Review of WiMax Services & Security Threats

Er VidhuKiran Sharma
#Dept of Computer Science
GZC College, PTU Campus, Bathinda
Dr Shaveta Rani, Dr. Paramjeet Singh
#Dept of Computer Science
GZC College, PTU Campus, Bathinda

Abstract—*Now a day, there is a lot of technologies for communication. Wimax is an anticipated technology for wireless communication. Its aim is to provide high data rate at low cost. In this paper, all the basics for Wimax and their security threats will be discussed. Wimax can provide high data rate, quality of services, scalability and routing method. This paper will describe possible numbers of threats in Wimax due to different reasons.*

Keyword: *Wimax, architecture, threats, cause, standards*

INTRODUCTION

Wimax stands for Worldwide Interoperability for Microwave Access. Wimax technology is a telecommunications technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoint links. The Wimax technology offers around 72 Mega Bits per second without any need for the cable infrastructure. Wimax technology is based on Standard that is IEEE 802.16, it usually also called as Broadband Wireless Access. WiMAX Forum created the name for Wimax technology that was formed in Mid June 2001 to encourage compliance and interoperability of the Wimax IEEE 802.16 standard. WiMAX framework is based on several core principles:

- Support for different RAN topologies.
- Well-defined interfaces to enable 802.16 RAN architecture independence while
- enabling seamless integration and interworking with Wi-Fi, 3GPP3 and 3GPP2 networks.
- Leverage and open, IETF-defined IP technologies to build scalable all-IP 802.16 access networks using common off the shelf (COTS) equipment.

How WiMAX Works

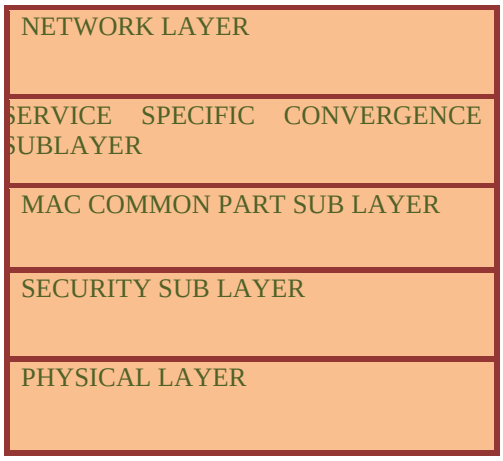
The backhaul of the Wimax (802.16) is based on the typical connection to the public wireless networks by using optical fiber, microwave link, cable or any other high speed connectivity. In few cases such as mesh networks, Point-to-Multi-Point (PMP) connectivity is also used as a backhaul. Ideally, Wimax (802.16) should use Point-to-Point antennas as a backhaul to join subscriber sites to each other and to base stations across long distance. A wimax base station serves subscriber stations using Non-Line-of-Sight (NLOS) or LOS Point-to-Multi-Point

A. Wimax types

B. Wimax can be of two types: wired (802.16) and wireless (802.16e)

B).Wimax Architecture

Wimax work most of the time in two layers: Physical and MAC Layer



At 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.
- 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.
- 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.

WiMax has two main topologies ~V namely Point to Point for backhaul and Point to Multi Point Base station for Subscriber station. 802.16 supports three physical layers. The mandatory physical mode is 256-point FFT OFDM (Orthogonal Frequency Division Multiplexing). The other modes are Single carrier (SC) and 2048 OFDMA (Orthogonal Frequency Division Multiplexing Access) modes. The corresponding European standard - the ETSI Hiperman standard defines a single PHY mode identical to the 256 OFDM modes in the 802.16d standard.

At MAC LayerThe MAC was developed for a point-to-multipoint wireless access environment and can accommodate protocols like ATM, Ethernet and IP (Internet Protocol). The MAC frame structure dynamic uplink and downlink profiles of terminals as per the link conditions. This is to ensure a trade-off of capacity and real-time robustness. The MAC uses a protocol data unit of variable length, which increases the

	Fixed Wimax	Mobile wimax
Standard	**802.16 developed at 2004**	**802.16e at 2005**
PHY	**256 OFDM**	**512 FDT OFDM**
Channel Sizes	**3.5,7,10 MHZ**	**5,7,10 MHZ**
Duplex	**TDD &FDD**	**TDD ONLY**
Modulation	**64 QAM on Uplink and Downlink**	**64 QAM on downlink,16 QAM on uplink**
System Feature	**Transparent Bridge, Self Install, Roaming**	**Handover Support, Paging, sleep mode**

standards efficiency. Multiple MAC protocol data unit can be sent as a single physical stream to save overload. Also, multiple Service data units (SDU) can be sent together to save on

MAC header overhead. By fragmenting, you can send large volumes of data (SDUs) across frame boundaries and can guarantee a QoS (Quality of Service) of competing services. The MAC uses a self-correcting bandwidth request scheme to avoid overhead and acknowledgement delays. This also allows better QoS handling than the traditional acknowledged schemes. The terminals have a variety of options to request for bandwidth depending on the QoS and other parameters. The signal requirement can be polled or a request can be piggybacked.

security in wimax

Security is a broad and complex subject, Well designed security architecture for a Wimax and other wireless communication networks should support the following essential requirements:

- Privacy: Provide protection from eavesdropping as the user data traverses the network from source to destination.
- Data integrity: Ensure that user data and control/management messages are protected from being tampered with while in transit.
- Authentication: Have a mechanism to ensure that a given user/device is the one it claims to be. Conversely, the user/device should also be able to verify the authenticity of the network that it is connecting to. Together, the two are referred to as mutual authentication.
- Authorization: Have a mechanism in place to verify that a given user is authorized to receive a particular service.
- Access control**:** Ensure that only authorized users are allowed to get access to the offered services.

Wimax security is typically handled at multiple layers within a system. Each layer handles different aspects of security, though in some cases, there may be redundant mechanisms. As a general principle of security, it is considered good to have more than one mechanism providing protection so that security is not compromised in case one of the mechanisms is broken. At the link layer, strong encryption should be used for wireless systems to prevent over-the-air eavesdropping. Also needed at the link layer is access control to prevent unauthorized users from using network resources: precious over-the-air resources.

Link layer encryptions are not often used in wired links, where eavesdropping is considered more difficult to do. In those cases, privacy is ensured by the comprehensive security mechanisms used at the higher layers. At the network layer, a number of methods provide security. The network itself may be protected from malicious attack through the use of firewalls. Authentication and authorization services are typically done through the use of Authentication, Authorization, and Accounting (AAA) protocols, such as RADIUS (Remote Access Dial-In User Service).. At the transport layer, TLS its precedent was called Secure Sockets layer (SSL) may be used to add security to transport layer protocols and packets. At the application layer, digital signatures, certificates, digital rights management, and so on are implemented, depending on the sensitivity of the application.

THREATS IN WIMAX

Rouge Base Station threa

A rogue base station is an attacker station that duplicates a legitimate base station. The **rogue base station** puzzles a set of subscribers trying to get service through what they believe to be a legitimate base station. It may result in long disturbance of service. The exact method of attack depends on the type of network. In a Wi-Fi network, which is carrier sense multiple access, the attacker has to capture the identity of a legitimate access point. Then it builds frames using the legitimate access point's identity. It then injects the crafted messages when the medium is available. In a **WiMax network**, this is more difficult to do because WiMax uses time division multiple access. The attacker must transmit while the **rogue base station** is transmitting. The signal of the attacker, however, must arrive at targeted receiver

subscribers with more strength and must put the signal of the rogue base station in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate base station. Then it builds messages using the stolen identity. The attacker has to wait until time slots allocated to the fake base station start and transmit during these time slots. The attacker must transmit while achieving a receive signal strength higher than the one of the fake base station. The receiver subscribers reduce their gain and decode the signal of the attacker instead of the one from the fake base station. The rogue base station is likely to occur as there are no technical difficulties to resolve. Extensible Authentication Protocol (EAP) supports mutual authentication, i.e. the base station also authenticates itself to the subscriber. When EAP mutual authentication is used, the likelihood of the threat is mitigated, but not totally and remains possible for reasons similar to EAP based authorization.

C. Denial of Service (DoS) Attacks on WiMAX

D. *when a wimax network has no downlink or uplink data, it will enter either Sleep Mode or Idle Mode, both of which aim to trim down the power utilization of the mobile station. Upon the availability of data, the serving base station will awaken the mobile station. The mobile station then establishes a connection with the base station via initial ranging. Ranging parameters are then adjusted for the connection. Finally, the service flow is reactivated for data transfer, and the mobile station returns to the normal operation stage. Depending on whether the serving base station has the necessary information, the mobile station may need to carry out more signaling operations, such as basic capability negotiation, authentication and key management, re-registration, as well as IP connectivity reestablishment. Given the above signaling procedures, attackers may also launch similar signaling attacks to WiMax base station by triggering unnecessary state transitions that overload the base station with signal processing that leads to denial of service (DoS) attacks*

E. Data link layer threats

WiMax Media Access Control (MAC) protocol, a sub layer of **the** data link layer, manage the consumer's access to the physical layer. However, the scheduling algorithm within the WiMAX MAC protocol offers optimal prioritization of this traffic based on First-In First-Out (FIFO) scheduling, in which clients seeking access to the base station are allocated bandwidth upon time of initial access, instead of random queue assignment based on order of Media Access Control **(**MAC) address as in Wi-Fi. Furthermore, the WiMax Media Access Control (MAC) protocol ensures optimal quality of service (QoS) over its Wi-Fi predecessor, allocating bandwidth effectively by balancing client's needs instead of best effort service; that is, equal distribution of what remains after allocation to other consumers.

In addition, before encrypting the radio signal with Wired Equivalent Privacy (WEP), WPA/PSK, or any other existing Layer 2 security protocol, WiMax basic authentication architecture, by default, employs X.509-based public key infrastructure (PKI) certificate authorization, in which the base station authenticates the client's digital certificate prior to granting access to the physical **layer.**

D. Application Layer Threats in Wimax

In an WiMax mesh network installation where routers or gateways will operate as intermediaries, or hot spots linking client and base station**, there is an increased potential of** security vulnerabilities**, as the intermediary routers that reside between base station and client are presentable and** vulnerable **to attacks. Popular** application level services**, such as voice over Internet protocol (VoIP), could be broken by hackers who can initiate the download of remote configuration settings and resynchronize clients' CPE settings to their specifications. Hackers may also replicate, or spoof the address of the intermediary router or server and deceive other clients into believing their**

connection is secure, thus opening them up to malicious attack. These routers and gateways will require robust security measures to ensure that unprotected clients remain protected behind the intermediary access point.

F. .Physical Layer Threats to Wimax Technology

Privacy Sub-layer resides on the top of **Physical layer** in IEEE 802.16 standard, therefore, **Wimax networks** are open to to **physical layer attacks** for example, blocking and rushing. Blocking is done by activating a source of strong noise to significantly lowering the capacity of the channel, therefore denying services (DoS) to all stations. Blocking or jamming is detectable with radio analyzer devices. Rushing or scrambling is another type of jamming, but it takes place for a short interval of time aimed at particular frames. Control or management messages could be jumbled, but it is not possible with delay sensitive message i.e., scrambling Uplink slots are comparatively hard, because attacker has to interpret control information and to send noise during a particular interval.

G. Privacy Sub Layer Threats to Wimax Technology

Privacy Sub layer's main objective was to protect service providers against theft of service, rather than securing network users. It is obvious that the **privacy sub layer** only secures data at the data link layer, but it does not ensure complete encryption of user data. Furthermore, it does not protect physical layer from being interrupted. It is essential to include technologies to secure physical layer and higher layer security for a converged routable network and devices within the system

G Mutual Authentication Problem in Wimax

There are two types of **certificate** are categorize by WiMax standard: one is for **Subscriber Station** (SS) certificates and the other is for manufacturer certificates but there is no provision for Base Station (BS) certificates. A manufacturer certificate identifies the manufacturer of a WiMax device. It can be a self signed certificate or subjected to any third party. A Subscriber certificate identifies a particular **Subscriber Station** and enclosed its MAC address in the subject field. Manufacturers normally create and sign **Subscriber Station certificates**.

H. Threat of Identity Theft In WiMAX

This method includes reprogramming of a device with the hardware address of another device. The address can be stolen over the air by interrupting management messages. A **rogue Base Station (BS)** is an attacker station which act as a genuine **Base Station (BS)**. It confuses a set of Subscriber Stations or Mobile Stations when attempting to get service through what they believe being a genuine **Base Station (BS)**. It is complicated in WiMax networks because of time division multiple access (TDMA) model. In this case, the attacker must transmit while the real **Base Station (BS)** is transmitting, with more signal strength and place the real **Base Station (BS)**'s signal in the background, additionally attacker has to capture the identity and wait until a time slot of genuine **Base Station (BS)** starts transmitting the data. **Threat of Water Torture in Wimax Technology**

I. Black Hat Threats to WiMAX Technology

Another threat to WiMax is **black hat** hackers, they are commonly known as awful people in our world with the negative thinking about cracking into the network or the computer system for their own financial benefit or mental satisfaction. They are also known as crackers or **Black Hats**. The essential thing to understand is not all the hackers are terrible as some people are doing penetration of a network or computer system in the limits of ethical standards to understand the vulnerabilities in their system or their clients system, also called white hat hackers. There are still the possibility that the WiMAX network can be a victim of **black hats** like WiFi and other wireless technologies.

conclusion

Security is a main concern in wireless communication as compared to wired communication. Researcher try to find solution for explored threats, but research for threats that are not in our knowledge is not possible. We try our best to conclude them for future research.

References

[1] L. Nithyanandan1 and I. Parthiban, *"vertical handoff in WLAN-wimax-lte heterogeneous networks through gateway relocation*", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 4, Aug 2012

[2] Payaswini P, Manjaiah D.H*," Simulation and Performance analysis of Vertical Handoff between Wi-Fi and WiMAX using Media Independent Handover Service* ", International Journal of Computer Applications (0975 – 8887) Volume 87 – No.4

[3] R. Augastiny, S. Sarala, C. Janani *,"A QoS based Vertical Handoff scheme for WiMAX/WLAN Networks*", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153

[4] R.Divya, T.Jayasimha*," LMS Algorithm for Smart WIMAX Antenna* ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, December 2013 ISSN: 2277 128X

[5]Prabhakar Telagarapu, K.Chiranjeevi,"*Analysis of Coding Techniques in WiMAX*, International Journal of Computer Applications (0975 – 8887) Volume 22– No.3, May 2011

[6] B.Sridevi, M.Brindha,R.Umamaheswari," I*mplementation of secure & cost effective authentication process in IEEE 802.16e wimax*", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012

[7] Prakash Kuppuswamy1, Sikandhar Shah," Improving Security Authentication of IEEE 802.16 WiMax with New Public key algorithm", International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 3 Issue 2 February, 2014 Page No. 3965-3970

[8]Rakesh Kumar Jha, Dr Upena D Dalal,"A Journey on WiMAX and its Security Issues", International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010, 256-263

[9]Rakesh Kumar Jha Dr. Upena D. Dalal,"A Performance Comparison With Modulation Schemes in WiMAX Physical Layer Security Aspect", International Journal of Computer Applications (0975 – 8887) Volume 6– No.8, September 201

[10] Hsien-Chou Liao and Cheng-Jung Lin," A Position-Based Connectionless Routing Algorithm for MANET and
WiMAX under High Mobility and Various Node Densities", Information Technology Journal 7 (3): 458-465, 2008