

WiMax-A Broadband Wireless Connectivity

Mr. Parminder Singh*, Mr. Manish Mahajan**, Sandeep singh kang***

*singh.parminder06@gmail.com, **manishmahajan4u@gmail.com

*/*** CEC Landran (Mohali), ** RIMT Mandi Gobindgarh

Abstract -This paper present the wireless broadband connectivity using Wi-Max earlier technology only provides local area wireless connectivity (i.e Wi-Fi). WiMax provides an appropriate solution to certain rural or hard to access zones that are today prevented from having access to broadband Internet because of cost considerations. This technology thus aims to introduce an alternative to DSL and cabled networks on the one hand, and interconnecting Wi Fi hot spots on the other.

Keywords: WiMAX. Authentication, authorization, connections, encryption, IEEE 802.16, security, standards.

I INTRODUCTION:

The term WiMAX (Worldwide Interoperability for Microwave Access) has become synonymous with the IEEE 802.16 Wireless Metropolitan Area Network (MAN) air interface standard. In its original release the 802.16 standard addressed applications in licensed bands in the 10 to 66 GHz frequency range and unlicensed bands from 2 to 11 GHz bands. The new 802.16a standard specifies a protocol that among other things supports low latency applications such as voice and video, provides broadband connectivity without requiring a direct line of sight between subscriber terminals and the base station (BTS) and will support hundreds if not thousands of subscribers from a single BTS. The standard will help accelerate the introduction of wireless broadband equipment into the marketplace, speeding up last-mile broadband deployment worldwide by enabling service providers to increase system performance and reliability while reducing their equipment costs and investment risks. The latest 802.16e amendment is supporting for mobility in WiMAX system. Like WiFi (IEEE 802.11) before it, WiMAX promises explosive growth. The key to taking advantage of WiMAX opportunities is to understand the technology's evolution and anticipated deployment.

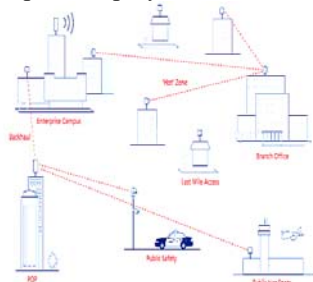


Figure: Wi-Max uses BWA

A. IEEE 802.16a Standard and wireless broadband connectivity WiMAX furnishes broadband connectivity over a much wider area than WiFi and does not require a direct line of sight between subscriber terminals and access points. In contrast to WiFi, WiMAX's range is typically measured in miles rather than feet. This distinction points up the difference between the two standards: WiFi is a local-area networking (LAN) technology, while WiMAX is a MAN technology. The "metropolitan" in "metropolitan-area network" does not restrict WiMAX to urban environments, however. This technology is much more efficient in several areas. It offers a maximum useful throughput of 60 megabytes per second (Mbps) in a 20-MHz channel, as compared to 25 useful Mbps under standards 802.11 a or g.

a. BWA Coverage

Broadband Wireless Access (BWA) is designed for optimal performance in all types of propagation environments. Advanced topologies (mesh networks) and antenna techniques (beam-forming, STC, antenna diversity) can be employed to improve coverage even further. These advanced techniques can also be used to increase spectral efficiency, capacity, reuse, and average and peak throughput per RF channel. WLANs and 802.11 systems have at their core either a basic CDMA approach or use OFDM with a much different design, and have as a requirement low power consumption limiting the range. OFDM (Orthogonal Frequency Division Multiplexing) in the WLAN was created with the vision of the systems covering tens and maybe a few hundreds of meters versus 802.16 which is designed for higher power and an OFDM approach that supports deployments in the tens of kilometers.

B. QoS

Several features of the WiMAX protocol ensure robust quality-of-service (QoS) protection for services such as streaming audio and video. As with any other type of network, users have to share the data capacity of a WiMAX network, but WiMAX's QoS features allow service providers to manage the traffic based on each subscriber's service agreements on a link-by-link basis.

The 802.16a MAC relies on a Grant/Request protocol for access to the medium and it supports differentiated service levels. By assuring collision-free data access to the channel, the 16a MAC improves total system throughput and bandwidth efficiency, in comparison with contention-based access techniques like the CSMA-CA protocol used in WLANs. The 16a MAC also assures bounded delay on the

data (CSMA-CA by contrast, offers no guarantees on delay). The TDM/TDMA access technique also ensures easier support for multicast and broadcast services.

If the number of CSMA/CA access-point users goes up to dozens or hundreds of users, many more users tend to collide, back-off and retransmit data. In such an environment, average network loading factors can easily rise past 20 to 30 percent, and users notice delays—especially in streaming-media services.

Another aspect of WiMAX QoS provisioning is link-by-link data-rate manageability. The signal strength between base and subscriber stations affects a wireless link’s data rate and ability to use various modulation schemes within the 256 OFDM framework. Signal strength depends mainly on the distance between the two stations. If the network were restricted to a single modulation scheme per carrier, subscribers that are farther away from the base station would limit the network’s ability to use the most efficient scheme.

In addition to general-purpose QoS features, WiMAX provides specific QoS support for voice and video. To enable toll-quality voice traffic, for example, voice packets can be tagged as such. The base-station’s scheduler then manages the passage of these packets through the air interface to provide deterministic latency.

B. IEEE 802.16 PROTOCOL LAYER

A. Physical Layer

WiMAX uses OFDM technology. Orthogonal frequency division multiplexing (OFDM) allows assigning sub carriers to different users. It is resilient to multipath that helps to overcome multiple signals hitting the receiver. The IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) and support both full and half duplex stations. TDD framing is adaptive, it has a fixed duration, which consists of one Uplink and one Downlink frame.

The IEEE 802.16 supports two types of transmission duplexing: Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) and support both full and half duplex stations. TDD framing is adaptive, it has a fixed duration, which consists of one Uplink and one Downlink frame. BS sends the complete downlink subframe (DLMAP,ULMAP). In TDD, the portion allocated for the downlink and portion allocated to the uplink may vary. The Uplink is time division multiple access (TDMA) where bandwidth is split into time slots. Each time slot is allocated to an individual MS being served by the BS.

B. IEEE 802.16 MAC

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 sublayer that can interface with a variety of higher-layer protocols, such as ATM, TDM Voice, Ethernet, IP, and any unknown future protocol. Given the predominance of IP and Ethernet in the industry, the WiMAX Forum has decided to support only IP and Ethernet at this time. Besides providing a mapping to and from the higher layers, the convergence sublayer supports MSDU header suppression to reduce the higher layer overheads on each packet. The WiMAX MAC uses a variable-length MPDU and offers a lot of flexibility to allow for their efficient transmission.

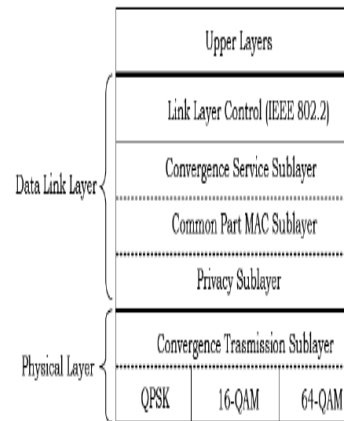


Figure 1: IEEE 802.16 Protocol Layer (IEEE, 2004)

C. Standard issues: interoperability and upgrades:

As the IEEE 802.16 standard continues to evolve, the WiMAX Forum will follow the latest version of the standard for interoperability testing. At the same time, the Forum seeks to maintain backward compatibility with deployed WiMAX Certified equipment.

Ongoing work on the 802.16 standard is adding significant new capabilities to the technology. For example, the 802.16 standard will define mechanisms for portability and nomadic mobility to enable ubiquitous connectivity.

To further support ubiquitous connectivity, the IEEE is defining a handoff mechanism between 802.11 and 802.16 equipment. Using this mechanism, a laptop could transition from using a WiFi hotspot or enterprise WiFi WLAN to a WiMAX network furnished by a local service provider. This handoff will take place seamlessly and without user intervention while maintaining network connectivity.

D. WiMAX security issues

WiMAX is the much-anticipated broadband wireless access mechanism for delivering high-speed connectivity over long distances, making it attractive to Internet and telecommunications service providers. Designed by the IEEE 802.16 committee, WiMAX was developed after the security failures that plagued early IEEE 802.11 networks. Recognizing the importance of security, the 802.16 working groups designed several mechanisms to protect the service provider from theft of service, and to protect the customer from unauthorized information disclosure.

i) Authentication

A fundamental principle in 802.16 networks is that each subscriber station (SS) must have a X.509 certificate that will uniquely identify the subscriber. The use of X.509 certificates makes it difficult for an attacker to spoof the identity of legitimate subscribers, providing ample protection against theft of service. A fundamental flaw in the authentication mechanism used by WiMAX's privacy and key management (PKM) protocol is the lack of base station (BS) or service provider authentication. This makes WiMAX networks susceptible to man-in-the-middle attacks, exposing subscribers to various confidentiality and availability attacks. The 802.16e amendment added support for the Extensible Authentication Protocol (EAP) to WiMAX networks. Support for EAP protocols is currently optional for service providers.

ii) Encryption

With the 802.16e amendment, support for the AES cipher is available, providing strong support for confidentiality of data traffic. Like the 802.11 specification, management frames are not encrypted, allowing an attacker to collect information about subscribers in the area and other potentially sensitive network characteristics.

iii) Availability

WiMAX deployments will use licensed RF spectrum, giving them some measure of protection from unintentional interference. It is reasonably simple, however, for an attacker to use readily available tools to jam the spectrum for all planned WiMAX deployments. In addition to physical layer denial of service attacks, an attacker can use legacy management frames to forcibly disconnect legitimate stations. This is similar to the deauthenticate flood attacks used against 802.11 networks.

iv) WiMAX Threats

Despite good intentions for WiMAX security, there are several potential attacks open to adversaries, including:

- a. Rogue Base Stations
- b. DoS Attacks
- c. Man-in-the-Middle Attacks
- d. Network manipulation with spoofed management frames

The real test of WiMAX security will come when providers begin wide-scale network deployments, and researchers and attackers have access to commodity CPE equipment. Other attacks including WiMAX protocol fuzzing may enable attackers to further manipulate BSs or SSs. Until then, the security of WiMAX is limited to speculation.

E. Vulnerabilities

a. VoIP is increasingly gaining traction among both consumers and enterprise users, offering an alternate, cost-effective means of communications against the traditional public switched telephone network (PSTN). Considering how WiMAX's enhanced MAC protocol offers higher QoS for low latency applications such as VoIP, it is expected that this service will comprise the bulk of bandwidth within the first few months of deployment. However, just as within a WiFi environment, there remain several vulnerabilities with VoIP in a WiMAX ecosystem. A VoIP system uses protocols like H.323, MGCP, Megaco and session initiation protocols (SIP) for signaling, and RTP/RTCP for media transport and control. Servers like media gateways, call agents, media gateway controllers, gatekeepers and proxies enable calling between the VoIP clients. SIP signaling protocols are exceptionally popular for their ease of implementation, interpretation and stateful analysis, but when left alone, are equally notorious for their vulnerability. Security risks remain within the signaling servers themselves, with hackers employing one of several methods to obtain unauthorized access. OEMs must address each of these methods individually, and as a whole, when developing an effective security infrastructure that can thwart against hackers.

i) *Client impersonation*: The SIP protocol can enable registration of multiple contacts for an individual user, with the "to" and "from" header fields unique per contact. By impersonating the client, a hacker can register his own contacts and make the incoming and voice mail notifications to the redirected contact addresses.

ii) *Server impersonation*: After a client registers with a credentialed server, hackers can intercept session initiation requests from the client and reply with a spoofed response that directs the request to a new server. The calls from the client will either fail or connect to the hacker's defined endpoints, either way exposing the client. Similarly, hackers can intercept session requests in the registration process itself, redirecting the register requests to a fake server and exposing the server's credentials.

iii) *Message tampering*: Considered as trusted intermediaries, proxy servers are often employed by clients to exchange session initiation requests and stream media. Hackers may implement spoofed proxy servers and unbeknownst to the clients, intercept their media session encryption methods and associated keys. With this vital information, they may redirect the media streams to their device and decrypt the information, or prevent the media stream from reaching its actual destination, allowing for wiretapping and eavesdropping.

iv) *Session tampering/hijacking*: After a call is established, messages are exchanged between the base station and CPE for session renewals and codec negotiations requests. However, during the call, it is possible for a hacker to tap into the stream and forge messages. When a client expects a session renewal message periodically, the session definition protocol (SDP) information is tampered with to divert the media stream, resulting in eavesdropped conversations.

v) *Signaling requests resulting in DoS attacks*: Proxy servers process registration and session initiation requests over a standard port number, through which hackers can instigate a flood of similar requests by spoofing multiple source IP addresses. Simultaneously barraging the server with multiple session initiation requests will result in server overload and denial of service.

vi) To protect against any of the aforementioned vulnerabilities, various 802.16-enabled devices within the WiMAX network, e.g. terminal adapters (TAs), integrated access devices (IADs), gateways, billing systems, voice mail

servers and unified messaging systems, must be equipped with software that can detect and prevent external infrastructure attacks before they take fruition. The complexity of this software varies with the type of the device, its usage, application and importance within the network.

CONCLUSION

WiMAX will revolutionize the broadband wireless access industry and open many opportunities to deploy systems in applications that was previously cost prohibitive. It's going to have a far bigger impact long term than we have seen from cellular phones in the past 15 years. Most of the other hot technologies, Video over Internet, Voice over Internet and others require high-speed access. In the next few years those who control the WiMax highways will become the next giants of IT industry

REFERENCES

Books:

[1] Stallings, W. Cryptography and Network Security: Principles and Practice, 2nd edition. Prentice Hall, 1999.

Websites:

www.wimaxforum.org

www.broadbandforum.co.in/wimax

www.wimax-vision.com