WiBro(Wireless Broadband Internet) 기술동향

정 길 현

◈ 목 차 ◈

1. 서 론

언제, 어디에 있든 인터넷에 접속이 가능한 휴대 인터넷인 와이브로 (WiBro)는 Wireless Broadband Internet을 줄여 쓴 것으로 기존의 초고속 인터넷 서비스 품질의 통신 환경을 모바일 환경에서 제공한다. 12월 말 한국정보통신기술협회에서 확정한 2단계 개정 표준안에 의하면 최고 100Km로 움직이는 차량에서 수십 Mbps 속도의 다운로드가 가능한 것으로 알려져 있다. 또한 지난 12월 초에 최종적으로 발표된 IEEE 802.16 표준안과 호환되는 국제적인 표준안으로 자리 매김을 하게 됨에 따라 국제 시장을 이끌어 나가는 계기를 마련하게 되었다.

정보통신부는 새로운 성장 동력 사업으로 IT839 전략을 도입하여 정보 통신 분야에서의 새로운 발전을 꾀하고 있으며 8대 서비스 중의 하나인 와이브로의 산업 파급 효과는 2006년부터 2012년까지 휴대인터넷 서비스 및 단말기 생산유발효과는 총 33.9조원, 휴대인터넷 서비스의 생산 활동으로 인해 2006년부터 2012년까지 유발되는 부가가치는 약 15조원에 이를 것으로 전망되고 있다[1].

현재 와이브로 사업자로는 KT, SKT가 선정되어 있으며 와이브로 서비스에 필요한 주파수를 할당받은 상태이다. KT는 이미 지난 APEC 정상회담이 열린 부산에서 와이브로를 성공적으로 시연해 보였다. SKT는 High Level QoS에 기반한 음성, 화상 전화를 주력 서비스로 하며 이동 전화 형태의 단말기로 대상을 한정하는 HSDPA (High Speed Downlink Packet Access)를 주력으로, 와이브로를 지원적인 성격으로 규정하고 있다[2].

본 논문의 구성은 다음과 같다. 2장에서 와이브로의 국제 표준안인 IEEE 802.16 MAC 계층에 대해서 간단히 살펴보며 3장에서는 와이브로의 기술적인 특징에 관하여 알아본다. 4장에서는 와이브로의 응용 애플리케이션에 어떤 것들이 있는지 살펴보며 5장에서 결론을 맺는다.

2. IEEE 802.16 MAC 계층

IEEE 802.16 MAC 계층은 물리 계층 매체(medium)에 독립적인 인터페이스를 제공한다. 802.16 물리 계층은 무선 기반이므로 MAC 계층의 주된 목표는 효율적인 자원 관리이다. 단편화, 패킹(packing) 등이 자원 관리의 예라고 말할 수 있다. 한편 802.16 MAC 계층은 연결 기반 프로토콜로 이는 특정 네트워크에 진입하는 경우 각 SS (Subscriber Station)는 BS (Base Station)와 데이터 전송 용도의 연결을 하나 또는 그 이상 생성해야 함을 의미한다. 802.16 MAC 계층은 SS의 네트워크 참여(entry), 탈퇴 등의 작업과 표준 PDU (Protocol Data Unit)의 생성을 담당한다.

* 장안대학 컴퓨터정보계열 교수

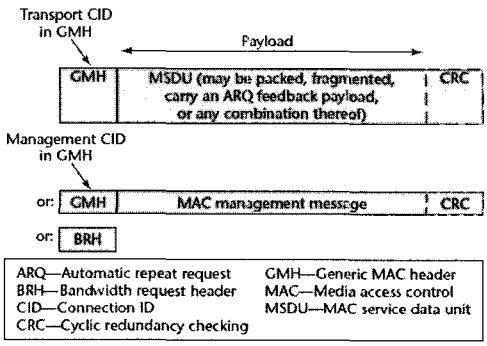
802.16 MAC 헤더에는 두 종류가 있는데 일반(generic) 헤더와 대역폭 요청(Bandwidth Request, BR) 헤더가 있다. 일반 헤더는 데이터 전송 또는 MAC 메시지 전송에 사용되며 BR 헤더는 SS가 업링크(UL)용으로 추가 대역폭을 요청할 때 사용한다. 점대다점 연결(Point to Multi Point, PMP)의 경우 SS와 BS간의 대역폭 할당 상태 통신 용도로 사용하는 {ARQ, Fast-feedback, Grant Management 서브 헤더}, 효율적인 대역폭 사용을 위한 {단편화(fragmentation), 패킹}을 MAC 계층에서 사용한다. 802.16 MAC 관리 메시지에는 셀 동기화, 자원 할당, 등록(registration), 인증(authorization), 연결 관리, ARQ, AAS (Adaptive Antenna System) 서비스, Burst 프로파일 변경, 채널 측정, 핸드오버와 관련된 것들이 있다[3].

성공적인 통신을 수행하기 위해 SS는 특정 네트워크에 참여해야 하는데 이는 802.16 MAC 계층이 담당한다. 네트워크 참여 과정은 크게 다운 링크(DL) 채널 동기화, Initial Ranging, Capabilities Negotiation, 인증 메시지 교환, 등록 및 IP 주소 부여 등의 단계를 거치게 된다.

① DL 채널 동기화 : BS로부터 전파되는 DL 신호를 검출한 다음 물리 계층에서 동기화 시킨다. 이 작업이 성공하면 DCD (Downlink Channel Descriptor) 및 UCD (Uplink Channel Descriptor)를 사용하여 변조, DL 및 UL의 전송 파라미터 정보를 획득한다.

② Initial Ranging : Ranging 작업은 BS에 SS의 파워 및 타이밍을 동기화하는 제어 작업의 기본이 되는 것으로 채널 환경이나 BS와 SS 사이의 거리가 변하는 경우 수행된다. Initial Ranging은 MAC 메시지가 전송되면서 시작되는데 BS로부터 응답 메시지를 받을 때까지 계속된다. 응답 메시지에는 파워 또는 타이밍 정보에 대해 SS가 수정해야 하는 작업이 포함된다. 이 단계가 끝나면 SS는 UL을 사용할 수 있게 된다.

③ Capabilities Negotiation : SS는 BS에 어떤 변조 레벨이 지원 되는지, 듀플렉싱 방법, 코딩 및 속도 등에 대해 질의한다. BS는 자신의 사양에 따라 SS를 거부하거나 수락하게 된다.



(그림 1) MPDU 구조

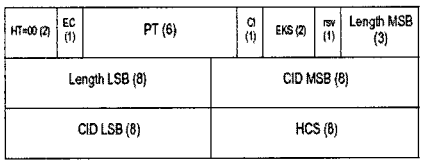
④ 인증 메시지 교환 : '3.3보안'을 참조한다.

⑤ 등록 : 인증 단계가 성공적으로 완료되면 SS는 BS에게 등록 요청 메시지를 전송하고 BS는 설정 정보와 함께 응답 메시지를 전송한다.

⑥ IP 주소 부여 : SS는 DHCP (Dynamic Host Configuration Protocol) 기반 서비스를 사용하여 BS로부터 IP를 설정 정보와 함께 부여받는다.

802.16 MAC 계층은 앞에서 밝힌 바와 같이 표준 PDU 생성 작업을 담당한다. MAC PDU (MPDU)의 세부 정보는 일반 MAC 헤더(GMH)에 저장되는데 연결 식별자(Connection ID; CID), 프레임의 길이, CRC 값의 존재 여부를 알리는 비트, 페이로드(Payload)가 암호화되었는지 등의 내용이 포함된다. 페이로드에는 관리 메시지 또는 전송 데이터가 포함된다. 페이로드에는 MSDU (MAC Service Data Unit)가 포함되는데 하나의 온전한 MSDU, 단편 MSDU 또는 여러 MSDU 단편의 집합, MSDU 집합 등 여러 종류가 될 수 있다. 그림 1에 MPDU의 구조가 나와 있다. CRC는 CCITT 표준 32비트 CRC이다.

일반 MPDU에는 전송 또는 관리 목적의 정보가 실리게 되는데 헤더에 있는 CID가 어떤 연결을 나타내는지에 따라 달라진다. 일반 MPDU는 GMH가 앞에 붙게 되는데 그림 2에서 HT는 0으로 설정되어 헤더가 GMH라는 것을 나타낸다. EC 비트는 암호화 여부를 알려주며 CI (CRC Indicator)는 MPDU의 끝 부분에 CRC가 있는지를 나타낸다. EKS



(그림 2) GMH 구조

(Encryption Key Sequence)는 해당 프레임의 암호화에 어떤 키를 사용했는지 나타낸다. LEN 필드의 11비트는 헤더와 CRC를 포함한 MPDU의 바이트 크기이며 이로 인해 프레임의 크기는 2047 바이트로 제한된다. CID는 해당 MPDU가 어떤 연결에 대한 것인지를 나타내며 HCS (Header Check Sequence)는 GMH 첫 5바이트에 대한 8바이트 CRC 값이다. 그림에서 Type 필드(PT로 표시)는 페이로드에 어떤 내용이 있는지를 알려주며 비트 위치에 따라 다음과 같은 의미를 나타낸다. 아래 목록에서 인가 관리 서브 헤더란 MAC 헤더나 CRC 계산과 같은 작업을 하지 않고 UL 대역폭 요청을 수행하는 경량의 (light-weight) 방법이다.

- 비트 0 : 페이로드에 인가(grant) 관리 서브 헤더가 있음
- 비트 1 : 패킹 서브 헤더가 있음
- 비트 2 : 단편 서브 헤더가 있음
- 비트 3 : 단편 또는 패킹 헤더가 확장된 경우
- 비트 4 : 프레임에 ARQ 피드백 페이로드가 있음
- 비트 5 : 메쉬(mesh) 서브 헤더가 있음

MSDU는 독립적으로 전송이 가능한 여러 개의 단편으로 나누어질 수 있는데 이를 표시하기 위해 페이로드의 앞부분에 FSH (Fragment Sub Header)를 붙인다. 2비트의 FC (Fragment Control) 비트는 해당 단편이 MSDU의 어느 부분인지를 나타내며 첫 번째인 경우 값은 10이 되며, 가장 마지막 단편인 경우 01, 그 외의 경우에는 11이 된다. FC 2비트가 00이면 단편이 되지 않았음을 의미한다. FSN (Frame Sequence Number)는 MSDU의 각 단편마다 1씩 증가하며 수신 측에서 단편을 재조립하는데 사용한다.

ARQ (Automatic Retrnasmission reQuest)는 에러로 인한 전송 실패의 경우 접속 양단의 한쪽에서 MSDU의 일부를 재전송하는 경우에 사용된다. MSDU는 마지막 블록을 제외하고는 같은 크기의 블록으로 이루어져 있으며 블록 크기는 시스템 파리미터로 관리된다.

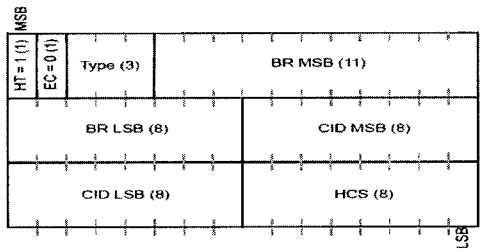
다수의 MSDU나 다수의 MSDU 단편을 모아 하나의 MSDU로 만들 수 있는데 이를 MAC 단계 패킷 수집(Packet Aggregation)이라고 한다. 이로 인해 패킷의 헤더를 줄임으로써 전송량을 줄일 수 있으며 GMH의 비트를 설정하여 패킹 서브 헤더가 있음을 나태낸다. 하나의 MPDU에는 여러 개의 패킹 헤더가 있을 수 있는데 MSDU나 MSDU 단편이 뒤이어 위치한다.

그림 3에서 BRH (Band Request Header)란 인가 받은 연결의 속성을 바꾸고자 하는 경우 GMH 대신 전송하는 6바이트의 대역폭 요청 헤더이다. 이 경우 HT (Header Type)의 값이 1로 설정 되어 GMH가 아닌 BRH라는 것을 나타내며 반드시 HT는 1로, EC (Encryption Control) 비트는 0으로 설정해야 한다. 대역폭 요청은 항상 CID 기반으로 이루어지며 대역폭 할당은 SS를 기반으로 이루어진다. 그림 3의 BR 필드는 요청하는 대역폭의 UL 바이트 수를 나타내며 HCS 필드는 BRH의 첫 5바이트에 대한 8비트 CRC 값이다[6].

3. 와이브로의 기술적인 요소

3.1 OFDMA (Orthogonal Frequency Division Multiple Access)

다중 액세스(Multiple Access)란 하나의 주파수를



(그림 3) 대역폭 요청 헤더

여러 사용자가 사용할 수 있도록 해주는 기술로서 FDMA(Frequency Division Multiple Access), TDMA (Time Division Multiple Access), CDMA(Code Division Multiple Access) 등이 있다. FDMA는 주파수에 의해 사용자가 구분되며 TDMA는 각 사용자가 주어진 시간 동안 신호를 전송하는 방식이다. CDMA는 사용자가 부호를 사용하여 구분되어 결과적으로 데이터 신호의 대역폭보다 넓게 사용되므로 확산 스펙트럼 다중 접속 방식이라고 한다. CDMA 시스템의 문제점은 모바일 통신과 같은 다중 경로 지연 요소가 존재하는 경우 코드 시퀀스가 상호 직교하지 않게 되어 동일한 셀 내에 있는 사용자들 간에 간섭이 발생할 수 있다는 점이다[5,7].

OFDM은 휴대 인터넷 서비스 와이브로의 물리 계층 전송 방식으로 채택되었으며 IEEE 802.11a/g, IEEE 802.16a와 더불어 유럽의 디지털 오디오 방송, 디지털 지상 텔레비전 방송의 전송방식으로 채택된 상태이다.

OFDM은 해당 주파수 대역을 다시 여러 개의 하위 주파수 대역으로 나누어 데이터를 전송하는 방식을 기본으로 한다. 따라서 FDM (Frequency Division Multiplexing) 방식의 한 종류라고 볼 수 있다. OFDM의 가장 큰 특징은 하위 주파수들이 상호 직교한다는 사실이다. 각 주파수는 주파수 보호 대역(Frequency Guard Bands)에 의해 다른 주파수와의 간섭을 방지하게 된다. OFDM에서 각 주파수 스펙트럼은 다른 스펙트럼과 겹침이 가능한데 이는 직교성에 의한 것이다.

3.2 이동성 기술

휴대 인터넷 와이브로는 수 십 킬로의 속도로 움직이는 차량 내에서도 끊김이 없는 통신 서비스를 제공한다. 이를 위해 중요한 요소 기술이 바로 이동성 기술이다. 현재 이동 전화의 경우, 셀 단위의 기지국 관리 단위 사이를 이동할 때 핸드오프(Hand-off)가 발생하게 된다. 핸드오프를 통해 통화가 끊어지지 않고 계속 유지가 되는 것이다. 핸드오프에는 하드(Hard) 핸드오프, 소프트(Soft) 핸드오프, 소프터(Softer) 핸드오프 등이 있다. 와이브로 서비스는 IP 기반 서비스이므로 이동성 기술을 효과적으로 구현하기 위해서 모바일 IP가 필요하게 된다.

Mobile IP는 인터넷에서 이동성을 지원하기 위해 만든 프로토콜로서 이동하는 노드의 홈 네트워크에 홈 에이전트(Home Agent)를 두고 외부 네트워크에서 사용하는 주소인 Care-of Address를 이 홈 에이전트에 등록한다. 이동 노드로 어떤 패킷이 전송되면 홈 네트워크의 홈 에이전트는 미리 등록되어 있는 Care-of Address로 패킷을 전달하는 방식으로 동작한다. 홈 에이전트는 Foreign Agent와 더불어 이동 에이전트로 분류된다. 홈 에이전트가 이동 노드의 현재 위치 정보를 Care- of Address형태로 유지/관리하는데 터널링(tunneling) 기법을 사용하여 이동 노드로 패킷을 전달하게 된다.

IEEE 802.16e는 DHCP를 사용하여 모바일 SS에 IP 주소를 할당하며 BS와 연결성을 유지하게 된다. 하지만 DHCP 서버로부터 IP 주소를 받은 SS가 BS간의 핸드오프를 발생시키면 DHCP의 속성 상 현재 연결이 끊어지게 된다. 이러한 문제점을 해결하기 위해서 모바일 IP에 의한 동적 주소 할당이 사용된다. 이를 위해 IEEE 802.16 프로토콜 스택에 이동 에이전트 계층이 사용되며 핸드오프의 물리적인 처리를 위한 과정 또한 MAC 계층에 구현이 되어 있다.

3.3 보안

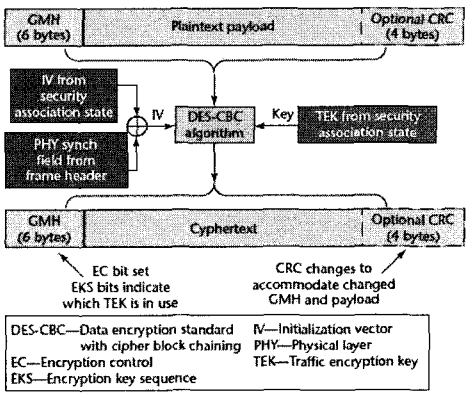
휴대 인터넷 와이브로에서 보안 기능은 MAC 계층의 프라이버시 부 계층(Privacy Sub-layer)에서 제공되며 크게 다음 다섯 가지 구성 요소로 나누어 생각해 볼 수 있다[4].

3.3.1 SA (Security Associations)

SA는 통신 연결과 관련된 보안 상태를 관리한다. IEEE 802.16에는 두 가지 SA 타입이 있지만 명시적으로 데이터 SA만 정의하여 사용한다. 데이터 SA는 다음과 같은 필드로 구성되며 BS와 하나 이상의 SS 사이의 전송 연결을 보호하게 된다.

· 16비트 SA 식별자

· CBC (Cipher Block Chaining) 모드 DES와



(그림 4) IEEE 802.16 암호화 과정

같은 암호기(Cipher)

- 2개의 TEK (Traffic Encryption Key); 현재 키와 현재 키가 만기가 될 경우 사용하는 키로 구성
- 2비트의 TEK 식별자 2개
- TEK 수명(최소 30분에서 최장 7일)
- 각 TEK의 64비트 초기화 벡터
- 데이터 타입을 나타내는 태그; Primary SA는 연결 초기화에 사용, Static SA는 BS에 설정, Dynamic SA는 동적 전송 연결용으로 사용

3.3.2 암호화(Encryption)

Payload 필드에 적용되는 것으로 MPDU를 암호화 대상으로 한다. MPDU GMH에는 TEK이 사용되고 있음을 나태내기 위해 2비트를 사용한다. 그림 4는 IEEE 802.16 암호화 과정을 나타내고 있다.

3.3.3 PKM (Privacy Key Management) 인증

PKM 인증 프로토콜은 인증 토큰을 공인된 SS로 분배하는 역할을 수행한다. 이 프로토콜은 3단계 메시지 교환으로 나누어지는데 SS와 BS간에 메시지가 교환된다. 이를 단계별로 살펴보면 다음과 같다.

① SS → BS Cert(Manufacturer(SS)) : 여기에서 Cert(Manufacturer(SS))는 SS의 제조자를 식별하는 X.509 인증서이다. 이를 받은 BS는 해당 SS가 신뢰할 수 있는 SS인지 결정하게 된다.

② SS → BS Cert(SS) | Capabilities | SAID : Cert(SS)은 SS의 공개키가 들어있는 X.509 인증서이다. 이는 BS가 해당 SS가 인증된 것인지의 여부를 알기 위해 사용하며 BS가 세 번째 메시지를 만드는데 사용한다. Capabilities는 SS가 지원하는 인증 및 데이터 암호화 알고리즘을 나타낸다. SAID는 SS와 BS 사이의 안전한 연결을 나타내는 일종의 식별자이다.

③ BS → SS RSA-Encrypt(PubKey(SS), AK) | LifeTime | SeqNo | SAIDList : 여기에서 RSA- Encrypt(k, a)는 키 k를 사용하여 a를 RSA-OAEP (Optimal Asymmetric Encryption Padding)으로 암호화하라는 의미이다. AK는 인증키를 의미하며 이 인증키는 32비트 부호 없는 숫자로서 AK의 수명을 초로 나타낸다. SeqNo는 4비트 AK 값이며 SAIDList는 SA에 대한 정보 리스트로서 SAID, SA 타입(Primary, Static, Dynamic), SA 암호기 등의 정보가 포함되어 있다. 세 번째 단계가 수행되면 SS와 BS 사이의 인증 SA가 구체화된다.

3.3.4 프라이버시, 키 관리

PKM 프로토콜이 일단 구체화되면 BS와 SS 사이에 데이터 SA를 만들게 되는데 2 또는 3 단계를 거쳐 이루어진다. 첫 번째 단계는 옵션으로서 새로운 SA를 생성하거나 데이터 SA를 rekeying 하는 경우에만 사용된다.

① BS → SS SeqNo | SAID | HMAC(1) : HMAC(1)은 AK의 다운링크 HMAC 키 하에서의 SeqNo | SAID의 HMAC-SHA1 다이제스트 값이다.

② SS → BS SeqNo | SAID | HMAC(2) : HMAC(2)은 AK의 업링크 HMAC 키 하에서의 SeqNo | SAID의 HMAC-SHA1 다이제스트 값이다.

③ BS → SS SeqNo | SAID | OldTEK | New-

TEK | HMAC(3) : 두 번째 단계에서 넘겨 받은 HMAC(2)이 유효하며 SAID에 SS의 SA를 식별할 수 있는 경우 BS는 세 번째 메시지를 사용하여 SA를 설정한다. OldTEK은 이전 생성 TEK의 초기화 벡터, 초 단위의 남은 수명, 데이터 SA의 일련 번호가 해당된다.

3.3.5 X.509 인증서 프로파일

인증서의 종류에는 제조자 인증서 및 SS인증서가 있다. 제조자 인증서는 IEEE 802.16 장치의 생산자를 식별하는 인증서이며 SS 인증서에는 MAC 주소가 포함되게 된다. X.509 인증서는 통신 주체를 식별하는 용도로 사용되며 다음과 같은 필드로 구성되어 있다.

- X.509 인증서 형식 버전 3
- 인증서 일련 번호
- 인증서 발급처의 서명 알고리즘(SHA1 해싱의 RSA 암호화 기법)
- 인증서 발급 주체
- 인증서 유효 기간
- 인증서 주체 (예를 들어 SS의 MAC 주소)
- 인증서 주체의 공개키
- 서명 알고리즘
- 발급 주체의 서명

4. 응용 애플리케이션

국제적인 표준 및 핵심 기술이 아무리 발전해도 응용 애플리케이션이 다양하게 제공되지 않는다면 와이브로는 성공적으로 성장할 수 없을 것이다. 와이브로 애플리케이션은 와이브로 네트워크만을 사용하는 것과 CDMA, WLAN 등의 다른 종류의 망과 연동하여 사용하는 경우가 있다. 와이브로의 성공 여부는 단말기 사업, 애플리케이션 개발, 모바일 컨텐츠 개발이라는 세 가지 축으로 진행이 될 것이다. 대표적인 와이브로 애플리케이션을 나열하고 그 특징에 대해서 알아보기로 한다.

4.1 DMB (Digital Multimedia Broadcasting)

H.264라고 하는 MPEG-4 AVC 인코딩 기법을 통해 대용량의 동영상 데이터의 고속 전송이 가능해짐에 따라 노트북, PDA, 휴대폰 등과 같은 모바일 환경에서 위성 DMB, 지상파 DMB 등의 서비스가 이미 시작되었다. 와이브로 단말기를 사용하는 사용자 또한 영상, 데이터 방송 등의 형태로 DMB 서비스를 제공받을 수 있다. 또한 고화질의 화상 통화 또는 화상 회의가 가능하게 된다.

4.2 모바일 Collaboration

모바일 Collaboration은 음성은 CDMA, 데이터 통신은 와이브로 망을 구분하여 사용한다. 주로 협력 작업이나 교육, 공유 작업과 같은 환경에 사용된다. 모바일 Collaboration 작업은 SIP (Session Initiation Protocol)을 사용하여 세션의 생성, 수정, 종료 등의 작업을 수행한다. SIP은 애플리케이션 계층에 해당되며 Internet Telephony, 화상 회의 등의 용도로 사용된다. 모바일 Collaboration에서 사용자들은 화이트 보드(White Board)를 사용하여 공동 작업 또는 데이터 공유를 실현하다.

4.3 텔레매틱스(Telematics)

차량에 단말기를 설치하여 운전자에게 위치 정보, 교통 정보, 재난 구조, 원격 진단 등의 서비스를 제공하기 위한 무선 인터넷 서비스가 해당된다. 텔레매틱스는 정부의 IT839 전략에도 포함될 만큼 기술 및 산업화에서의 전망을 밝게 하고 있다. 진행되고 있거나 앞으로 서비스가 예상되는 와이브로 기술 기반 대표적인 텔레매틱스 서비스는 다음과 같다[2].

- 센싱 기반 차량 관리 서비스
- 자동 운전지원 및 원격진단
- 지능형 교통안내 서비스
- 실시간 동적 경로 안내 서비스
- 멀티미디어 여행정보 서비스
- 차량 상태 센싱 기술

· 차량 간 통신 통합 기술
· 고 정밀 차량 측위 기술
· 교통/위치 데이터 마이닝 기술
· 이동 멀티미디어 스트리밍 기술
· 텔레매틱스 음성인식 기술

5. 결 론

본 논문에서는 와이브로와 관련된 표준, 와이브로의 기술적인 특징, 와이브로 관련 애플리케이션 등에 대해 알아보았다. 와이브로는 국내 기술로 만들어낸 결과물로서 미래 통신 시장을 선도하고 산업 구조를 재편할 가능성이 충분히 있는 분야이다. 이를 위해서 기술적인 발전 및 컨텐츠 사업 및 비즈니스 모델 개발이 이어져야 할 것이다.

참 고 문 헌

[1] 지경용, 와이브로 서비스 사용자 조사 및 파급효과 분석, 한국전파진흥협회, 2004.
[2] 김용석 외 5인, "훤히 보이는 WiBro," u-Book, 2005.
[3] Govindan Nair 외 5인, "IEEE 802.16 Medium Access Control and Service Provisioning," Intel Technology Journal, Vol. 8 Issue 03, 2004..
[4] David Johnston and Jesse Walker, "Overview of IEEE 802.16 Security," IEEE Security and Privacy, 2004.
[5] J. H. Stott, "The How and Why of COFDM," EBU Technical Review, Winter 1998.
[6] David Johnson and Hassan Yaghoobi, "Peering into the WiMAX Spec," http://www.commsdesign. com, 2005.
[7] W. Y. Zou andY. Wu, "COFDM: An Overview," IEEE Trans. Broadcasting, Vol. 41, No. 1, 1995.

◐ 저 자 소 개 ◑

정 길 현
1983년 한양대학교 전자통신공학과 졸업(공학사)
1986년 이화여자대학교 대학원 수학과(전자계산전공) 졸업(이학석사)
2001년 한양대학교 대학원 컴퓨터공학과 졸업(공학박사)
1990년~현재 장안대학 컴퓨터정보계열 교수
관심분야 : 프로토콜성능분석, 데이터통신, 통신망 etc.