

# 차세대 무선 LAN 기술 동향

## Technologies for Next Generation Wireless LAN

김윤주(Y.J. Kim) 차세대무선LAN연구팀 연구원  
 김명순(M.S. Kim) 차세대무선LAN연구팀 연구원  
 이석규(S.K. Lee) 차세대무선LAN연구팀 선임연구원, 팀장  
 황승규(S.K. Hwang) 무선전송기술연구그룹 책임연구원, 그룹장

홈 네트워크, 기업의 무선 네트워크 그리고 핫스팟 등과 같은 다양한 환경이 가능하면서 무선 LAN 기술 및 무선 LAN 제품에 대한 요구는 더욱더 증가하고 있으며, 기존 제품과의 호환성을 바탕으로 고속으로 무선 데이터 서비스를 지원할 수 있는 차세대 무선 LAN 기술에 대한 관심이 집중되고 있다. 본 논문에서는 현재 표준화가 진행중인 IEEE 802.11n의 차세대 무선 LAN 기술에 있어 주요하게 언급되고 있는 MAC 프로토콜 및 전송방식들에 대하여 소개한다. IEEE 802.11n은 IEEE 802.11e에서 논의중인 EDCA 및 HCCA를 기반으로 QoS를 보장하고 고속의 무선 LAN 서비스를 지원하기 위해 보다 개선된 MAC 프로토콜의 요구사항을 정의하여 물리계층의 관점에서 MIMO, spatial division multiplexing, space-time block coding 등과 같은 다중 안테나 방안을 고려하고 있다. 또한 주파수의 효율을 증가시키는 방식, 대역폭을 증가하는 방식 그리고 적응 변조를 적용하는 방식 등을 차세대 무선 LAN 전송 방식으로 논의하고 있다.

## 1. 서론

무선 LAN 기술은 유선 네트워크에 비하여 속도가 낮기 때문에 특정한 환경의 일부 사용자에 의해서만 이용될 수 있는 기술로 여겨졌었다. 그러나 1999년 IEEE 802.11 매체 접근 제어(Medium Access Control: MAC) 프로토콜 및 2.4GHz 대역에서의 IEEE 802.11b와 5GHz 대역의 IEEE 802.11a 전송기술의 표준이 정의되고, 또 802.11b 무선 LAN 시스템이 상용화되어 널리 사용되기 시작하였고, 802.11a와 g 전송방식을 기반으로 하는 제품들이 연이어 출시되면서 현재에는 무선으로 54Mbps의 데이터 전송이 가능한 무선 LAN 기술이 가능하다. 이러한 무선 LAN 기술은 무선 매체를 통한 전송과 함께 고속이라는 특성을 동시에 지원할 수 있기 때문에 기존의 유선 네트워크와 접목되는 경우, 가정에서 사용하는 유선 네트워크 망과 연동하여 홈 네트워크 또는 호텔이나 카페, 사무실 등과

같이 좁은 지역을 중심으로 무선 LAN 서비스를 지원하므로 무선 LAN 기술을 응용한 다양한 시장이 점차적으로 형성되고 있다. 따라서 그 영향력을 넓히고 있는 무선 LAN 기술과 이를 기반으로 고속을 지원할 수 있는 차세대 무선 LAN 시스템에 대한 관심과 연구가 집중되고 있다.

무선 LAN 서비스의 범위를 홈 네트워크, 기업의 무선 네트워크 그리고 핫스팟(hot-spot) 등으로 확장하고자 하는 차세대 무선 LAN 기술은 2003년 9월부터 활동을 시작한 IEEE 802.11n이라는 작업 그룹(Task Group: TG)에 의하여 표준화가 진행중이며, 기존의 802.11a와 g의 호환성을 지원하며 동시에 고속으로 무선 데이터 서비스를 지원하는 것을 목표로 하고 있다. 이를 위해 IEEE 802.11n은 물리계층의 관점에서 다중 안테나를 이용하여 주파수의 효율을 증가시키는 방식, 대역폭을 증가하는 방식 그리고 적응 변조를 적용하는 방식 등을 고려하고 있다. 또한 기존의 표준 규격 제정의 경우에 있었던

내용과는 달리 단순한 물리계층의 전송률이 아닌 MAC 계층에서의 최대 스루풋을 100Mbps 이상으로 높이는 것을 목표로 하고 있으며, 기존의 무선 LAN 기술이 유선 best-effort 서비스만을 지원하기 때문에 무선 이더넷에서 벗어날 수 없었던 한계를 극복하고 무선 환경에서 Voice over IP(VoIP), Audio/Video(AV) 스트리밍 등 멀티미디어 통신을 지원하고자 한다. 다시 말해서, 차세대 무선 LAN 기술에 대한 표준화 작업은 단순히 물리계층만을 고려하는 것이 아니라 물리계층과 MAC 계층을 동시에 고려하고자 하는 것에 있다.

본 논문에서는 기존 무선 LAN 기술인 IEEE 802.11 MAC 프로토콜 및 IEEE 802.11 a/b/g의 물리계층 규격에 대해서 살펴보고 IEEE 802.11 TGn에서 차세대 무선 LAN MAC 프로토콜을 기반으로 하는 IEEE 802.11e MAC 프로토콜과 차세대 무선 LAN 전송방식에 대하여 알아본다. 또한 차세대 무선 LAN을 통해 전송되는 데이터에 대한 인증 및 보안을 지원하기 위해 802.11 TGi에서 정의하고 있는 RSNA(Robust Security Network Association) 보안 메커니즘을 함께 살펴본다.

## II. IEEE 802.11 기술 개요 및 표준화 동향

현재까지 완료된 무선 LAN 표준은 IEEE 802.11을 기본으로 하여, 3개의 추가 문서(amendment)인 IEEE 802.11a, b, d로 구성되어 있다. IEEE 802.11 1999 Edition[1]-[3]에는 MAC 계층과 DSSS, FHSS(Frequency Hopping Spread Spectrum), IR(Infrared) 물리계층이 포함되어 있다. 이 중에서 DSSS 방식은 802.11b에 반영되면서 아직까지 쓰이고 있다고 할 수 있고, FHSS는 IEEE 802.15 WPAN의 물리계층과 동일하여 그 자취가 남아 있지만, IR 방식은 완전히 사장되었다. 802.11b에는 2.4GHz 대역에서 1, 2Mbps를 위한 DSSS와 5.5, 11Mbps를 위한 CCK 방식을 이용하는 물리계층 규격을 기술하고 있고, 이것은 802.11의 MAC과 결합하게 되어

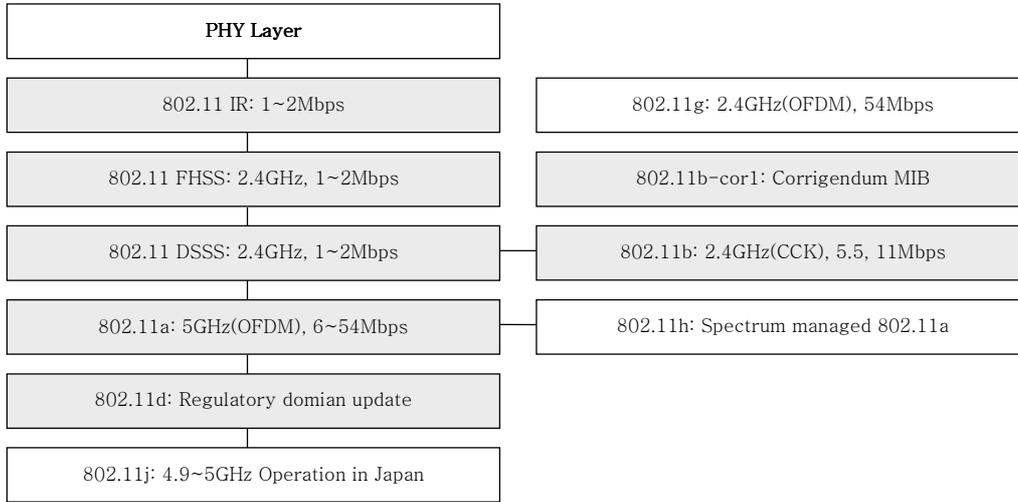
있다. 802.11a는 5GHz 대역에서 6~54Mbps를 제공할 수 있도록 OFDM 방식을 이용한 물리계층을 정의하고 있다. 802.11a 역시 MAC은 기존의 802.11의 MAC에서 약간의 변수만을 변경하는 형태로 구성되어 있다.

802.11d는 특정 물리계층이나 MAC을 정의하는 것이 아니라 다른 규제영역(regulatory domain)을 위해서 802.11에서 추가되거나 수정되는 부분을 설명하고 있다. 그리고 802.11b-cor1이 있는데, 이것은 802.11b에서 추가 및 수정 부분을 정리한 것이며 본 논문에서는 언급하지 않는다. 이와 더불어 현재까지 TG을 통하여 표준화를 진행하고 있는 부분들에 대하여 알아보자. 간단히 정리하기 위해서 기존의 표준들과 같이 물리계층과 MAC 또는 같이 다루는 부분으로 나누어 그림으로 나타내면(그림 1)과 같다.

(그림 1)에서 어둡게 되어 있는 부분은 언급한 바와 같이, 현재 정식표준이 공개되었으며, 802.11g도 표준화가 완료되어 공개를 앞두고 있는 상황이다.

802.11g는 지난 2000년 6월에 IEEE standards board에 의해서 최종 승인을 얻은 상태이다. 여기에서는 2.4GHz ISM 대역에서 기존의 802.11b와 호환성을 유지하면서 20Mbps 이상의 전송속도를 달성하기 위한 목적으로 시작되었다. 그래서 기존 802.11b의 DSSS 1, 2Mbps와 CCK 5.5, 11Mbps 그리고 802.11a의 OFDM 방식 중에서 6, 12, 24Mbps를 필수사항으로 채택하여 20Mbps를 달성하였다. 그리고 802.11a에서 정의했던 나머지 전송 모드와 ERP-PBCC(Extended Rate PHY-Packet Binary Convolutional Code), DSSS-OFDM이 선택 사항으로 들어간다. 그리고 스루풋을 향상시키기 위한 짧은 슬롯타임 모드가 추가되고, 기존의 802.11b로부터 802.11g의 프레임 보호하기 위한 보호 메커니즘(protection mechanism)도 추가되었다[4].

802.11h는 802.11a에 시스템 성능 향상 및 레이더와 같은 간섭을 고려, 주파수의 효율적인 사용을 위한 TPC(Transmit Power Control)와 DFS(Dynamic



(그림 1) 802.11 물리 계층에 관련된 표준 그룹의 구조

Frequency Selection) 기능을 추가하는 것이다. 그러나 이것은 유럽의 5GHz 대역의 규제를 만족시키기 위한 목적이 강하며 802.11 무선 LAN 시스템의 유럽 시장 진출을 위해서 시작한 것이라고 할 수 있다. 이것 역시 현재는 거의 마무리 단계에 와있다.

802.11j는 지난 2002년에 일본에서 할당된 4.9~5GHz의 무선접속서비스를 위한 물리계층을 802.11a를 기반으로 만드는 것을 목표로 하여 2002년 하반기에 시작되었다. 여기서는 아직 기술적인 내용이 정해지지 않았지만, 기존의 802.11a에서 클럭속도를 반으로 낮추어 10MHz의 대역폭을 갖는 선택사항을 추가하여 실외 환경에 대응하는 형태로 진행될 것으로 예상된다.

802.11e는 802.11의 DCF 전송방식을 근간으로 하며 동시에 MAC 계층에서 QoS 프로토콜을 지원할 수 있는 EDCA 및 HCCA를 정의[5]함으로써 best effort 데이터 외에도 비디오 스트림이나 음성 데이터 등 전송 지연에 민감한 트래픽을 전송할 수 있는 enhanced MAC 프로토콜에 대한 표준화를 진행 중이다.

802.11f는 IEEE 802.11 무선 LAN 기술을 분산 시스템(distribution system)에서 서로 다른 사업자들이에 의해서 운용되는 AP 장비들 사이에 상호 작용을 수행하기 위해 무선 단말의 이동 과정에서 AP와

AP 사이의 핸드오프 방안인 Inter-Access Point Protocol(IAPP)을 정의하고 있다. IEEE 802.11f에서 표준화가 진행된 문서는 2003년 7월에 공개되었으며, 현재 IEEE 802.11f와 함께 IETF의 SEAMOBY WG(Work Group)에서 seamless 및 authenticated fast-handoff를 지원하는 방안에 대한 표준화가 진행 중이다.

802.11i는 기존 무선 LAN 보안 메커니즘인 WEP을 보완하여 802.1X(802.1aa)와 EAP 프로토콜을 사용하는 RSNA 인증 시스템과 무선 LAN 암호화 알고리즘으로 RC4 보다 강력한 AES 기반의 수학적 암호화 메커니즘을 정의[6]하고 있으며 2004년 말에 표준화 작업이 완료될 것으로 기대되고 있다.

802.11k는 다양한 물리계층에서 사용하는 전파 자원 측정에 대한 향상을 위해 전파 및 네트워크 측정을 위한 상위계층이 갖는 메커니즘을 제공하는 것을 목적으로 2003년 초에 활동을 시작하였고, 현재 드래프트 0.14를 기반으로 수신신호 파워, noise, hidden nodes 등을 고려하며 다양한 무선 자원의 측정방안에 대한 논의를 진행하고 있다.

마지막으로 WNG SC는 IEEE 802.11 그룹의 새로운 안전이 있을 때, 이를 공문화할 수 있는 창구역할을 하는 그룹이다. 최근 이 그룹에서는 2003년 9

월부터 DSRC study group을 구성하여 차량간의 또는 차량과 노변 장치 사이의 통신을 위한 물리계층을 정의하는 TG를 구성하려는 준비작업을 하고 있다. 또한, fast roaming study group과 ESS mesh networking study group을 구성하여 해당 스킴을 정의하는 TG 구성에 관한 준비작업이 완료된 상태이다.

### III. 차세대 무선 LAN 기술 개요

#### 1. TGn(802.11n)의 개요

IEEE 802.11TGn은 차세대 무선 LAN에 대한 새로운 표준 그룹을 만들기 위해서 만들어진 TG이다. 처음에는 단순히 802.11a/g의 전송속도를 높이는 것을 목표로 논의가 되었으나, 802.11 MAC 계층의 한계를 뛰어넘지 않고서는 물리계층에서의 전송률 향상이 아무런 의미가 없다는 의견이 나오면서 MAC까지를 동시에 고려하여 MAC에서의 스루풋을 향상시키려는 목적의 TG를 구성하는 것으로 방향이 전환되었다. 2002년 5월 회의에서 차세대 무선 LAN 기술을 연구하는 새로운 HTSG의 구성을 승인 받았으며, 2002년 9월 회의부터 study group으로서의 활동을 시작하였다. 또한, TG으로서의 활동의 시작은 2003년 9월이다.

TG의 범위 및 목표 등을 나타내는 PAR(Project Authorization Request) 문서[7]와 TG의 가치나 다른 TG과의 차별성 등을 기술하는 5 criterion 문서[8]가 study group에 의해서 작성되었다. 이렇게 만들어진 PAR에서 가장 중요한 부분이라고 할 수 있는 목표는 MAC SAP에서의 최대 스루풋을 적어도 100Mbps를 달성하기 위해서 기존의 802.11의 물리계층과 MAC 계층을 수정 추가하는 것이다. 그래서 현재의 MAC만을 고려할 경우에는 적어도 전송률을 4배 증가하여 200Mbps 이상을 달성해야 MAC에서 최대 100Mbps의 스루풋을 낼 수 있을 것으로 생각된다. 그리고 추가적으로 설명한 부분에서는 기존의 802.11a와 g와의 호환성을 보장하는 모드도 존재해야 한다는 것을 규정하고 있다. 그리

고 홈 네트워크, 기업 네트워크, 핫스팟을 그 응용분야로 하고 있고, 주파수 효율을 3bits/sec/Hz 이상이 되어야 한다고 규정한다. 이 PAR와 5 criterion에 대하여 다른 TG 및 WG의 이견을 해결한 후에 2003년 7월에 ExCom(Executive Committee)의 최종 승인을 얻었다. 9월 회의부터 802.11n이라는 TG으로 활동을 시작하였다. 또한, 2004년 1월부터 제안들을 받기 시작하였으며, 7월까지 이들 제안에 대한 선정을 마무리할 예정이며 7월에 첫번째 802.11n에 대한 초안을 작성하는 것을 계획으로 하고 있다. 지난 5월 L.A. 회의에서는 8월 13일까지 규격 제출을 완료하고 9월 베를린 회의 때부터 제안된 규격들에 대한 발표와 후보 규격들을 선정하기 위한 일정이 확정되었다. 이후로 최종 후보 규격이 나올 때까지 계속해서 투표를 통해 최종 후보 규격을 TGn에서 선정하게 된다. 표준의 최종 승인은 2005년 하반기 정도로 예상되고 있다.

#### 2. 차세대 MAC 프로토콜

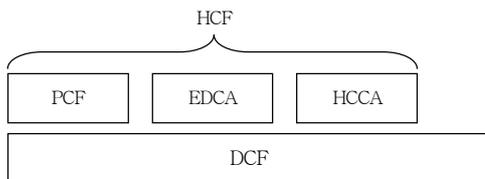
IEEE 802.11에서 정의하는 MAC 프로토콜은 기본적으로 CSMA/CA를 이용하는 DCF 전송 방식에 기반을 두고 있으며, 무선 매체를 접근하는 데 있어 단말과 단말 사이의 우선 순위를 고려하지 않는다. 이러한 특성은 다양한 형태의 데이터 전송을 반영하지 못하며, QoS를 지원할 수 없다. IEEE 802.11에서는 AP에서 단말에 대한 서비스를 직접 제어하는 PCF 전송 방식을 또한 정의하고 있지만, 데이터 특성에 따른 서비스는 지원하지 않으며 널리 구현되고 있지 않으므로 효율적인 면은 거의 없다. 이에 본 장에서는 IEEE 802.11 TGn 표준화 과정에 의해 MAC SAP에서의 최대 100Mbps 스루풋을 지원하고 홈 네트워크 등 다양한 서비스를 지원해야 하는 요구사항을 갖는 차세대 무선 LAN 시스템의 특성을 고려하였을 때, 802.11n에서 제시하는 기능적인 요구사항(FR)에 적합한 QoS 메커니즘 및 다양한 추가적인 요소를 포함하는 IEEE 802.11e의 enhanced MAC 프로토콜의 구조를 살펴보기로 한다.

가. IEEE 802.11e Enhanced MAC 프로토콜 개요

IEEE 802.11 TG e는 IEEE 802.11의 DCF 및 PCF 프로토콜을 기반으로 하는 HCF(Hybrid Co-ordination Function)을 정의한다. HCF는 DCF에 의해 제어되는 CP(Contention Period)와 PCF에 의해 제어되는 CFP(Contention Free Period) 동안 QoS 데이터를 전송할 수 있는 메커니즘으로, 경쟁(contention)을 기반으로 하는 EDCA(Enhanced Distributed Channel Access)와 채널에 대한 무선 단말의 접근을 제어하는 HCCA(HCF Channel Access)로 구성되며 동시에 legacy MAC과의 호환성을 지원한다.

(그림 2)는 802.11 DCF 서비스와 함께 802.11 PCF와 802.11e HCF를 지원하는 enhanced MAC 프로토콜의 구조를 보여준다. 802.11 DCF 전송방식은 중앙에서 매체접근을 제어하는 PCF 또는 HCF 전송방식과 함께 동일한 BSS 서비스를 지원한다. 특히 QBSS에 존재하는 HC(Hybrid Coordinator)는 CP 동안에만 동작하는 DCF나 CFP 동안에만 동작하는 PCF와 달리, 채널이 CP 서비스를 지원하는 동안에도 contention-based인 EDCA와 polled 기반의 HCCA의 동작을 모두 지원한다.

HCF를 지원하는 QSTA은 하나 이상의 채널 접근 메커니즘을 사용하여 무선 매체를 통해 frame exchange sequence의 전송을 시작하고 프레임 전송을 계속 유지할 수 있는 권한을 얻는다. 이러한 권한은 802.11e에서 transmission opportunities (TXOPs)으로 정의되며, 전송의 시작 시점을 기준으로 하여 일정한 시간 동안 이루어진다. 802.11e enhanced MAC 프로토콜에서는 일반적으로 경쟁에 의해 획득된 EDCA TXOP과 controlled channel



(그림 2) 802.11e MAC Architecture

접근 방식에 의해 얻어진 HCCA TXOP, 특히 QoS(+) CF-Poll에 의해 얻어진 polled TXOP을 정의하고 있다.

나. EDCA 프로토콜

EDCA 전송방식은 8개의 서로 다른 우선 순위 (User Priority: UP)를 갖는 QSTA이 무선 매체에 대하여 차별화되고 분산되어 접근할 수 있도록 정의하고 있다. IEEE 802.1D 브리지 규격에서 정의하는 데이터의 QoS 우선순위를 따라서 규정된 UP는 <표 1>과 같이 각각의 트래픽 특성에 따라 다시 4개의 Access Categories(AC)로 분류되어 각 우선 순위에 따라 독립적으로 EDCA의 서비스를 제공 받는다.

이 때, 서로 다른 우선 순위를 갖는 각 AC에 대한 TXOP contention은 AIFS[AC], aCWmin[AC], aCWmax[AC] 등과 같이 QAP의 dot11QAPEDCA Table MIB와 non-AP QSTA의 dot11EDCATable MIB에 저장되어 있는 EDCA 파라미터 세트의 각 변수를 사용하여 독립적으로 이루어지며, 전송하고자 하는 프레임이 존재하는 각 AC들은 (그림 3)에서 보이는 것과 같은 IFS 관계를 가지므로 경쟁을 통해 매체에 대한 접근을 시도한다.

각 AC에 따른 AIFS[AC]의 계산 식을 통해서 얻어진 값은 각 AIFS(Arbitration Interframe Space)의 값으로 설정되며, 개별적인 AC에 대하여 존재하

<표 1> User Priority

Priority	User Priority (UP)	802.1D Designation	Access Category (AC)	Designation
Lowest ↓	1	BK	AC_BK	BackGround
	2	-	AC_BK	BackGround
	0	BE	AC_BE	BestEffort
	3	EE	AC_BE	BestEffort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

는 채널 접근을 위한 타이머는 매체가 busy에서 idle로 상태가 전이되는 순간 각 트래픽의 우선 순위에 따라서 결정된 AIFS[AC] 동안 채널이 idle인지 기다리고, 채널이 idle이면 백오프 과정을 수행한다.

각 AC가 갖는 독립적인 채널 접근방식은 (그림 3)에서 보이는 것과 같이, 앞서 설명한 AIFS[AC] 값을 사용함으로써 contention을 기반으로 수행된다.

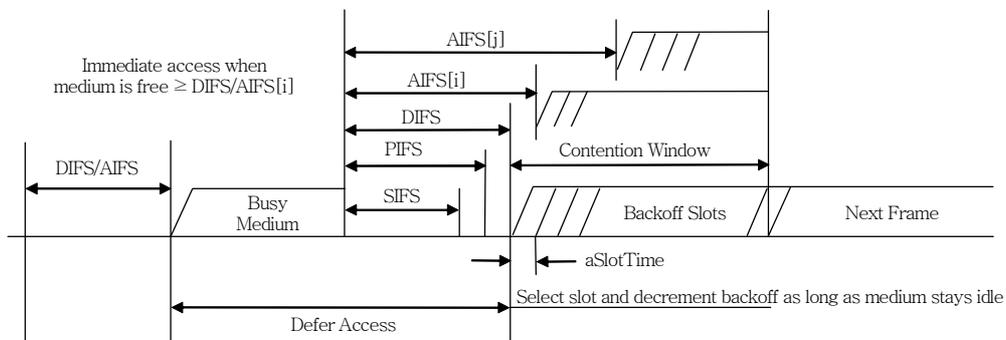
이때, Non-AP QSTA의 AIFSN[AC]는 '2'와 같거나 큰 값으로 QAP가 전송하는 비컨이나 probe response에 포함되어 각 STA에게 전달된다. 반면 QAP의 AIFSN[AC]는 '1'이거나 '1'보다 큰 값을 유지하게 된다. EDCA의 각 AC는 AIFS와 백오프 타이머를 통해 채널에 대한 점유를 획득하게 되면 EDCA TXOP을 얻을 수 있다. EDCA 전송방식은 STA의 어떤 AC가 TXOP 동안 전송을 성공적으로 유지하면, 전송할 프레임이 존재하지 않더라도 ACK 프레임을 수신하거나 임의의 frame exchange sequence가 성공적으로 전송된 후에 계속 채널에 대한 접근 권한을 시도할 수 있는 포스트 백오프 과정을 지원한다. 이렇게 AP와 각 STA의 AC에 따라서 관리되는 TXOP은 QAP에 의하여 알려진 TXOPLimit을 초과할 수 없다. 만약 TXOPLimit 값이 '0'으로 전달된다면 이는 RTS/CTS 또는 CTS 프레임의 전송을 포함하여 하나의 MSDU 또는 MMPDU를 전송할 수 있는 시간만을 할당할 수 있다는 것을 의미한다. 따라서 EDCA 전송과정에 있어 TXOP은 non-AP QSTA이 외부 영향 없이 무선

매체를 제어할 수 있는 시간으로 정의되기 때문에 TXOP holder에 의해 전송된 프레임의 응답 프레임을 성공적으로 수신하기 위한 시간을 모두 고려해야 한다.

다. HCCA 프로토콜

8개의 UP에 따른 트래픽이 다시 4개의 AC로 분류되어 서비스를 제공 받는 EDCA는 prioritized QoS를 지원하며, 이와 달리 HCCA는 QAP와 QSTA 사이에 지원하고자 하는 트래픽의 특성을 변수(parameters)로서 구분하고 분류하여 각 특성에 맞는 QoS 서비스를 제공하는 parameterized QoS를 정의한다. 특히 HCCA를 위한 QAP의 HC는 QoS-aware centralized coordinator 기능을 수행하며 CP와 어떤 CFP 기간 동안 TC 또는 TS의 QoS 요구사항을 파악하여 HC 자신이나 QSTA에게 TXOP을 할당하는 전송 방식으로, HC가 각기 다른 TC 또는 TS 특성을 갖는 트래픽의 양을 얼마나 파악하고 있는지, 또는 QBSS의 특정한 QoS 정책이 무엇인가에 따라서 TXOP의 할당 및 관리를 수행할 수 있다.

따라서 HCCA의 AP는 parameterized QoS 트래픽을 교환하기 전에 교환될 트래픽 스트림(Traffic Stream: TS)의 특성(characteristics)을 정의하는 프레임을 교환함으로써 QoS 및 트래픽 전송에 대한 요구 사항을 서로 교환한다. 이 때 교환되는 트래픽의 특성으로는 nominal MSDU size, mean data rate, maximum burst size 등이 있고



(그림 3) EDCA IFS Relationships

이와 함께 QoS 요구사항 및 스케줄 정보 등이 있다. HC는 CFP 또는 CP 내의 TXOP을 시작하기 위하여 무선 매체의 상태가 idle 인지 또는 busy인지 감지한다. 만약 PIFS 구간동안 채널의 상태가 idle 이라면 HC는 CFP 또는 TXOP 동안 전송될 수 있는 frame exchange sequence 내의 첫번째 프레임의 전송을 시작한다. HC가 PIFS 동안 채널이 idle 로 감지된 후에 획득한 CAP(Channel Access Phase)는 연속적인 TXOP이나 하나 이상의 polled TXOP로 이루어지며, CP 또는 CFP와 함께 (그림 4)와 같이 구성된다. 이에 동일한 QBSS 내의 모든 QSTA와 QoS 정보가 교환된 HCCA의 HC는 non-AP QSTA보다 더 높은 매체 접근 권한을 갖기 때문에, non-AP QSTA에게 MSDU를 전송하고 TXOP을 할당할 수 있다. 또한 CP와 CFP 동안에 모두 QBSS에 연결된 QSTA에게 데이터를 전송할 수 있으므로 QoS(+) CF-Poll 프레임에 명시된 기간 동안에 non-AP QSTA에게 polled TXOP을 할당할 수 있다.

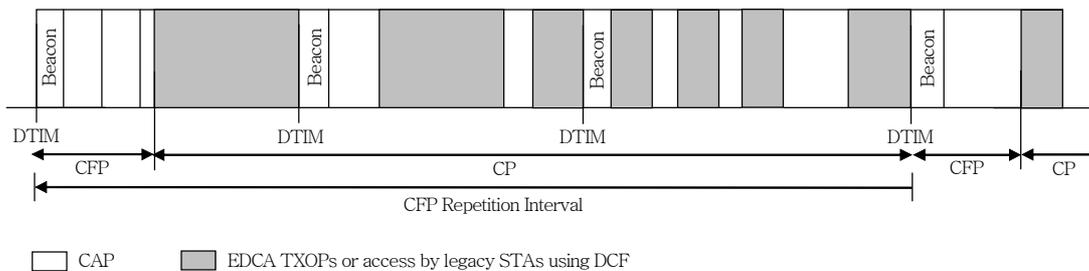
CF-Poll을 포함하는 QoS 데이터는 TXOPLimit 값을 포함하며, polled TXOP은 QoS(+) CF-Poll을 포함하는 프레임의 duration 값으로 NAV를 설정함으로써 유지된다. Polled TXOP은 SIFS로 구분되는 하나 이상의 frame exchange sequence의 전송으로 구성되며, 남아 있는 TXOP 내에서 ACK 또는 적절한 response를 수신함으로써 frame exchange sequence가 완료되지 않는다면 다른 프레임의 전송을 시작하지 않는다. 따라서 TXOPLimit 값은 응답 프레임을 수신하는 동작도 함께 고려하지만 최대 TBTT, dot11CFPMaxDuration, dot11MaxDwellTime 또

는 dot11CAPLimit은 초과하지 않은 값으로 설정되어야 한다.

EDCA와 HCCA 채널 접근 방식 외에도 802.11e의 enhanced MAC 프로토콜은 기존의 802.11 MAC 프로토콜이 stop-and-wait과 ARQ를 기반으로 프레임의 전송에 대하여 반드시 ACK 프레임을 송신함으로써 채널에 대한 낭비를 극복하기 위해 블록 ACK 기법을 정의하고 있다. 블록 ACK 기법은 하나 이상의 QoS 데이터 프레임을 SIFS 간격으로 전송하고, 이를 수신한 수신 QSTA은 하나의 블록 Ack 프레임을 전송하는 방식으로 채널을 보다 효율적으로 사용할 수 있다. 또한 동일한 BSS 내의 STA으로 데이터를 전송하는 경우에도 항상 AP를 경유해야 하는 기존의 전송방식은 전송지연에 민감한 다양한 트래픽을 효과적으로 지원할 수 없다. 따라서 802.11e는 QSTA와 QSTA 사이에 직접 데이터를 송수신할 수 있는 Direct Link Protocol(DLP)을 정의하고 있다.

### 3. 차세대 인증 및 보안 기술

IEEE P802.11 TGi는 IEEE 802.11에서 정의하는 WEP 보안 알고리즘의 문제점을 파악하여 개선된 인증 및 무선 LAN의 보안을 강화하기 위한 방안으로는 RSNA 보안 구조를 정의한다. RSNA는 무선 단말이 AP에 접속하는 과정에서 협상을 통해 보안 세션관리 및 4단계 키교환을 수행하고, 이를 통해 생성된 키를 계층적으로 관리함으로써 MAC에서 보다 강화된 보안을 제공할 수 있으며 다음과 같은 보안 특성을 갖는다.



(그림 4) CAP/CFP/CP Period

- AP와 STA를 위한 강화된 인증 메커니즘
- 키 관리 알고리즘
- 암호학적 키 생성
- CCMP와 TKIP(선택적)이라 불리는 강화된 데이터 프라이버시 메커니즘

#### 가. RSNA 인증 시스템

RSNA 인증 시스템은 IEEE 802.1X를 기반으로 하고, 무선 LAN MAC 프로토콜을 지원하며 supplicant 역할을 수행하는 무선 단말과, authenticator 역할을 담당하며 MAC 프로토콜과 상호 동작할 수 있는 인터페이스를 지원하는 AP, 그리고 IEEE 802.11i에서 정의하는 키 교환 프로토콜을 따르는 인증 서버를 구성요소로 갖는다.

EAP 인증은 AP가 EAP-Request를 보내거나 STA이 EAPOL-START 메시지를 송신할 때 시작되며, EAP 인증 프레임을 통해 AP는 IEEE 802.1X의 uncontrolled port를 사용하여 STA과 AS 사이의 RSNA 인증 연결을 생성하기 위한 인터페이스 기능을 수행한다.

PMK를 공유한 authenticator AP와 supplicant STA은 각기 유지하고 있는 PMK를 기반으로 IEEE 802.11i에서 정의하는 4단계 키 교환 프로토콜(4-way handshake)을 수행한다. 4-way handshake는 먼저 상대방의 PMK의 존재를 확인한 후, 일치하면 PMK로부터 PTK(Pairwise Transient Key)를 생성하고, 다시 생성된 PTK를 계층적으로 관리하여 MAC 프로토콜로 전달하는 과정을 수행한다. PTK가 성공적으로 전달된 후, AP는 IEEE 802.1X의 controlled port를 허가함으로써 일반적인 데이터 프레임이 IEEE 802.11 서비스를 제공 받을 수 있도록 조정한다.

#### 나. 보안 알고리즘

RSNA는 단기적인 보안 기법으로 기존의 AP와 무선 단말기에 소프트웨어적으로 패치하는 방식으로 보안기능을 강화할 수 있는 TKIP(Temporary Key Integrity Protocol)과 중장기적인 기법으로

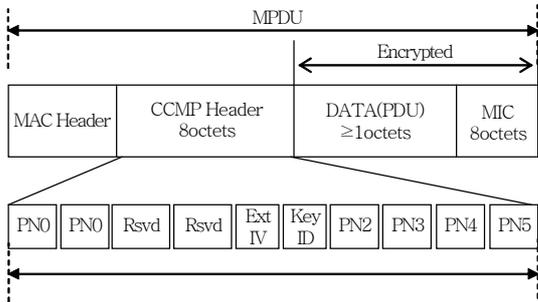
AES 엔진 기반의 CCMP(Counter-mode/CBC-MAC Protocol)를 정의하고 있다. CCMP는 모뎀 칩셋이 바뀌어야 하므로 기존 제품과의 호환성에 문제가 있지만 고속으로 견고한 무선 데이터의 암호화 및 복호화를 제공할 수 있으므로 반드시 지원되어야 하는 RSNA의 주요한 암호화 기법이다.

TKIP은 WEP이 갖는 취약점을 보완하기 위하여 MSDU를 교환하는 전송자와 수신자의 주소, priority, MSDU의 데이터 값을 사용하여 무결성을 검증하기 위한 MIC(Message Integrity Code)을 계산하고 MSDU 데이터에 추가한다. 또한 TKIP의 MIC이 공격 받을 수 있다는 단점을 보완하기 위하여 공격의 횟수를 제한하는 counter-measure를 수행한다.

TKIP은 pre-RSNA 하드웨어에서 WEP 프로토콜을 강화한 암호 모음으로 초기화 벡터(Initialization Vector: IV)와 extended IV로부터 MPDU의 수열번호인 TSC(Transient Sequence Counter)를 설정하여 임시 키(Temporal Key: TK)와 함께 WEP seed를 생성하고, IEEE 802.11에서 정의한 WEP의 RC4를 사용하여 암호화 및 복호화 과정을 수행한다.

이에 반해 RSNA에서 정의하는 CCMP는 기밀성을 위하여 사용되는 counter(CTR) 모드와 인증 및 무결성을 위한 CBC-MAC(Cipher Block Chaining Message Authentication Code)를 결합한 프로토콜로서 AES(Advanced Encryption Algorithm) 엔진을 기반으로 기밀성, 무결성 및 재생 방식을 위한 보안 서비스를 제공한다. (그림 5)는 CCMP를 사용하여 암호화된 MPDU로 매 MPDU 마다 새로운 값을 갖는 PN(Packet Number)와 키 ID가 CCMP header에 포함된다. CCMP의 PN은 TKIP MPDU에서 사용하는 TSC와 동일한 기능을 위해 정의되었다.

CCMP에서 사용하는 AES 기반의 CCM 모드는 일반적으로 데이터 인증 및 암호화 기능을 모두 지원하는 블록 암호화 방식이며 CCMP가 기반으로 하고 있는 AES는 128bit의 키를 사용하여 128bit 단위로 블록 암호를 수행할 수 있다. AES의 블록 암호



(그림 5) Expanded CCMP MPDU

모드는 기존의 암호화 방식인 RC4의 스트림 암호(stream chipper) 모드에 비하여 고속으로 동작할 수 있으며 또한 매 세션마다 새로운 임시 키(temporal key)를 필요로 하기 때문에 보다 강화된 암호화 특성을 제공한다.

#### 4. 차세대 무선 전송 기술

현재 IEEE 802.11의 표준화 회의에서 11n을 위한 전송방식에 대한 제안을 공식적으로 받고 있는 단계는 아니지만, 지금까지 WNG SC나 HTSG 회의동안에 발표되었던 기고서를 중심으로 살펴보면 802.11n에 제안될 수 있는 기술들은 예상할 수 있다. 본 논문에서는 지금까지 발표되었던 기고서를 중심으로 차세대 무선 LAN의 물리계층 전송방식을 정리하고자 한다.

우선 거의 대부분의 무선 LAN 개발 업체들이 생각하고 있는 것은 다중 안테나를 이용하는 MIMO 기술이다. 이 방식으로서 크게 3가지가 고려되고 있다. 한 가지는 각 송신 안테나에서 각각 다른 데이터를 전송하여 전송률을 송신 안테나 수만큼 향상시키는 공간 분할 다중화(Spatial Division Multiplexing: SDM) 방식이고, 다른 하나는 시공간 부호(space-time code)의 다이버시티 이득을 이용하여 성능 이득을 얻는 것이다. 많은 경우, 시공간 부호 중에서는 구현 복잡도를 고려하여 시공간 블록 부호(Space-Time Block Code: STBC)만을 고려하고 있다. 위에서 언급한 다중안테나 방식 이외에 기존의 MAC의 다중 접속 방식을 변형하여 여러 STA(Station)을 동시에 접속할 수 있도록 하는 공간 분할 다중 접속

속(Space Division Multiple Access: SDMA) 방식도 고려되고 있다. 그러나 SDMA의 경우는 하나의 AP(Access Point)에 여러 STA를 지원하기 때문에 AP에서의 전체 네트워크 스루풋은 높일 수 있지만, 개개의 일 대 일 링크에서의 스루풋이 증가하는 것은 아니다. 다중안테나 이외에 고려되고 있는 기술들 중에는 기존의 20MHz 대역에서 대역폭을 2배 늘려서 전송률을 2배 향상하는 것과 그 외에도 적응 변조를 적용하는 방식 등이 포함되고 있다.

차세대 무선 LAN 802.11n에서 고려하고 있는 서비스의 모델이 다양하고 그 각각의 특성이 아주 달라 어떤 한 가지의 기술이 아닌 여러 가지 기술이 접목된 형태가 될 가능성이 아주 높다. 즉, 홈 네트워크의 경우 서비스의 커버리지는 25m 이내로 아주 작지만, DVD 및 HDTV 신호의 전송과 같이 고용량을 필요로 하는 서비스가 주가 될 것이다. 그래서 802.11n에서 말하는 최대 전송속도가 구현되어야 하는 환경이 바로 홈 네트워크가 될 것이다. 반면 또 하나의 큰 응용 분야가 될 핫스팟의 경우는 최대 전송률은 그렇게 높을 필요는 없지만, 서비스 커버리지를 수백 미터까지 확장해야 한다. 이 두 가지 예만 보더라도 두 응용분야의 요구사항이 상반되기 때문에 이를 모두 수용하기 위해서는 어느 한 기술이 아닌 여러 가지 기술이 결합된 형태이어야 한다.

##### 가. 공간 분할 다중화(SDM)

SDM은 우리가 흔히 MIMO 기술이라고 말하는데, 본 논문에서는 다중 안테나를 사용하는 모든 기술을 MIMO 기술이라고 분류하고 그 중 각 안테나에서 서로 다른 독립적인 데이터를 전송하여 전송률을 향상시키는 것을 SDM이라고 정의한다.

SDM 기술은 G.J. Foschini가 [9]에서 다중 안테나에서의 채널 용량의 증가를 입증하면서, 송수신단의 다중 안테나를 이용하여 주파수 효율을 높일 수 있다는 것을 보였다. 그리고 [10]에서는 SDM 기술의 초기 버전인 D-BLAST(Diagonal-Bell Labs Layered Space-Time)를 간단히 한 V-BLAST(Vertical-BLAST)가 제안되었다. 이런 과정에서

SDM 기술이 기존의 시간, 주파수 또는 코드가 아닌 공간을 이용하여 주파수 효율을 획기적으로 높일 수 있는 가능성을 보여 주었다.

SDM/OFDM 방식에서 각 송신 안테나의 송신 심볼을 검파하기 위해서 부반송파별로 검파를 수행하며, 검파 기법에는 ML(Maximum Likelihood) 검파, 선형 검파, V-BLAST 형태의 연속적인 간섭 제거를 이용한 검파 등이 있을 수 있다. 이들에 대해서는 [11]에서 자세히 설명하고 있는데, 이를 요약하면 다음과 같다. 우선 가장 좋은 성능을 보이는 방식은 ML 방식이다. 모든 가능한 송신 심볼 조합 중에서 우도 함수(likelihood function)를 최대로 하는 조합을 선택하는 방식이다. 그리고 가장 간단히 생각할 수 있는 것은 선형 검파인데, 이는 채널 행렬의 역함수를 이용하는 것으로 성능은 가장 떨어지지만 구현이 가장 간단하다. 선형 검파는 잡음 전력의 고려 여부에 따라 ZF(Zero Forcing)와 MMSE(Minimum Mean Square Error) 방식으로 나눌 수 있다. 그리고 마지막으로 V-BLAST 검파가 있는데, 여러 개의 송신 심볼 중에서 하나씩 검파하고, 그 영향을 제거한 후에 다시 검파하는 형태로 CDMA(Code Division Multiple Access)의 간섭 제거기와 비슷한 형태로 검파하는 것이다. 이런 V-BLAST 검파기의 경우 중간 과정에서 모든 결정이 정확하게 이루어지는 경우 데이터 전송률을  $N$  배 높일 수 있을 뿐만 아니라 평균적으로  $N \times M/2$ 의 다이버시티 차수가 얻어진다. 이와 같은 방식은 ML 검파기에 비해서는 간단하지만 선형 검파기에 비해서는 상당히 복잡하다.

#### 나. 시공간 블록 부호(STBC)

다중 안테나를 이용하는 방식 중에 다른 하나로 STBC를 들 수 있다. STBC에 대해서는 [12]와 [13]에서 언급하고 있기는 하지만, STBC 자체가 전송률을 향상시키는 기술은 아니기 때문에 SDM만큼 활발하지는 않다. 그러나 차세대 무선 LAN 802.11n에서 커버리지에 중점을 둔 핫스팟 서비스를 위해서는 STBC가 채택될 것으로 보인다. 그리

고 SDM을 이용한 스루풋 향상을 위해서 다중 안테나를 비롯한 아날로그 경로가 구현되어 있다면, 단순한 기저 대역 디지털 연산으로 다이버시티 이득을 얻을 수 있다. 가장 대표적인 예로 Alamouti 부호를 들 수 있다[14].

Alamouti 부호를 비롯한 STBC에 대해서는 [15]에 자세히 설명되어 있어서, 구체적인 설명은 생략한다. 그리고 [16]에서는 STBC를 SDM과 결합하는 데 있어서 최적의 결합 방식들이 HTSG에서 제안되었다. 송신 안테나 개수에 따라 주어진 전송률을 얻을 수 있는 방법은 여러 가지가 있을 수 있다.

#### 다. 공간 분할 다중 접속(SDMA)

다중 안테나를 이용하는 또 다른 방식으로 SDMA을 고려할 수 있다[17]. SDMA 기술은, AP에 여러 개의 안테나를 설치하여 얻은 공간상의 자유도를 이용하여 여러 개의 STA이 동시에 접속할 수 있도록 하는 것이다. 기존의 MAC의 개념을 완전히 바꿔야 한다는 데 문제가 있기는 하지만 AP의 스루풋을 높일 수 있는 좋은 방식이다.

다중 사용자를 구분하는 기술적인 면에서는 SDM과 유사하다. STA에서 여러 개의 안테나를 가지고 각각 다른 데이터를 보내서 전송률을 높이는 대신 한 개의 안테나를 갖고 있는 여러 개의 STA에서 전송되는 여러 데이터를 구분하는 것이다. 그래서 상향링크의 경우, 검파방식도 SDM의 경우와 같다.

SDMA는 AP의 MAC에서의 스루풋을 향상시킬 수 있을 뿐만 아니라, AP와 한 STA의 링크에서 봤을 때는 다이버시티 이득을 통한 성능 향상까지도 얻을 수 있다.

#### 라. 대역폭 확장

대역폭을 늘려서 전송률을 향상시킬 수 있는 가장 간단한 방식이다. 이 방식들에 대해서 뚜렷한 기고가 있는 것은 아니지만 일부 업체에서 터보 모드라고 하면서 현재 802.11a/g를 지원하는 칩셋에서 2배의 전송률을 지원하고 있다. 대역폭을 확장하는 것은 여러 가지 방식으로 생각할 수 있다. 우선, 기

존의 802.11a/g의 두 개의 채널을 합쳐서 사용하는 것을 고려할 수 있다. 그리고, 802.11a/g의 클럭을 두 배 향상하는 것도 생각할 수 있고, 처음부터 확장한 40MHz 대역폭을 가지고 OFDM 시스템의 파라미터를 다르게 설계할 수도 있다[12].

각각의 방식들의 장단점에 대하여 알아보자. 첫 번째, 802.11a/g의 두 채널을 동시에 사용할 경우에는 기존 무선 LAN과의 호환이 쉽고, 기저 대역은 바뀌지 않아도 된다는 장점이 있지만, 아날로그 경로가 두 개가 있어야 한다는 단점이 있다. 그리고 클럭을 2배로 올리는 경우 역시 기저대역 디지털 부분은 거의 바뀌지 않지만, 20MHz와의 호환을 위해서는 클럭을 바꾸는 기능이 추가되어야 한다. 그리고 아날로그 경로도 두 개가 있어야 하는 것은 아니지만, 어느 정도 수정이 있어야 한다. 그리고 심볼 구간이 짧아져서 보호구간 역시 줄어든다는 단점이 있지만, 이와 같은 방식을 홈 네트워크 환경에서만 사용한다면 그렇게 문제가 되지는 않는다. 그리고 OFDM의 부반송파 개수부터 다시 설계하는 경우도 있을 수 있으나, 이 경우는 호환성을 전혀 고려하지 않는 것이라서, 기저 대역 모델이 두 개가 있어야 한다.

이와 같이 채널 대역폭을 40MHz로 2배 늘려 사용할 경우, 5 criterion인 경제적 타당성(economical feasibility)에 있어서 구현단가가 높아지고, 넓은 시장 잠재성(broad market potential)에 있어서 20MHz 규정이 있는 유럽 등과 맞지 않아서 글로벌 표준이 불가능하다는 이유, 전체 채널 수가 현재의 반으로 줄어든다는 이유 등으로 인한 반대가 아주 많다[18]. 그러나 200Mbps 이상의 전송률을 달성하기 위해서 4×4 MIMO의 SDM을 사용하는 것이 경제적 타당성 측면에서는 더욱 타당성이 없다고 생각된다. 40MHz의 대역폭을 이용하면서 2배의 전송률 향상을 얻고, SDM을 통하여 전송률을 2배 높여서 전체적으로 200Mbps급의 전송률을 얻는 것이 현재 구현 기술을 고려할 때 적당하다고 생각된다.

#### IV. 결론

본 논문에서는 다양한 서비스 시장에 대한 기대

가 증가하고 있는 무선 LAN과 관련하여 IEEE 802.11에서의 진행중인 작업 그룹의 표준화 동향 및 차세대 무선 LAN의 표준화 동향을 살펴보고, IEEE 802.11의 MAC 프로토콜 및 IEEE 802.11 a/b/g의 물리계층 전송방식에 대하여 설명하였다. 그리고 현재 표준화가 진행중이며 IEEE 802.11 TGn에서 차세대 무선 LAN 시스템을 정의하기 위하여 기반으로 하고 있는 IEEE 802.11e MAC 프로토콜과 차세대 무선 LAN 전송방식에 대하여 살펴 보았다. 또한 기존의 무선 LAN 시스템에서 가장 취약한 보안 문제를 다루기 위해 차세대 무선 LAN 시스템의 데이터 인증 및 보안을 위해 802.11 TG에서 정의하고 있는 RSNA 보안 메커니즘을 다루었다.

차세대 무선 LAN 기술의 경우는 아직 정식으로 표준화를 시작하지 않았지만 Functional Requirement (FR)와 Comparison Criteria(CC)를 모두 만족하는 차세대 무선 LAN 표준의 제안서가 빠르면 2004년 7월부터 제출되어야 하고, 기존 시스템과는 다르게 MAC과 물리계층을 동시에 고려하기 때문에 MAC과 물리계층 사이의 구분이 없는 혹은 두 계층 사이의 상호 관계를 동시에 만족시킬 수 있는 방안이 고려되어야 한다. 따라서 이미 표준화가 이루어졌거나 또는 현재 표준화가 진행중인 무선 LAN 기술들을 모두 지원하고 동시에 MAC 스투트 향상을 고속 무선 데이터의 전송을 목표로 이들을 적절하게 지원할 수 있는 전송 특성이 차세대 무선 LAN 기술의 표준화 과정에서 논의되고 추가되는 것이 불가피하다고 할 수 있다.

#### 참고 문헌

- [1] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," IEEE Std 802.11, 1999.
- [2] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification: Higher-Speed Physical Layer Extension in the 2.4GHz Band," IEEE Std 802.11b, 1999.
- [3] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification: High-speed

- Physical Layer in the 5GHz Band," IEEE Std 802.11a, 1999.
- [4] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification: Further Higher Data Rate Physical Layer Extension in the 2.4GHz Band," IEEE Std 802.11g/D8.2, Apr. 2003.
- [5] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification: Medium Access Control(MAC) Quality of Service(QoS) Enhancements," IEEE Std 802.11e/D8.0, Feb. 2004.
- [6] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification: Medium Access Control(MAC) Security Enhancements," IEEE Std 802.11i/D7.0, Oct. 2003.
- [7] Jon Rosdahl, "Darft PAR," Doc. Number: IEEE 802.11-02/798r7.
- [8] Jon Rosdahl, "Draft 5 criterion," Doc. Number: IEEE 802.11-02/799r6.
- [9] G.J. Foschini, "Layered Space-time Architecture for Wireless Communication in a Fading Environment when Using Multi-Element Antennas," *Bell Labs Technical Journal*, Autumn 1996, pp.41-59.
- [10] P.W. Wolniansky, G.J. Foschini, G.D. Golden, and R.A. Valenzuela, "V-BLAST: An Architecture for Realizing very High Data Rates over the Rich-Scattering Wireless Channel," *Proc. IEEE ISSSE'98*, Pisa, Italy, Sep. 1998, pp.295-299.
- [11] Heejung Yu, "HDR 802.11a Solution Using MIMO-OFDM," Doc. Number: IEEE 802.11-02/294r1.
- [12] Gerhard Fettweis and Gunnar Nitsche, "1/4 Giga-bits/s WLAN," Doc. Number: IEEE 802.11-02/320r0.
- [13] Minisha Ghosh, Xuemei Ouyang, and Guido Dolmans, "On the Use of Multiple Antennae for 802.11," Doc. Number: IEEE 802.11-02/180r0.
- [14] S.M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE Journal on Selected Areas in Commun.*, Vol. 16, No. 8, Oct. 1998, pp.1451-1458.
- [15] 안재영, 유희정, "차세대 무선 LAN 전송 기술," *Telecommunications Review*, 제 12권 6호, 2002. 12., pp.810-825.
- [16] Taehyun Jeon, Heejung Yu, and Sok-kyu Lee, "Optimal Combining STBC and Spatial Multiplexing for MIMO-OFDM," Doc. Number: IEEE 802.11-03/513r0.
- [17] Minnie Ho, Qinghua Li, Sumeet Sandhu, Cliff Prettie, and David Cheung, "Multiple Antennas: Performance Gains with Channel Measurements," IEEE 802.11-03/379r1.
- [18] John Terry, "Why 20MHz Channelization in HTSG?," IEEE 802.11-03/213r1.