IOSR Journal of Electronics and Communication Engineering (IOSRJECE)
ISSN : 2278-2834 Volume 2, Issue 2 (July-Aug 2012), PP 22-29
www.iosrjournals.org

Wireless Communication and Security in Wimax

Fazil Sarfaraz, Tarranum Parveen
(Department of Electronics and Communication, LNCTS/RGPV, India)

Abstarct: *Wireless communication deals with data transmission over air as interfacing medium between the transmitting and receiving stations posing data security as biggest challenge. Although, technologies other than wireless introduced earlier pay significant service to users, the broadband wireless, with mobility is the first choice of people all over. In this, WiMAX 802.16e is one possibly technology supporting data security. It uses different authentication and authorization protocols between the client and agent. This paper describes strategy of WiMAX and security mechanisms used in it.*
Keywords: *WiMAX, DSN, AAA, WWAN, WBA*

I. Introduction

In this era of scientific and technical growth, effective communication is a major concerned issue. Therefore it is mandatory to discuss about the latest communication technology. Wireless technology has taken vast coverage over wired communication technology. Wireless means transmitting signals using radio waves as the medium instead of wires. Wireless technologies are used for tasks as simple as switching off the television or as complex as supplying the sales force with information from an automated enterprise application. Examples today include cordless keyboards and mice, PDAs, pagers and digital and cellular phones and many more.
Wireless technology provides numerous advantages which make it attractive for the users which include mobility, reachability, simplicity, maintainability, roaming services, new smart services such as SMS and MMS and many more.

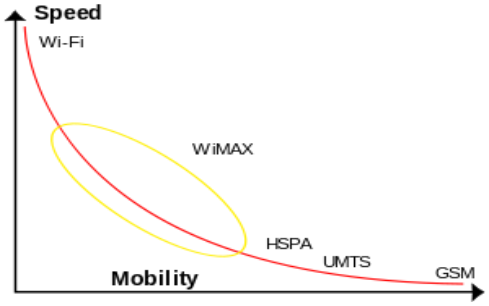
Wireless technologies are classified depending on their ranges and are designed to serve a specific usage segment that includesa variety of variables including bandwidth requirements, distance needs and power. The classifications include Wireless Wide Area Network (WWAN), Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), etc. all these networks are region specific and differ in terms of speed and range.

However, though comprising of proliferate inherent features and advantages, wireless networks suffer three major issues i.e. Quality of Service (QoS), Security risk and reachable range. QoS involve interference to service due to atmospheric imbalance and lost packets of data during transfer. Security risks involve security to data transfer over wide area. Security mechanisms like the Service Set Identifier (SSID) and Wireless Equivalency Privacy (WEP) may be adequate for residences and small businesses but they are inadequate for entities that require stronger security. Reachable range is not so a major issue as it is extended to tens of miles today.

Wireless Broadband Access (WBA) is a technology that ensures high speed connection over the air. It uses radio waves to transmit and receive data directly to and from the potential users. This technology includes 3G, Wi-Fi, WiMAX.WBA is a point to multipoint system in which the base station uses an outdoor antenna to send and receive high-speed data.

II. Competing Technologies

Within the marketplace, WiMAX's main competition came from widely deployed wireless systems such as Universal Mobile Telecommunications System (UMTS), CDMA2000, existing Wi-Fi and mesh networking. In the future, competition will be from the evolution of the major cellular standards to so-called 4G, high-bandwidth, low-latency, all-IP networks with voice services built on top. The worldwide move to 4G for GSM/UMTS and AMPS/TIA (including CDMA2000) is the 3GPP Long Term Evolution (LTE) effort.



Speed vs. mobility of wireless systems: Wi-Fi, High Speed Packet Access (HSPA), Universal Mobile Telecommunications System (UMTS), and GSM

III. Comparison between WiMAX and Wi-Fi

Refer to the following TABLE that gives a brief comparison between WiMAX and Wi-Fi

PARAMETERS	Wi-Fi WAVE (802.11p)	Wi-Fi (802.11)	WiMAX (802.16d)	WiMAX ODFMA (802.16e)
Frequency Band	5.9 GHz	5/2.4 GHz	2-11 GHz	2.3-3.5 GHz
Channel Bandwidth	10	20	10	5/10/20
Supported Data rate	3 to 7 Mbps	6 to 54 Mbps	54 Mbps	54 Mbps
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	BPSK, QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Channel Coding	CC 1/2, 2/3,3/4	CC 1/2, 2/3,3/4	CC 1/2, 2/3,3/4	CC 1/2, 2/3,3/4
No. of data subscribers	48	48	192	360/720/1440
No. of pilot Carriers	4	4	8	60/120/240
Guard subcarriers	12	12	56	92/184/368
FFT/IFFT	64	64	256	512/1024/2048
FFT/IFFT interval	6.4	3.2	22.22	91.43
Subcarrier spacing	15625 MHz	0.3125 MHz	0.045 MHz	0.0109 MHz
Preamble Duration	32 us	16 us	55.56 us	102.9 us
Cyclic prefix	1.6 us	0.8 us	[5.56](1/4-1/16)Tb us	11.43 us
OFDMA symbol duration	8 us	4 us	27.78 us	102.9 us
Layer	CSMA MAC	CSMA MAC	TDMA	OFDMA
Multipath	PHY tolerates only low multipath	PHY tolerates only low multipath	PHY tolerates only medium multipath	PHY can tolerate high multipath (10 us)

IV. WiMAX Theory

WiMAX (Worldwide Interoperability for Microwave Access) was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is a high throughput packet data transfer technology that supports both delay tolerant, burst-based services like web browsing, messaging and delay-intolerant services like audio/video calls. These services are provided to the end-user even while the user is mobile. WiMAX is a wireless communication standard designed to provide 30 to 40 mbps data rates. It is a part of a 'fourth generation' or 4G of wireless communication technology. More strictly WiMAX is an industry trade organization formed by leading communications component and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that confirms to the IEEE 802.16 and ETSI HIPERMAN standards.WiMAX is to 802.16 as the Wi-Fi is to 802.11.

V. Features of WiMAX Technology

The following potential applications are supported by WiMAX:

- Provides portable mobile broadband connectivity across cities and countries through a variety of devices.
- Provides a wireless alternative to cable and digital subscriber line (DSL) for large mile broadband access.
- Provides data, telecommunications (VoIP) and IPTV services (triple play).
- Provides a source of internet connectivity as part of a business continuity plan.
- Smart grids and metering.
- Can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down.
- Can provide wide area coverage and quality of service capabilities.

5.1 Internet Access

WiMAX can provide home or mobile internet access across whole cities or countries. Given the relatively low costs associated with the deployment of a WiMAX network, it is now economically viable to provide last-mile broadband Internet access in remote locations.

5.2 BAckhaul

Mobile WiMAX was a replacement entity for cellular phone technologies such as GSM and CDMA or can be used as an overlay to increase capacity. Fixed WiMAX is also considered as a wireless backhaul technology for 2G, 3G and 4G networks in both developed and developing nations.

5.3 Triple-A

Wimax supports the technologies that make triple-play service offerings possible (such as Quality of Service and Multicasting). As wireless progresses to higher bandwidth, it inevitably competes more directly with cable and DSL, inspiring competitors into collaboration. Also, as wireless broadband networks grow denser and usage habits shift, the need for increased backhaul and media service will accelerate, therefore the opportunity to leverage cable assets is expected to increase.

5.4 Deployment

- Wimax access was used t assist with communications in Indonesia, after the tsunami in December 2004. It provided broadband access that helped regenerate communication to and from Indonesia.
- WiMAX hardware was donated to FCC (Federal Communications Commission) an FEMA in their communications efforts in the areas affected by Hurricane Katrina. Volunteers used mainly self-healing mesh, Voice over Internet Protocol (VoIP), and a satellite uplink combined with Wi-Fi on the local link.

VI. The IEEE 802.16 Standard

WiMAX is based upon IEEE Std 802.16e-2005, approved in December 2005. It is a supplement to the IEEE std 802.16-2004. Thus, these specifications need to be considered.

IEEE 802.16e-2005 has following merits:

- Adding support for mobility (soft and hard handover between base stations)
- Scaling of the Fast Fourier Transform (FFT) to the channel bandwidth in order to keep the carrier spacing constant across different channel bandwidths
- Advanced antenna diversity schemes, and hybrid automatic repeat request (HARQ)
- Adaptive Antenna Systems (AAS) and MIMO technology
- Denser sub-channelization, thereby improving indoor penetration
- Introducing Turbo-Coding and Low Density Parity Check (LDPC)
- Introducing downlink sub-channelization, allowing administrators to trade coverage for capacity or vice-versa
- Adding an extra QoS class for VoIP applications.

VII. WiMAX Physical Layer

The updated IEEE 802.16e-2005 uses scalable orthogonal frequency division multiple access. OFDM (Orthogonal Frequency Division Multiplexing) is a method of encoding digital data on multiple carrier frequencies. OFDM has developed into a popular scheme for wideband digital communication, whether wireless or over copper wires, used in applications such as television and audio broadcasting. OFDM is an elegant and efficient scheme for high data rate transmission in o non-line-of-sight or multipath radio environment.

7.1 PHY-Layer Data Rates

Because of the flexible nature of physical layer of WiMAX, data rates performance varies based on the operating parameters. These include channel bandwidth and the modulation and coding scheme used. Other parameters, such as number of subchannels, OFDM guard time, and oversampling rate, also have an impact.

7.2 WiMAX OFDM

OFDM belongs to a family of transmission schemes called multicarrier modulation, which is based on the idea of dividing a give 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 intersymbol 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%) fraction of the symbol duration. OFDM is spectrally efficient versions 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 non overlapping subcarrier channels to eliminate inter carrier 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 guard interval, however, implies power wastage and a decrease in bandwidth efficiency.

VIII. Adaptive Modulation andCoding in WiMAX

WiMAX supports a variety of modulation and coding schemes and allows for the schemes 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.

	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	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6

IX. WiMAX MAC (Medium Access Control) Layer (data link 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 organize them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse. 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 that include the following:

- Privacy key management (PKM) for MAC layer security.
- Broadcast and multicast support.
- Manageability primitives.
- High-speed handover and mobility management primitives.
- Three power management levels, normal operation, sleep and idle.
- 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.

Support for QoS is a fundamental part of the WiMAX MAC-layer design. WiMAX borrows some of the basic ideas behind its QoS design for 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.

X. WiMAX Quality of Service (QoS)

WiMAX Quality of Service or WiMAX QoS is a key element in the delivery of service over the WiMAX medium. With techniques such as Internet Protocol being used, delays or latency and jitter can be introduced into the data transmission arena. To overcome the effects of latency and jitter, the concept of quality of service is used. For WiMAX Qos several techniques and definitions are at the core of implementation.
In order to categorize the different types of quality of service, there are five WiMAX QoS classes that have been defined.

10.1 Unsolicited Grant Service

The Unsolicited Grant Service, UGS is used for real-time services such as Voice over IP, VoIP for applications where Wimax is used to replace fixed lines such as E1/T1.

10.2 Real-time Packet Services

This WiMAX QoS class is used for real-time services including video streaming. It is also used for enterprise access services where guaranteed E1/T1 rates are needed but with the possibility of higher bursts if network capacity is available. This WiMAX QoS class offers a variable bit rate but with guaranteed minimums for data rate and delay.

10.3 Extended Real Time Packet Services

This WiMAX QoS class is referred to as the Enhanced Rea Time Variable Rate, or Extended Real Time Packet Services. This WiMAX QoS class is used for applications where variable packet sizes are used – often where silence suppression is implemented in VoIP. One typical system is Skype.

10.4 Non-real time Packet Services

This WiMAX QoS class is used for services where a guaranteed bit rate is required but the latency is not critical. It might be used for various forms of file transfer.

10.5 Best Effort

This WiMAX QoS is that used for Internet services such as email and browsing. Data packets are carried as space becomes available. Delays may be incurred and jitter is not a problem.

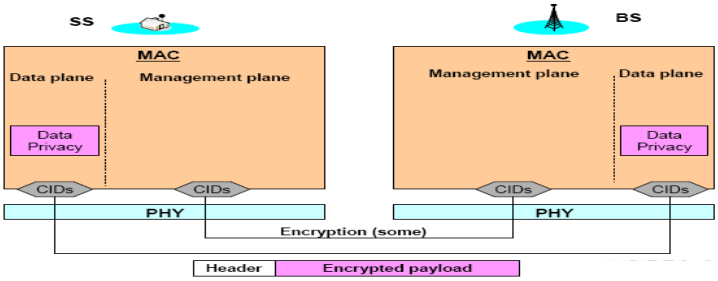
XI. WiMAX Security

Security in WiMAX is handled by a privacy sublayer within the WiMAX MAC. The key aspects of WiMAX security are as follows:

11.1 Support for Privacy

User data using cryptographic schemes of proven robustness to provide privacy. Both AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard) are supported.

11.1.1 Encryption in WiMAX



- When transmitting a MAC PDU on a connection that is mapped to a SA, the sender should perform encryption and data authentication of the MAC PDU payload as specified by that SA. When receiving a MAC PDU on a connection mapped to an SA, the receiver shall perform decryption and data authentication of the MAC PDU payload, as specified by that SA.
- Two bits of a MAC header contain a key sequence number. The keying material associated with an SA has a limited lifetime, and the BS periodically refreshes an SA's keying material. The BS manages a 2-bit key sequence number independently for each SA and distributes this key sequence number along with the SA's keying material to the client SS. The BS increments the key sequence number with each new generation of keying material. The MAC header includes this sequence number to identify the specific generation of that SA keying material being used to encrypt the attached payload. Being a 2-bit quantity, the sequence number wraps around to 0 when it reaches 3.

Security Associations (SA)

A security association is a set of security information a BS and one or more of its client SSs share in order to support secure communications across the IEEE 802.16 network. Three types of SAs are defined: Primary, Static and Dynamic. Each SS establishes a primary security association during the SS initializing process. Static SAs are provisioned by the BS. Dynamic SAs are established and eliminated, on the fly, in response to the initiation and termination of specific service flows. Both static and dynamic SAs may be shared by multiple SSs. Each SS shall establish an exclusively Primary SA with its BS. The SAID of any SA's Primary SA shall be equal to the basic CID of that SS.

11.2 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 operators can use the certificates for device authentication and use a username/password or smart card authentication on top of it for user authentication.

11.2.1 EAP Protocol

The Extensible Authentication Protocol (EAP)is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time password and public key authentication.

11.2.1.1 EAP-TLS

EAP-TLS is an extension to the Extensible Authentication Protocol and provides Transport Level Security (TLS). EAP-TLS provides for mutual authentication ciphersuite negotiation and key exchange between two endpoints. In WiMAX, EAP-TLS is used in cases where no user authentication is being done and instead just server and device authentication is done.

11.2.1.2 EAP-TTLS

EAP TTLS is an extension to EAP-TLS. It allows the server to authenticate the client within a secure connection established during the TLS handshake. Within the secure connection, a number of protocols may be used to authenticate the client. The CHAP authentication method and MS-CHAPv2 uses a secret only known by the server and the client. Tunneled CHAP and MS-CHAPv2 authentication shall be supported by the MS and its AAA server.

11.2.1.3 AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING) Server

AAA monitors user access in the network. In AUTHENTICATION, the identity of the user is verified, using a password etc. During AUTHORIZATION, a check on what services a user is allowed to access and how much Quality of Service (QoS) the user can get etc. is done. In ACCOUNTING, billing for all services availed are done, based on the IP flow, duration of access etc.

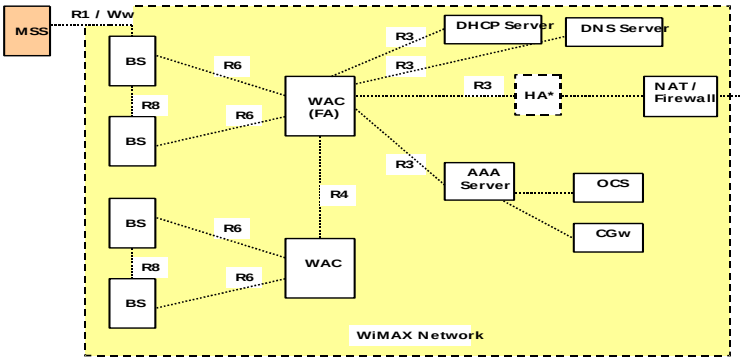


Fig. 1 WiMAX echo system

WAC: WAC provides/participates in authentication and authorization of MS, MS IP establishment (by the DHCP relay/proxy function), MP procedures, idle mode and Paging procedures, QoS management, BS management etc.

Omc-R (Operation & Maintainance Controller-Radio)

- OMC-R is used as the management platform of the WiMAX Radio Access Network (RAN), provisioning and providing template-based radio configuration.
- Performs network surveillance, quality o service monitoring and radio network planning/optimization for the WiMAX Access Network.

Ntp (Network Time Protocol) Server

- It is used toensure time synchronization between every entity that provides timestamps, in order to have a unique time in the network.

Csn (Core Service Network)

This represents a set of network elements between every entity that provides timestamps, in order to have a unique time in the network.

Dns (Domain Name Server)

- Used to allocate IP address to all RAN NEs, MSs (in the subnet associated to the HA)
- Update DNS dynamically (DDNS)

Session Border Controllers (Sbc)

- Present at the border of the core network
- Acts signaling Application Layer Gateway (ALG) and media gateway for VoIP service.
- Handles QoS and acts as the SIP proxy (P-CSCF) between MS and Softswitch.

Charging Gateway

The user's usage duration, quantity etc. are sent to the charging gateway. It calculates the charges based on the usage.

HOME AGENT (HA)

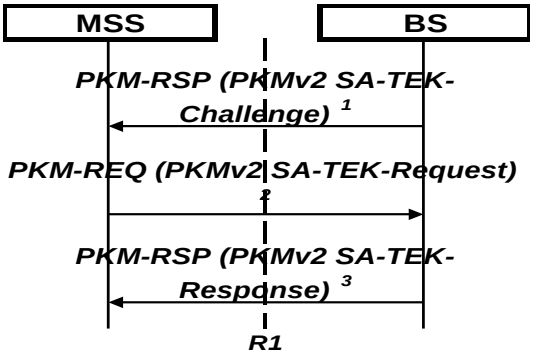
- It is a router responsible for routing packets from the MS subnet to ASP/ISP and vice-versa.
- It makes a match between the CoA (care-of-address) and the HoA (Home address=IP address of the MS in the network).

Foreign Agent (Fa)

- The WAC acts as the FA. It has the CoA of the MS. Any packet meant for the MS is redirected from HA to FA, which in turn sends to the corresponding MS.
- It is router responsible for routing packets from the MS subnet to ASP/ISP and vice-versa. It makes a match between the CoA (care-or-address) and the HoA (Home address=IP address of the MS in the network).

Authentication And Encryption

- The authentication of the MS is done by means o a signaling exchange using EAP (Extensible authentication protocol).
- EAP allows for a variety of user credentials, including username/password, digital certificates and smart cards.
- The authentication during INE is always started by WAC.
- NAI (network access identifier) is given by MS during authentication. It is used for identifying the MS, as well as routing messages.
-



PKM Key exchange

- SA-TEK3-way handshake is performed to validate the ASK.
- All three messages in the handshake are integrity protected using the new PMK/AK context.
- The challenge message maps the AK Sequence number (assigned to PMK) and AKID.
- Security parameters negotiation is done in the Request response messages.

11.3 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.

11.4 Protection of control messages

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

11.5 Support for fast handover

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

XII. Conclusion

The spread of different broadband wireless technologies all over has led to increased dependency and concern regarding the drawbacks it suffers. Of all drawbacks, security has always been the biggest threat and is covering broader areas of research. Albeit, with the help of WiMAX technology 802.16e that offers security relief to a greater extent. The different versions of WiMAX, as defined by IEEE protocols introduced till today compete in different features. Earlier use of landline and other wired equipments has been replaced by the use of smart cards, cellular wireless devices and many more and hence, this dependency graph on wireless communication will also extend to higher limits. Hence, continuous research in this field is always expected.

References

[1]. Thesis on WiMAX.
[2]. WiMAX Forum technology (retrieved 2008).
[3]. Roger Marks- IEEE 802.16 WirelessMANStandard:myths and facts.
[4]. Carl Weinschenk : Speeding up WiMAX.
[5]. IEEE 802.16e Task Group (Mobile WiMAX).
[6]. HIPERMAN/WiMAX testing (retrieved 2008).
[7]. K. Fazel and S. Kaiser, Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX. 2nd edition, John Wiley $ Sons,2008.
[8]. M. Ergen, Mobile Broadband-including WiMAX and LTE, Springer, NY, 2009.
[9]. Prashant Sharma (2009), Facts about WiMAX.