An Emerging Technology in Broadband Wireless Access Technology for 3G Evolution Path towards 4G

Amit Kumar Chauhan*, Manish Kumar Chauhan*, Himadri Chauhan**
*Department of Computer Science
Phonics Group of Institutions, Roorkee, Haridwar, Uttarakhand, India
** Dept. of Information Technology
Graphic Era University, Dehradun, UK, India.
manishchauhan41@gmail.com.

Abstract— WiMax will be to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area. With WiMAX users could really cut free from today. Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a Metro Zone.

Keywords—WiMAX, OFDM, 802.16e, QoS, WiMAX MAC LAYER

1. INTRODUCTION

The most obvious technical development in wireless MANs and wireless WANs are embodied by the IEEE 802.16, and ETSI HIPERMAN standards. Based on the open IEEE 802.16 and HIPERMAN, a commercialized technology called WiMax has been derived. WiMAX is one of the most recent broadband wireless access technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. WiMAX would operate similar to WiFi but at higher speeds, over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure. WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the Wi-Fi Alliance is to 802.11. WiMAX is acronym for Worldwide Interoperability for Microwave Access and is based on Wireless MAN technology. It is a wireless technology optimized for the delivery of IP centric services over a wide area and a scaleable wireless platform for constructing alternative and complementary broadband networks. A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models:

- A fixed usage model (IEEE 802.16-2004).
- A portable usage model (IEEE 802.16e and IEEE 802.16m).

2. WHY WE NEED WIMAX

WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, Wi-Fi and cellular backhaul, providing last-100 meter access from fibre to the curb

and giving service providers another cost-effective option for supporting broadband services. WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value, multimedia services. It can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types. WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications. In an IP-based wireless broadband technology, WiMAX can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks, allowing it to become part of a seamless anytime, anywhere broadband access solution. Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

3. WiMAX NETWORK ARCHITECTURE

This describes the network architecture of the WiMAX system, which consists of the MS/SS, ASN, and CSN. MS or SS are used by the users to connect the VPN or Internet by using air interface. All the MS or SS connects to the BS(Base Station) and BS further connects to the ASN-Gty.

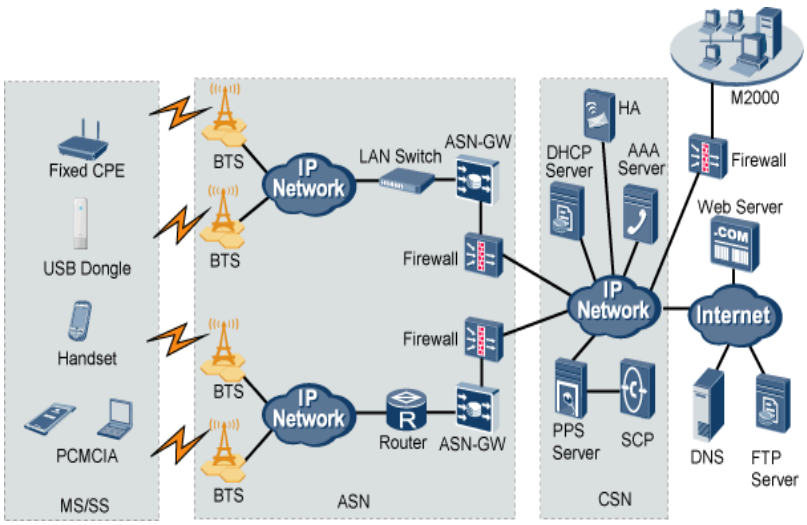

Figure 1. WiMAX Network Architecture

The following part describes the components of the WiMAX network.

3.1 MS / SS (Mobile Station/ Subscriber station)

The MS/SS is the subscriber device that communicates with the BS. A subscriber device may be a fixed terminal, mobile terminal, or USB terminal.

3.2 ASN (Access Service Network)

The ASN consists of the BS and the ASN-GW. The ASN can be connected to the CSNs of multiple NSPs. The ASN manages the IEEE 802.16e air interface to provide WiMAX subscribers with wireless access. The ASN performs the following functions:

- Establishing layer-2 connections between the BS and MS
- Sending AAA messages to the home NSP of the MS
- Assisting the upper level of the system to establish layer-connections with the MS and allocating IP addresses.
- Establishing and managing the tunnels between the ASN and the CSN.
- Implementing mobility management and handovers.
- Implementing paging and location management within the ASN.
- Implementing radio resource management (RRM).
- Storing the information of temporary subscribers.

The ASN has the following NEs:

3.2.1 BS: The BS receives and transmits radio signals and thus enables the communication between the WiMAX network and the MS.

3.2.2 ASN-GW: The ASN-GW is a logical NE that performs control functions. The ASN-GW communicates with its own NEs, such as the BS, and with the NEs within the CSN or other ASNs. The ASN-GW also performs data routing and bridging on the bearer plane.

3.3 CSN (Core or connectivity Service Network)

The CSN includes the router and AAA server. You can construct a new CSN or use the existing equipment for implementing CSN functions. The CSN provides WiMAX subscribers with IP connections and its functions are as follows:

- Assigning IP addresses and session parameters for the MS
- Providing Internet access
- Establishing layer-3 connections and forwarding messages, such as IP assignment messages, for the MS
- Sending RADIUS messages to the home NSP of the MS and performing authentication, authorization, and accounting for subscriber sessions
- Implementing the functions of the AAA server
- Implementing accounting and settlement
- Implementing QoS management and admission control based on the system parameters of the MS
- Implementing mobility management between ASNs
- Establishing and managing the tunnels between the ASN and the CSN
- Providing WiMAX services, such as location-based services and multicast services
- The CSN has the following NEs:
- The Authentication, authorization and accounting (AAA) server is a remote verification server for authentication, authorization, accounting, and data value-added services. The

AAA also provides robust agent functions and flexible operations and supports various databases.

3.3.1 PPS: The prepaid service (PPS) is the service that allows subscribers to pay for the service before using it. The PPS data service is measured by time or data flow. The service traces the status of the service usage, either by time or by data flow, and then deducts the charging fees from the current account of the subscriber in real time.

3.3.2 SCP: The service control point (SCP) is the core component of the intelligent network. The SCP stores the subscriber data and service logics. On receipt of query requests from the SSP, the SCP searches the database and decodes messages as required. Based on the call events reported by the SSP, the SCP sets up relevant service logics and sends call control commands to the corresponding SSP, thus enabling intelligent calls.

3.3.3 HA: The home agent (HA) maintains the current location information when the MS leaves the home link. The HA encapsulates the packets destined for the MS and then forwards the packets in tunnel mode. In addition, the HA assigns home IP addresses for mobile IP subscribers.

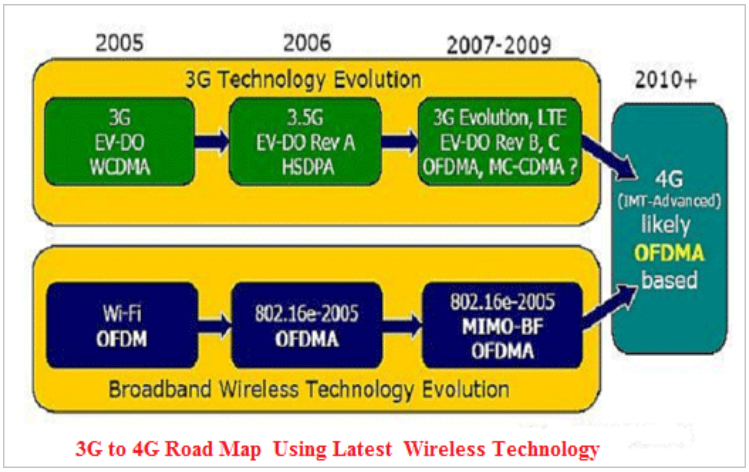

Figure 2. 3G to 4G Road Map

4. WiMAX PHYSICAL LAYER

The WiMAX physical layer is based on orthogonal frequency division multiplexing. OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems, including DSL, Wi-Fi, Digital Video Broadcast-Handheld (DVB-H), and MediaFLO, besides WiMAX. OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

4.1 Adaptive Modulation and Coding in WiMAX

WiMAX supports a variety of modulation and coding schemes and allows for the scheme to change on a burst-by-burst basis per link, depending on channel conditions. Using the channel quality feedback indicator, the mobile can provide the base station with feedback on the downlink channel quality. For the uplink, the base station can estimate the channel quality, based on the received signal quality.

Techniques/ Frequencies	Downlink	Uplink
Modulation	BPSK, QPSK, 16 QAM, 64 QAM; BPSK optional for OFDMA-PHY	BPSK, QPSK, 16 QAM; 64 QAM optional
Coding	**Mandatory:** convolutional codes at rate 1/2, 2/3, 3/4, 5/6 **Optional:** convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC, RS-Codes for OFDM-PHY	**Mandatory:** convolutional codes at rate 1/2, 2/3, 3/4, 5/6 **Optional:** convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC

Table 1. A list of the various modulation and coding schemes supported by WiMAX.

4.2 PHY-Layer Data Rates

Because the physical layer of WiMAX is quite flexible, data rate performance varies based on the operating parameters. Parameters that have a significant impact on the physical-layer data rate are channel bandwidth and the modulation and coding scheme used. Other parameters, such as number of sub channels, OFDM guard time, and oversampling rate, also have an impact.

5. WiMAX - OFDM Basics

OFDM belongs to a family of transmission schemes called multicarrier modulation, which is based on the idea of dividing a given high-bit-rate data stream into several parallel lower bit-rate streams and modulating each stream on separate carriers often called subcarriers, or tones. Multicarrier modulation schemes eliminate or minimize inter symbol interference (ISI) by making the symbol time large enough so that the channel-induced delays. Delay spread being a good measure of this in wireless channels. are an insignificant (typically, < 10 percent) fraction of the symbol duration. Therefore, in high-data-rate systems in which the symbol duration is small, being inversely proportional to the data rate, splitting the data stream into many parallel streams increases the symbol duration of each stream such that the delay spread is only a small fraction of the symbol duration. **OFDM** is a spectrally efficient version of multicarrier modulation, where the subcarriers are selected such that they are all orthogonal to one another over the symbol duration, thereby avoiding the need to have no

overlapping subcarrier channels to eliminate intercarrier interference. In order to completely eliminate ISI, guard intervals are used between OFDM symbols. By making the guard interval larger than the expected multipath delay spread, ISI can be completely eliminated. Adding a guard interval, however, implies power wastage and a decrease in bandwidth efficiency.

6. WiMAX - MAC Layer

The IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications. The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the physical layer. The MAC layer takes packets from the upper layer. These packets are called MAC service data units (MSDUs).and organizes them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse. The IEEE 802.16-2004 and IEEE 802.16e-2005 MAC design includes a convergence sub layer that can interface with a variety of higher-layer protocols, such as ATM TDM Voice, Ethernet, IP, and any unknown future protocol. The 802.16 MAC is designed for point-to-multipoint (PMP) applications and is based on collision sense multiple access with collision avoidance (CSMA/CA). The MAC incorporates several features suitable for a broad range of applications at different mobility rates, such as the following:

- Privacy key management (PKM) for MAC layer security. PKM version 2 incorporates support for extensible authentication protocol (EAP).
- Broadcast and multicast support.
- Manageability primitives.
- High-speed handover and mobility management primitives.
- Three power management levels, normal operation, sleep and idle.
- Header suppression, packing and fragmentation for efficient use of spectrum.
- Five service classes, unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), best effort (BE) and Extended real-time variable rate (ERT-VR) service.

These features combined with the inherent benefits of scalable OFDMA make 802.16 suitable for high-speed data and bursty or isochronous IP multimedia applications. Support for QoS is a fundamental part of the WiMAX MAC-layer design. WiMAX borrows some of the basic ideas behind its QoS design from the DOCSIS cable modem standard. Strong QoS control is achieved by using a connection-oriented MAC architecture, where all downlink and uplink connections are controlled by the serving BS. WiMAX also defines a concept of a service flow. A service flow is a unidirectional flow of packets with a particular set of QoS parameters and is identified by a *service flow identifier* (SFID).

7. WiMAX MOBILITY SUPPORT

WiMAX envisions four mobility-related usage development:

7.1 Nomadic: The user is allowed to take a fixed subscriber station and reconnect from a different point of attachment.

7.2 Portable: Nomadic access is provided to a portable device, such as a PC card, with expectation of a best-effort handover.

7.3 Simple Mobility: The subscriber may move at speeds up to 60 kmph with brief interruptions (less than 1 sec) during handoff.

7.4 Full Mobility: Up to 120 kmph mobility and seamless handoff (less than 50 ms latency and < 1% packet loss) is supported.

It is likely that WiMAX networks will initially be deployed for fixed and nomadic applications and then evolve to support portability to full mobility over time. The IEEE 802.16e-2005 standard defines a framework for supporting mobility management. In particular, the standard defines signaling mechanisms for tracking subscriber stations as they move from the coverage range of one base station to another when active or as they move from one paging group to another when idle. The standard also has protocols to enable a seamless handover of ongoing connections from one base station to another. The standard also has protocols to enable a seamless handover of ongoing connections from one base station to another. The WiMAX Forum has used the framework defined in IEEE 802.16e-2005 to further develop mobility management within an end-to-end network architecture framework. The architecture also supports IP-layer mobility using mobile IP.

8. WiMAX SECURITY FUNCTIONS

WiMAX systems were designed at the outset with robust security in mind. The standard includes state-of-the-art methods for ensuring user data privacy and preventing unauthorized access, with additional protocol optimization for mobility. Security is handled by a privacy sub layer within the WiMAX MAC. The key aspects of WiMAX security are as follow:

8.1 Support for Privacy

User data is encrypted using cryptographic schemes of proven robustness to provide privacy. Both AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard) are supported. The 128-bit or 256-bit key used for deriving the cipher is generated during the authentication phase and is periodically refreshed for additional protection.

8.2 Device / User Authentication

WiMAX provides a flexible means for authenticating subscriber stations and users to prevent unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards. WiMAX terminal devices come with built-in X.509 digital certificates that contain their public key and MAC address. WiMAX operators can use the certificates for device authentication and use a username/ password or smart card authentication on top of it for user authentication.

8.3 Flexible key- Management Protocol

The Privacy and Key Management Protocol Version 2 (PKMv2) is used for securely transferring keying material from the base station to the mobile station, periodically reauthorizing and refreshing the keys.

8.4 Protection of Control Messages

The integrity of over-the-air control messages is protected by using message digest schemes, such as AES-based CMAC or MD5-based HMAC.

8.5 Support for Fast Handover

To support fast handovers, WiMAX allows the MS to use preauthentication with a particular target BS to smooth the progress of accelerated reentry.

A three-way handshake scheme is supported to optimize the reauthentication mechanisms for supporting fast handovers, while simultaneously preventing any man-in-the-middle attacks.

9. CONCLUSION

This paper described the emerging to the latest 4G technology with the help of the WiMAX. We identify and analyze that there is more broadband access choices, especially in areas where there are gaps: worldwide urban centers where building access is difficult; in suburban areas where the subscriber is too far from the central office; and in rural and low population density areas where infrastructure is poor. Although based on a simple idea, the new method can provide mobile user privacy protection and enhance the security of mobile WiMAX. The latest upcoming IEEE for Project 802.16n for Higher Reliability Networks and Project 802.16p for Enhancements to Support Machine-to-Machine Applications discuss later.

10. REFERENCES

IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004, http://www.ieee802.org/16/, 2004.

M. Barbeau, "WiMax/802.16 threat analysis," ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, 2005, pp. 8–15.

IEEE Std 802.16e-2005, http://ieee802.org/16/published.html, 2005.

Jukka Ylitalo, Tony Jokikyyny, Tero Kauppinen, Antti J. Touminen, Jaako Laine. "Dynamic Network Interface Selection in Multihomed Mobile Hosts" IEEE 2002.

Whitfield Diffie and Martin E. Hellman: New Directions in Cryptography, Invented Paper.

Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, Andreas Deininger :Security Vulnerabilities and Solutions in Mobile WiMAX, KDDI R&D Laboratories, 2-1-15, Ohara, Fujiminoshi, Saitama 356-8502, Japan.

Sanida Omerovic, "WiMAX overview", Faculty of Electrical Engineering, University of Ljubljana, Slovania.

D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 40-48, May-June 2004.

E. Kaasenbrood, "WiMAX Security - A Formal and Informal Analysis," Master's thesis, Eindhoven University of Technology, Department of Mathematics and Computer Science, Groningen, Netherlands, August 2006.

S. Xu and C. T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions," In Proceedings of 3rd International Symposium on Wireless Communication Systems (ISWCS 2006), Valencia, Spain, September 2006.

White Paper "Mobile WiMax Security" by Airspan Networks Inc. 2007.

Jamshed Hasan "Security Issues of IEEE 802.16 (WiMax)",2006 Society of London, vol. 426, pp. 233-271, 1989.

Rajesh Srivastava, Deepak Kumar Mehto , Prevention of Security Threats in IEEE 802.16 Standards 108. International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-1, Issue-4, September 2011.

Kumar Deepak , Srivastava Rajesh , "An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile Wimax" International Journal of Soft Computing and Engineering, Volume-1, Issue-4, September 2011.