.11ac/ad

Ⅰ. 서 론

무선 LAN(Wi-Fi: Wireless Fidelity)은 스마트폰 대중화와 더불어 급속히 확대되는 통신망으로 컴퓨터, 노트북 등 다양한 기기에 접속되어 사용되고 있으며, 유비쿼터스 기반의 핵심 네트워크로 자리 잡아 가고 있다. 현재 많은 무선 LAN 통신 기술이 개발되어 다양한 데이터 전송이 가능해졌으며, 이 중 표준인 IEEE 802.11n은 2.4GHz 대역과 5GHz 주파수 대역을 사용하고 있다. 2.4GHz는 파장이 길고 회절 및 수신 거리가 좋아서 802.11b/g 방식으로 많이 사용되고

있으며, 5GHz 대역은 2.4GHz보다 활용할 수 있는 더 많은 채널을 가지고 있어 블루투스, RFID 등 다른 무선 장치의 주파수 대역과 간섭이 없으며 주파수 사용자가 적어 채널 간섭이 적은 특징을 가지고 있다.

무선 LAN은 유선 LAN과는 달리 기본적으로 모든 단말에 데이터를 전송하는 브로드캐스팅 망이므로, 액세스 포인트의 비콘(Beacon) 프레임 수신 영역 내에 있는 모든 단말은 다른 사람의 송수신 데이터 내용을 청취할 수 있어 의도된 수신자 이외의 다른 사람으로부터 데이터를 보호하기 위해서는 기밀성 및 무결성 서비스와 상호인증 서비스가 매우 중요하다. 현재 대부분의 무선 LAN 보안 방식으로 WEP 보안방식이 이용되고 있으나, 이에 대한 보안 취약점이 알려지면서, 무선 LAN 해킹을 위한 깊은 지식 없이 간단한 인터넷 검색만으로 해킹 툴을 다운받아 공격을 시도할 수 있다. 이에 추가적으로 WAP, WAP2 보안 등도 등장하여 사용되고 있으나 아직 대중화되지는 못하였다.

이에 본 논문에서는 먼저 현재 사용되고 있는 802.11 표준 기술[1]에 대하여 살펴보고 관련 기술들을 분석한다. 더불어 최근 차세대 무선 LAN 기술로 대두되고 있는 802.11ac[2]와 802.11ad의 개발 현황 및 표준화 방향에 대하여 서술하도록 한다. 또한 이들 무선 LAN 통신망을 통해 발생 가능한 보안 취약점 및 이를 위한 보안 기술들[3-4]에 대하여 고찰하고자 한다.

II. 관련연구

2.1. 802.11 표준

802.11은 2Mbps의 최고속도를 지원하는 무선 네트워크 기술로, 적외선 신호나 ISM 대역인 2.4GHz 대역 전파를 사용해 데이터를 주고 받으며 여러 기기가 함께 네트워크에 참여할 수 있도록 CSMA/CA 기술을 사용한다.

802.11b는 802.11 규격을 기반으로 더욱 발전시킨 기술로, 최고 전송속도는 11Mbps이나 실제로는 CSMA/CA 기술의 구현 과정에서 6-7Mbps 정도의 효율을 나타내는 것으로 알려져 있다. 표준이 확정되자마자 시장에 다양한 관련 제품이 등장했고, 이전 규격에 비해 현실적인 속도를 지원해 기업이나 가정 등에 유선 네트워크를 대체하기 위한 목적으로 폭넓게 보급되었다.

두 번째로 등장한 전송방식인 802.11a는 5GHz 대역의 전파를 사용하는 규격으로, OFDM 기술을 사용해 최고 54Mbps까지의 전송속도를 지원한다. 5GHz 대역은 2.4GHz 대역에 비해 다른 통신기기(무선 전화기, 블루투스 기기 등)와의 간섭이 적고, 더 넓은 전파 대역을 사용할 수 있다는 장점이 있지만, 신호의 특성상 장애물이나 도심 건물 등 주변 환경의 영향을 쉽게 받고, 2.4GHz 대역에서 54Mbps 속도를 지원하는 802.11g 규격이 등장하면서 현재는 널리 쓰이지 않고 있다.

세 번째로 등장한 802.11g 규격은 a 규격과 전송 속도가 같지만 2.4GHz 대역 전파를 사용한다는 점만 다르다. 널리 사용되고 있는 802.11b 규격과 쉽게 호환되어 현재 널리 쓰이고 있다.

802.11n은 상용화된 전송규격이다. 2.4GHz 대역과 5GHz 대역을 사용하며 최고 600Mbps 까지의 속도를 지원하고 있다. IEEE 802.11n-2009 표준은 최대 600Mbps까지 대역폭을 넓힐 수 있으며 MIMO(multiple-input multiple-output) 와 40MHz 채널 대역폭을 가진 물리 계층(physical layer), 맥 계층(MAC layer)의 프레임 집적(frame aggregation) 기술을 추가하여 만들어졌다. MIMO와 넓은 채널 대역폭을 이용해서 물리 계층의 전송 속도를 802.11a (5GHz)나 802.11g (2GHz)에 비해 향상시킬 수 있다.

IEEE 802.11 TGi는 기존의 802.11 무선LAN에 QoS와 보안을 강화하기 위해 결성된 TGe에서 무선LAN 보안 부분만을 따로 분리하여 2001년 만들어졌다. 기존의 취약했던 인증 및 키 분배문제를 802.1X가 맡을 수 있도록 프레임 워크를 제공하며, WEP로 사용하돈 암호화 방식을 ASE(Advanced Encryption Standard) 등 새로운 방식으로 대체해 802.11 무선망에서의 보안을 강화한 것이다. 802.11i는 802.11의 기존 인증방식에 ULA(ULA(Upper Layer Authentication)를 추가하였다. 인증을 ULA로 선택한 경우 오픈 시스템 또는 쉐어드키 인증 과정 없이 곧바로 조합 과정을 거치게 된다. 조합이 성공하면, 사용자에 대한 인증 및 통신은 상위 계층은 802.1x에서 수행하게 된다.

802.11 network standards

802.11 Protocol	Release[4]	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)[5]	Typ throughput (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate Outdoor range (m)
–	Jun 1997	2.4	20	1, 2	0.9	1	DSSS	20	100
a	Sep 1999	5 3.7[5]	20	6, 9, 12, 18, 24, 36, 48, 54	23	1	OFDM	35	120 5000[5]
b	Sep 1999	2.4	20	1, 2, 5.5, 11	4.3	1	DSSS	38	140
g	Jun 2003	2.4	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	19	1	OFDM, DSSS	38	140
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[2]	30-130[6][7]	4	OFDM	~70	~250[8]
			40	15, 30, 45, 60, 90, 120, 135, 150[2]					

그림 1. IEEE 802.11 protocols

2.2. 무선 LAN 통신망의 보안 취약점

현재 무선 LAN보안은 허술한 설정과 허술한 암호화로 인한 취약점 두 가지가 있다. 무선 네트워크는 설치와 적용이 매우 쉬워 보안 설정이 전혀 없거나 부적절하게 되어 있는 경우가 많다.

2.2.1. 무선 환경의 물리적 특성에 의한 취약점

- 위협요소 : Rogue AP

- 악의 적인 용도로 내/외부인이 Ap를 설치하여 내부 정보의 유출 및 공격이 가능하다.

● 위협 요소 : Mis-configured AP
- AP의 보안설정이 되지 않아, 비인가자가 불법으로 접속이 가능하다.

● 위협요소 : Ad-Hoc 연결
- 외부 비인가자와 내부의 인가된 사용자가 Ad-Hoc 방식으로 네트워크를 구성하여 불법적으로 접근이 가능하다.

● 위협 요소 : Mis-associations
- 무선 단말은 자동으로 SSID를 검색하여 성공적으로 연결하려는 특성이 있어 의도하지 않게 다른 Ap와 연결될 수 있다.

2.2.2. 인증 및 암호화 메커니즘의 취약점

● 위협 요소 : Unauthorized associations
- 비인가자가 내부의 허가된 Ap에 불법적으로 접속하는 경우

● 위협요소 : Denial of Sevice
- 많은 수의 사용자가 동시에 이용하는 기업이나 서비스 사업자에게 상당히 위협적인 공격, 공격자가 Ap로 위장하여 사용자의 AP 접속을 방해합니다.

● 위협 요소 : MAC Spoofing
- 외부 Ap가 사내 Ap와 동일하게 보이기 위해 사내 AP의 MAC 주소와 SSID를 동일하게 복제 한다[2].

Ⅲ. 차세대 무선 LAN통신 기술

3.1. 802.11ac

수백 Mbps 이상의 초고속 전송 속도를 요구하는 멀티미디어 서비스를 이용하려는 사용자의 대부분이 주로 유목적 환경에서 서비스를 사용하고 있는 실정이다. 따라서 OFDM을 이용하는 고속 무선 LAN 계열 서비스의 중요성이 날로 높아지고 있으며, 최근에는 최대 600Mbps까지 지원하는 IEEE802.11n 기반의 무선 LAN 제품이 시장에서 팔리고 있다.

IEEE 802.11n 은 MIMO, LDPC, Aggregation 등의 핵심 기술을 활용하여 기존 IEEE 802.11a에 비해 PHY 에서의 최대 성능을 54Mbps에서 600Mbps 로 11배 가까이 속도가 늘어났으며, 더불어 동작 범위는 대폭 늘리고 신호의 품질 또한 향상되었다. 그래서 요즘 이슈가 되고 있는 Full HD급 동영상을 무선으로 재생할 수 있는 기술로 기대 되고 있다.

VHT Study Group의 논의에 있어서 주요한 특징으로는 기존에 802.11n이 사용하는 5GHz대역 주파수 자원의 포화 가능성으로 인하여 기존 PAN 서비스에 사용되었던 60GHz 대역이 VHY 서비스를 위한 또 하나의 가능한 주파수 자원으로 제시되었다는 것이다. 따라서, VHT 규격에 대한 논의는 5GHz 대역을 사용하는 VHTL6 와 60GHz 대역을 사용하는 VHY60로 이원화 되어 정식 TG로 전환되어 802.11ac 라는 이름으로 본격적인 표준화를 시작하였다.

3.2. 802.11ad

802.11ad 규격은 새롭게 사용할 60GHz 스펙트럼을 사용하기 위해 오늘날 Wi-Fi에서 쓰여지고 있는 2.4GHz나 5GHz의 영역을 사용하지 않는다. 왜냐하면 이 60GHz 스펙트럼 영역은 미국을 포함한 거의 대부분의 나라에서 사용가능하기 때문이다. 따라서 압축되지 않은 각각의 영상을 1Gbps가 넘는 속도로 전송하기 위해 이 스펙트럼 영역에서 다중의 분리된 채널을 사용하게 될 것이다. 하지만 불행하게도, 60GHz의 신호를 이루고 있는 밀리미터 길이의 파장은 벽과 가구를 잘 통과하지 못하며, 산소가 이 파동의 에너지를 쉽게 흡수해 버린다. 따라서 802.11ad는 같은 방 안에 있는 기기 사이의 짧은 거리 사이의 데이터 전송에 가장 적합하다. 802.11ad는 USB 3.0의 속도 또는 블루투스 2보다 1,000배 더 빠르게 장치들 사이에서 파일 전송 및 데이터를 동기화를 가능하게 할 것이다. 802.11ad 규격은 스펙트럼의 60GHz 영역을 사용하기 위한 경쟁력 있는 아이디어이다. WiGig(Wireless Gigabit Alliance)가 네트워킹과 소비자 사용을 주시하는 반면, 소비자 전자기기 회사의 협회인 무선 HD(Wireless HD)는 60GHz 영역의 영상 사용에 대해 초점을 맞추고 있다. 이렇게 다양한 단체의 회원들은 겹치기 때문에 아마도 통합될 가능성이 있는 규격으로 만들 것으로 관측된다. 비록 802.11ad는 영상에 대해서 구체적으로 언급하고 있지는 않지만, 많은 종류의 데이터 사용에 대한 편의를 도모할 수 있는 포괄적인 기술이 될 것으로 보인다.

Ⅳ. 무선 LAN 보안 대응 현황

현재 무선 LAN 보안은 AP 관리자 권한 획득 및 시스템 해킹, 비인가 AP 설치 및 허가받지 않은 접근 시도 등의 문제에 있어 취약점을 가짐을 알 수 있다. 이러한 공격에 대응하기 위해서는 추가적인 보안 기술 적용 및 대책이 필요한 시점이다.

그에 대한 대응 방안으로 사용되고 있는 WEP 보안은 가장 기본적인 보안기능 제공 상태로써 무선 단말과 액세스 포인트가 WEP 키를 공유하는 공유 키 인증방식을 사용하며, 공유된 키를 통해 WEP 암호화 기능을 수행한다. 이러한 WEP 보안은 사용자 인증, 접근제어, 데이터 기밀성을 지원한다. 처음 사용은 정적인 WEP 키

전개방식이었으나, 이는 WEP 알고리즘 자체가 IV(Initialization Vector)의 평문전송, 키 스트림의 단순성으로 인하여 악의적인 공격자에 의해 WEP 키 값이 노출될 수 있는 취약한 알고리즘인데다 하나의 액세스 포인트를 사용하는 다수의 사용자가 동일한 WEP 키를 사용하기 때문에 공중망 서비스의 개별 사용자 보호라는 측면에서 볼 때는 보안 기능의 의미가 없게 된다. 따라서 현재, 동적인 WEP 키 전개방식을 사용하고 있다. 그러나 이 방법 역시 보안적 측면에서 사용자 인증, 접근제어, 데이터 기밀성 기능만을 지원하며, 데이터 무결성, 부인방지, 안전한 핸드오프 등의 보안에 대해서는 여전히 취약하다 할 수 있다.

이후 WEP의 문제점을 해결하기 위해 WPA(Wi-Fi protected access), WPA2 보안이 등장하였다. 먼저 WPA는 IEEE의 802.11i 표준이 완성될 때까지 임시로 사용되는 표준으로, 원래의 Wi-Fi 보안 표준인 WEP 보다 개량된 것이다. WPA는 WEP에 비해 보다 정교한 데이터 암호화를 제공하는 것은 물론, 사용자 인증이 다소 불충분했던 WEP와는 달리 완전한 사용자 인증 기능을 제공한다. WEP은 그리 복잡하지 않은 가정용으로는 아직도 유용하지만, 대량의 메시지 흐름으로 인해 암호화키가 보다 신속하게 발견될 수 있는 기업용에는 충분치 않다. 이후 등장한 WPA2는 AES 알고리즘이 적용되는 데, 사실상의 산업 암호화 표준으로 DES와 3DES를 대체하고 있다. 계산이 필요한 집약적인 AES는 하드웨어 보조를 필요로 하는데, 이는 구형 무선랜 장비에서 발견되곤 한다. WPA2는 데이터와 MIC를 암호화할 수 있는 CTR(Counter Mode)와 인증, 보존을 위해 CBC-MAC(Cipher Block Chaining Message Authentication Code) 프로토콜을 사용하며, 대용량의 데이터가 전송되는 기업용을 위해 주로 사용되고 있다.

무선 프로토콜별 비교

구 분	WEP	WPA	WPA2
인 증	N/A	IEEE 802.1x/EAP/PSK	IEEE 802.1x/EAP/PSK
암호화 알고리즘	RC4	RC4	AES
키 사이즈	40또는 104비트	128비트	128비트
암호화 방법	WEP	TKIP	CCMP
데이터 무결성	CRC-32	마이클(MIC)	CCM
프레임당 키잉	No	Yes	Yes
IV 길이	24비트	48비트	48비트

그림 2 무선 프로토콜별 비교

V. 결 론

본 논문은 초기부터 사용된 802.11b/a/g와 현재 사용되고 있는 802.11n 기술 분석 및 동향 그리고 최근 차세대 무선 LAN 통신망으로 대두되고 있는 802.11ac와 802.11ad의 개발 현황 및 표준화 방향에 대하여 살펴보았다.

근거리 무선 환경에서 다양한 멀티미디어 서비스 요구가 지속적으로 증가하고 스마트 폰 등 무선 서비스를 이용하는 디바이스들의 발전으로 인해, 현재 최대 600Mbps까지 지원 가능한 IEEE 802.11n 기반의 무선 LAN 제품이 시장에 퍼지고 있다. 그러나 초고화질 영상을 압축하지 않고 전송하려면 Gbps 이상의 전송 속도가 필요하다. 따라서 새로운 표준 제정을 위한 움직임이 일고 있으며, IEEE 802.11ac, 802.11ad 등 차세대 무선 LAN 기술의 개발 및 표준화를 진행하고 있다.

또한 기존의 무선 LAN 보안을 위해 WEP 보안을 사용하고 있으나, 이는 심각한 취약점을 가지는 것으로 밝혀졌으나, 아직까지 일반 기업과 가정에서는 계속 사용되고 있다. 또한 WEP 보안의 보안 취약점을 해결하기 위하여 추가적으로 WAP, WAP2 보안 등이 제시되고 있으나, 아직까지 대중화가 되지 않고 있다.

이러한 점을 미루어 보아, 무선 LAN 보안을 위한 가장 중요한 점은 기술의 개발과 더불어, 다양한 매체들을 통한 사용자의 인식 변화가 그 무엇보다 우선된다 할 수 있다.

참고문헌

[1]http://ko.wikipedia.org/wiki/IEEE_802.11
[2] 정보통신산업진흥원, “IEEE 802.11ac Gigabit 무선랜 표준화 동향”, 주간기술동향 통권 1429호, 2010. 1.
[3] 강유성, 오경희, 정병호, “무선랜 보안기술의 진화동향 및 전망”, 전자통신동향분석 제18권 제4호, 2003. 8.
[4] 김성훈의 네트워크, “무선 네트워크 보안”, http://www.hardnara.com/kimsnetwork/