ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Review on WiMAX Security

G.Rama Subba Reddy
Research Scholar,
Department of Computer Science and Engineering,
Sunrise University, Alwar, Rajasthan, India.

Dr.Akash Saxena
Professor,
Department of Computer Science and Engineering,
Sunrise University, Alwar, Rajasthan, India.

Abstract:
WiMAX is broadband wireless system being used for long range wireless networking, which makes this system vulnerable to security breaches. Authentication is one of the most important security processes in Worldwide Interoperability for Microwave Access (WiMAX) networks. This process allows the receiver (whether base station or subscriber station) of a packet to be confident of the identity of the sender and the integrity of the message. we review the state of art of WiMAX authentication mechanisms, namely, PKMv1, PKMv2, and the recent authentication protocols. In this paper ,we discuss their mechanisms, strengths, weaknesses, and potential countermeasures against each other.

Keywords:
WiMAX, security, authentication, PKMv1, PKMv2.

1. INTRODUCTION:

Security has become a primary concern in order to pro-vide protected communication in Wireless environment IEEE Standards Board in 1999 Established , the IEEE 802.16 is a working group on Broad Wireless Access (BWA). Worldwide-Interoperability for Microwave-Access (WiMAX) is an emerging wireless internet technology which provides higher data transmission rate up to 70 Mbps with a broad coverage upto 50km. Broad coverage of WiMAX makes it suitable for Wireless Last Mile Technology. WiMAX apply point-to-point (PP) and point-to-multipoint (PMP) applications to provide its services. It supports two types of transmission techniques Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS).

The motive behind this technology is to ply fixed broadband wireless access to IP based user, as it is optimal for the distribution of IP centric service over a wide geographical area. The deployment of such rising broadband networks provides opportunities for services models and new applications. WiMAX system provides broadband access avails to the residential and enterprise customer in an frugal way, so it's become very popular and growing vast day by day. Since the wireless medium is available to all, the assaulters can easily admittance to network and the network becomes more vulnerable for the user. Therefore, the security support is highly desired for this system. To understand WiMAX security issues, it is needed to understand WiMAX architecture [1]. Poorly maintained network and device security opens the door for service disruption and theft. Not only the users of broadband service must protect their own personal information, but public networks must be designed and implemented with security in mind. In Section two concentrate our study on WiMAX ,section three will focus on WiMax security attacks and security mechanisms and then conclusion will be given in section four.

2. OVERVIEW OF WIMAX:

The overview of WiMAX (802.16) Layered Architecture is shown in below figure 1. Here we will discuss the all layers.

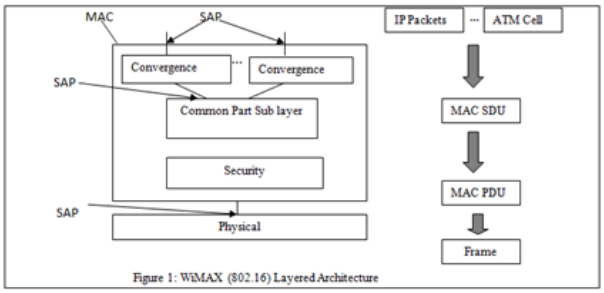

Figure 1: WiMAX (802.16) Layered Architecture

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.1 Physical Layer (PHY):

Physical layer provides two-way mapping between MAC Layer PDUs and PHY layer frames. Physical layer defines the transmission power and modulation demodulation techniques [2].

2.2 Medium Access Control Layer (MAC):

MAC layer of WiMAX provides an edge between the network layer and the physical layer. MAC layer prepares MAC PDUs from the packets or ATM Cells received from the network layer. In addition, MAC Layer maintains the scheduling and multiple access connection. Sub-Layers of MAC Layer are discussed below.

2.2.1 Convergence Sub-Layer (CS):

CS layer adapts data units (IP packets or ATM cells) from higher layers and prepares MAC Service Data Unit (SDU). Mapping between higher level data services to MAC layer service is also done by Service Access Points (SAP) at CS layer.

2.2.2 Common Part Sub-Layer (CPS):

CPS defines the rules for system access, grant connection control, uplink scheduling, bandwidth request and allocation etc. CPS also handles MAC PDU construction, connection establishment and bandwidth management. MAC SAPs exchanges MAC SDUs with the CS layer. SPS is tightly incorporated with the Security Sub-Layer.

2.2.3 Security Sub-Layer:

Security Sub-Layer exchanges MAC PDUs with physical layer. This Sub-layer is responsible for the encryption/decryption of MAC SDUs and MAC PDUs including with authentication handling and secure key exchange. Figure 2 shows the security sub-layer of MAC for Mobile WiMAX. Security Sub-Layer of MAC defines all the security specifications related to IEEE 802.16 standard [2].

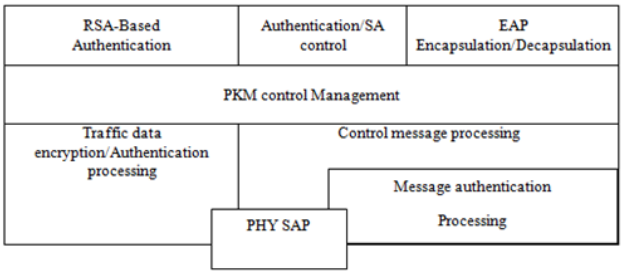

Figure 2: Security sub-layer components

Security Sub-Layer applies three steps to support WiMAX security; Subscriber Authentication (at the time of entry in to the network), Subscriber Authorization (if the subscriber is provisioned by the NSP), and then Encryption (for the secure key exchange and data traffic). Component Protocols at Security Sub-layer guarantee the authorization and confidentiality at the time of link establishment between the authorized parties (service provider and subscriber). Encapsulation Protocol (EP): EP secures packet data across the IEEE 802.16d (fixed BWA) network. It defines a set of well defined cryptographic suites (pairs of data encryption and authentication algorithms) and protocol to apply those algorithms to MAC PDUs.

Protocol for Key Management (PKM):

PKM provides secure distribution of featured data from BS to SS. PKM helps SS and BS in the synchronization of featured data. PKM imposes restricted network access to the BS [4]. The security procedure of PKM protocol is implemented in three successive steps:

(i) authentication, wherein the BS verifies and grants the SS to access the network resources;
(ii) exchanging of keys between BS and SS; and
(iii) data encryption by using exchanged keys.

3. WIMAX SECURITY ATTACKS:

WiMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack including interception, fabrication, modification, and replay attacks. Some vulnerabilities of WiMAX originate from flaws of IEEE 802.16 on which

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

WiMAX is based. A lot of problems and flaws have been fixed in the enhanced version but WiMAX still has some exposes. In this section some possible threats or vulnerabilities will be reviewed [3].

3.1 THREATS TO THE PHY LAYER:

WiMAX security is implemented in the security sub-layer which is above the PHY layer. Therefore the PHY is unsecure and it is not protected from attacks targeting at the inherent vulnerability of wireless links such as jamming, scrambling or water torture attack. WiMAX supports mobility, thus it is more vulnerable to these attacks because the attackers do not need to reside in a fixed place and the monitoring solutions presented below will be more difficult [9].

3.1.1 Jamming Attack:

Jamming is described by M. Barbeau as an attack "achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel". Jamming can be either intentional or unintentional. It is not difficult to perform a jamming attack because necessary information and equipment's are easy to acquire and there is even a book by Poisel which teaches jamming techniques.

3.1.2 Scrambling Attack:

Also described in, scrambling is a kind of jamming but only provoked for short intervals of time and targeted to specific WiMAX frames or parts of frames at the PHY layer. Attackers can selectively scramble control or management information in order to affect the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more difficult to perform a scrambling attack than to perform a jamming attack due to "the need, by the attacker, to interpret control information and to send noise during specific intervals".

3.1.3 Water Torture Attack:

According to D. Johnson and J. Walker, this is also a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources.

3.1.4 Other Threats:

In addition to threats from jamming, scrambling and water torture attacks, 802.16 is also vulnerable to other attacks such as forgery attacks in which an attacker with an adequate radio transmitter can write to a wireless channel. In mesh mode, 802.16 is also vulnerable to replay attacks in which an attacker resends valid frames that the attacker has intercepted in the middle of forwarding process.

3.2 THREATS TO THE MAC LAYER:

This section begins with an overview of the WiMAX/802.16 MAC layer, including a description of its connections, the process used by an MS for joining the network, and the MAC security model. The causes of MAC layer security issues are due to certain un-encrypted MAC management messages [4]. The major security issues in PMP network are,

- DoS/Reply attacks during MS Initial network entry
- Latency during handover and unsecured pre authentication
- Downgrade attack
- Cryptographic algorithm computational efficiency
- Bandwidth spoofing

3.2.1. Security Sub-Layer:

The security sub-layer generally provides a secure communication between BS and SS. The security sub-layer consists of two main protocols. The first protocol is an encapsulation protocol for data encryption, thus ensuring privacy and confidentiality. The second protocol is the PKM protocol, which provides authorization, authentication, and key exchange between BS and SSs. Two versions of the PKM protocol have been approved in the IEEE 802.16 standard. The first version is PKMv1, which has been specified in the IEEE 802.16 d-2004 standard.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This version uses RSA as an authentication mode and provides one direction of authentication (i.e., from SS to BS). The second version is PKMv2, which has been designed to address the limitations found in PKMv1 [5]. The following authentication protocol methods are supported in PKM:

RSA: This protocol is mandatory in PKMv1 and optional in PKMv2;

EAP: This protocol is supported in PKMv2.

3.3 SECURITY MECHANISMS:

In order to provide data integrity and privacy over an open radio channel, the MAC layer of 802.16 includes a security sub layer. The security mechanisms include the encryption of data between the base station (BS) and subscriber station (SS), certificate-based authentication of the SS, and privacy key management (PKM) as an authenticated client-server key management protocol. In order to patch up some major security issues described below and to account for the addition of mobile services, the standard 802.16e has specified some changes in the security measures [6].

3.3.1 Encryption:

802.16 includes RSA (Rivest Shamir Adleman), DES-CBC (Data Encryption Standard- Cipher Block Chaining) and AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) as the standard encryption algorithms and HMAC (Hashed Message Authentication Code) and CMAC (Cipher-based Message Authentication Code) as the cryptographic algorithms. These algorithms are used for the encryption of traffic encryption keys (TEKs), traffic data, and Authorization Reply messages.

3.3.2 Security Associations:

Security Associations (SAs) are information sets that support secure communication that is shared between a Base Station (BS) and its client SSs or mobile stations (MSs) .This may include information such as the cryptographic suite used for the SA, data encryption methods, and TEKs along with their lifetimes and state information. Upon entering a network, an SS will set up a primary SA, and then may add static and dynamic SAs depending on specific service flows.

3.3.3 Certificate-Based Authentication:

X.509 Version 3 certificate formats must be used by SSs in order to comply with the 802.16 standard. The manufacturer provides and installs a unique X.509 certificate in each SS, which contains the SS RSA Vandana V. Gawit et al, International Journal of Computer Science and Mobile Computing, public key and SS MAC address. In standards 802.16-2004 and above there is also an X.509 certificate for the BS so that both the SS and BS can mutually verify authenticity.

3.3.4 Privacy Key Management Protocol (PKM):

PKM establishes a shared secret between the SSs and BS to allow the BS to distribute keying materials such as Authorization Keys (AKs) and SAs to client SSs as well as periodic renewal and reauthorization of keys. The authorization and TEK state machines manage keys in the SS. PKM request and Response messages are sent between the BS and SS as MAC management messages to handle transmission of the AKs [8] . A new instance of the TKE state machine is started by the SS for each SA that it receives from the BS.

PKMv1 is used in the standard up until 802.16e when PKMv2 was introduced to provide stronger security. The greatest difference between the two is that in PKMv1 the BS authenticates the SS and then enables the ciphering of data by providing it with keying material, whereas in PKMv2 there is mutual authentication between the BS and MS. Also, in PKMv1, public key cryptography is used for the establishment of a shared secret between the SS and BS, but in PKMv2 RSA-based or EAP-based authentication protocols are used along with RSA and EAP as sources of keying materials [7].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Table 1: WiMAX Threats and Countermeasure

Layer	Attack	countermeasure
Physical Layer	Jamming attack	Increase the power or bandwidth of signals
	Scrambling attack Anomalies monitoring,	Anomalies monitoring DCJS
	Water-Torture attack	Discarding bogus frames
	Forgery attack	Mutual authentication
MAC Layer	DoS Attack	Digital Signatures
	Access Network Security	PKI based key exchange
	MITM Attack	Diffie-Hellman key exchange protocol

4. CONCLUSION:

WiMAX is the emerging technology alternate for WiFi in wireless networks. Many studies have investigated WiMAX network security and developed or enhanced the authentication process. In this paper explains WiMAX architecture and security sub-layer components followed by WiMAX security threats and security mechanisms. This paper has been discussed WiMax security issues ,BS Authentication ,Replay and Dos Attack. Security mechanisms For WiMax Encryption, Security Associations, Certificate based authentication, privacy key management protocol.

REFERENCES:

[1] Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful Jahari Hashim, Borhanuddin M. Ali1 and Abbas Jamalipour "Authentication process enhancements in WiMAX networks" published in security and communication networks.

[2] Vinod Kumar Jatav, Dr. Vrijendra Singh 'Mobile WiMAX Network Security Threats and Solutions: A Survey" published in 2014 5th International Conference on Computer and Communication Technology.

[3] Ahmadi S. An overview of next-generation mobile WiMAX technology. IEEE Communications Magazine 2009; 47: 84–98.

[4] Sameni K, Yazdani N, Payandeh A. Analysis of attacks in authentication protocol of IEEE 802.16e. Int. J. Com. Net. Tech 2013; 1(1): 33–44.

[5] Bogdanoski M., Latkoski P., Risteski A., Popovski B. IEEE 802.16 security issues: a survey. 16th Telecommunication Forum (TELEFOR), 2008; 199–202.

[6] Vandana V. Gawit1, Namrata D. Ghuse2 "Wireless Broadband Network, WiMAX Security and Applications" published in IJCSMC, Vol. 4, Issue. 3, March 2015, pg.641 – 646.

[7] M. Chakraborty, D. Bhattacharyya, Overview of end-to-end wimax network architecture, WiMAX SECURITY AND QUALITY OF SERVICE (2010).

[8] V. K. Jatav, M. Tripathi, M. S. Gaur, & V. Laxmi, (2012, February). Wireless Sensor Networks: Attack Models and Detection. In 2012 IACSIT Hong Kong Conferences, IPCSIT vol. 30 (2012)©(2012) IACSIT Press, Singapore.

[9] A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka, Security vulnerabilities and solutions in mobile wimax, Int. Journal of Computer Science and Network Security (IJCSNS), 2007, pp. 7–15.

[10] W. C. Taeshik Shon, "An analysis of mobile wimax security: Vulnerabilities and solutions," in Lecture notes in computer science, Springer, 2007.

[11] Mahmoud Nasreldin, Heba Aslan Magdy, El-Hennawy Adel, El-Hennawy "WiMax Security" published in 22nd International Conference on Advanced Information Networking and Applications IEEE-2008.