Evolution of Wimax Technology, Security Issues and Available Solutions

Rajesh Yadav
Research Scholar,
Mewar University, India

S. Srinivasan
PDM College of Engineering
Bahadurgarh, India

ABSTRACT

Over the period, Wimax has under gone series of changes in its technologies with various new versions. In every version it has faced serious security threats and various attempts have been made to plug the security holes. In this paper we discuss about various security problems in each version and how they have been handled, here we give an overview of the evolution of Wimax Technology as well as the various security issues associated with this Technology & solutions available for it.

Keywords

MAC, ASN, CSN, PKM, EAP

1. INTRODUCTION

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communication technology intended to offer 40Mbps data rates, and enhanced version capable of providing up to 1 Gbit/s for fixed stations. With WiMAX, data rates like WiFi-like data rates are easily achievable, but the problem of interference during communication process is lessened. Due to its capability of operating on both licensed and non-licensed frequencies, WiMAX is the right technology to provide a regulated environment and a very good model for wireless carriers.

2. WiMAX

2.1 IEEE 802.16 protocol architecture

The protocol architecture of IEEE 802.16 is divided into two main layers: the Medium Access Control (MAC) layer [1] and the Physical (PHY) layer. MAC layer consists of three sub-layers. The first sub-layer is the Service Specific Convergence Sub-layer (CS), it accepts the higher-layer PDUs from the higher layers as well as Classifying and mapping the MSDUs into appropriate CIDs (Connection Identifier).The second sub-layer is Common Part Sub-layer (CPS), which is the main part of the protocol architecture is responsible for allocation of bandwidth, establishment of connection as well as maintenance of the connection between the two sides. The last sub-layer of MAC layer is the Security Sub-layer which deals with issues like authentication addressing, establishment and exchange of key, encryption encryption and integrity control. The PHY layer deals with physical transport of data itself, for which OFDM like technologies are utilized, Ranging, Power Control, DFS, Transmit & Receiving process are also being done by physical layer.

2.2 Intention of the paper

WiMAX is the much-awaited broadband wireless technology for providing high-speed connectivity over long distances [6], making it suitable for service providers. Security support is compulsory for communication networks and for wireless systems, security is even more important to protect the users as well as the network. Because wireless medium is in reach of all, the attackers can easily access the network and the network becomes more defenseless for the user as well as service provider. This paper throws a light on the security issues in Wimax and discusses their solutions.

3. WiMAX EVOLUTION

WiMAX can be explained as: “a telecommunications technology to provide data transfer wirelessly over long distances in a different ways, from point-to-point link access to mobile type [2]. It is based on IEEE 802.16 standard [3]. There are different protocols standards for WiMAX, starting from 802.16a to 802.16m, detailed information of all these standards can be found at the official IEEE website. The most relevant for this paper are 802.16d (officially called 802.16-2004) i.e. fixed Wimax and 802.16e (802.16e-2005) i.e. Mobile Wimax. Mobility was added as an amendment to 802.16-2004 in 2005 and officially published in 2006[2].

3.1 Wimax Standards & amendments

Table 1. Wimax Standards

Version	Features
802.16 (Oct 2002)	Speed : 70 Mbps.
	Coverage :30 miles
	Configuration:LOS only, Frequency 11 and 60 GHz using OFDM
	Protocol: ATM,ETHETHERNET,802.1Q,IP
	Security issues: Data Privacy (vulnerable to Bruce force attack), failed to explicitly define the authorization, Key Management.
	Solution: Now withdrawn. This is the basic 802.16 standard that was released in 2001
802.16a (Oct 9, 2003)	Speed :75 Mbit / s
	Coverage: Upto 30 miles.
	Configuration:NON-LOS,Licensed Frequency 2 GHz to 11 GHz
	Protocol: Automatic Retransmission request (ARQ), Security and encryption (Triple DES), 802.16a uses TDM (for downlink) and dynamic TDMA-based (for uplink) MAC with on-demand bandwidth allocation, which makes more efficient use of bandwidth.
	Security issues: Key Management, Privacy
	Solution: Now withdrawn. This amendment addressed certain spectrum issues and enabled the standard to be used at frequencies below the 11 GHz minimum of the original standard.

802.16d (802.16-2004)	Speed: 75 Mbps
	Coverage : 10 km
	Configuration: 2 GHz to 66 GHz
	Protocol: 3DES for AK,DES for TEK
	Security issues: Key Management, Privacy
	Solution:3DES,
802.16e (802.16-2005)	Speed: 30 Mbps
	Coverage : 1-3 miles
	Configuration: NON LOS,< 6GHZ
	Protocol: AES-CCM, PKMv2,EAP (optional)
	Security issues: DoS (Denial of Service) /Replay attack, Authorization vulnerability, Key space vulnerability, Downgrade attack, Authorization attack
	Solution: IEEE 802.16e standard has changed several security mechanisms, It will use AES (Advanced Encryption Standard) as a main encryption method and introduce a flexible authentication method based on theExtensible Authentication Protocol i.e., EAP TLS,EAP TTLS, PEAP, EAP SIM,which extends the authentication to AAA server. AESCCM mode is a new data link cipher for data authenticity mechanism[4].
802.16m (May,2010)	Speed: 100 Mbps for mobile stations, 1 Gbps for fixed
	Coverage : 3 km, 5-30 km and 30-100 km[18].
	Configuration: It will allow cellular, macro and micro cell coverage, with currently there are no restrictions on the RF bandwidth although it is expected to be 20 MHz or more[18].
	Protocol:EKMP, HARQ
	Security issues: Authentication & Authorization.
	Solution:Use of AES, AES CCM

3.2.Wimax Architecture

The WiMAX Forum's Network Working Group (NWG) has created a network reference model[7] to function as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

This model visualizes a mixed network architecture for fixed and mobile deployments and is based on an IP service model.

Written below is about an IP-based WiMAX network architecture, where the overall network may be distributed into different parts[7]:

1. Mobile Stations (MS) used by the end user to access the network.
2. The access service network (ASN), which consists of one or more [16] stations and ASN gateways to create the radio access network at the edge.
3. Connectivity service network (CSN) to offer IP connectivity and all the IP main network functions.Fig. 1 illustrates the Wimax network architecture with its entities.

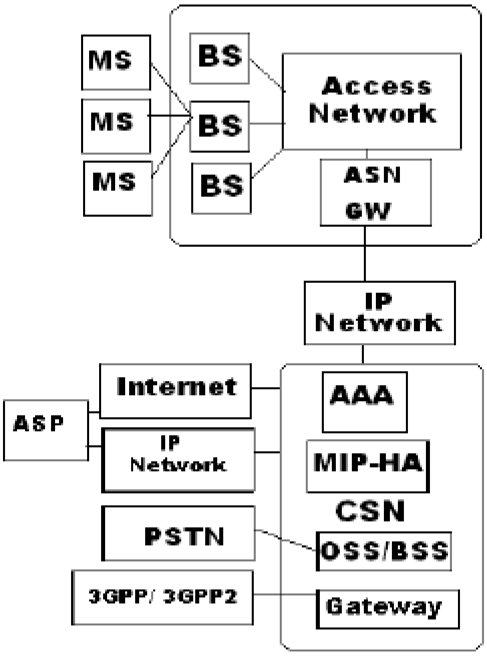

Fig.1 IP-Based Wimax Network Architecture

3.2.1 Base station (BS):

A base station is a radio receiver/transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. The Mobile station gets air interface[7] through Base station. Base Station also performs functions like mobility management, handoff triggering, tunnel establishment, radio resource management etc.

3.2.2 Mobile Station (MS or subscriber station,SS):

It is a "Generalized mobile[4] equipment set providing wireless connectivity between one or more hosts and the WiMAX network." from [5].

3.2.3 Access service network gateway (ASN-GW):

It The ASN[7] gateway typically acts as a layer 2 traffic aggregation point. It offers a logical boundary for functional of nearby clients. ASN also performs intra-ASN location management, caching of subscriber profiles and encryption keys, establishment and management of mobility tunnel with base stations[16],as well as routing to the selected *CSN.*

3.2.4 Connectivity service network (CSN):

It provides connectivity to the Internet, other public networks, and corporate networks[7].CSN is owned by the Network service provide r & includes authentication & accounting server to add authentication process for devices & users. Address management of IP , roaming between different NSPs, as well as location management between ASNs also comes under its responsibility[3].It involves routers, servers, user databases and gateway devices thereby providing internet services, roaming functionality, peer-to-peer services[2].The WiMAX architecture framework allows for the decomposition of entities like ASN may be decomposed into base station transceivers (BST), base station controllers (BSC)[16], an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).[7]

3.3. Relationship to 4G

Fourth generation mobile technology has been developed to provide mobile ultra-broadband Internet access. Standards such as WiMAX 2 & LTE works as actual technology behind LTE.When actually working under LTE, one of the main features of 4G standard as specified by International Telecommunications Union (ITU), is the condition for all IP packet switched networks i.e. No difference is being made between voice and data packets as well as voice and data traffic, which will have serious effects cost of mobile services.When considering the evolution of mobile technologies, it is very crucial to note that each generation, as well as each standard, is an improvement on earlier generations or standards[8].Moreover due to different types of standards available and also being used by mobile operators, it can be challenging to go through their working effect on user experience of mobile services.When talking about WiMAX or WiMAX 2 & LTE, it should be kept in mind that maximum data speeds can vary depending on speed of user’s mobility. Let us take an example of WiMAX 2 & LTE , if user is in a high-speed mobility like in a moving vehicle or in a train, maximum possible data speed is around 100 Mbps (download) and 50 Mbps (upload), whereas , if user is fixed(stationary) or even walking, download and upload speeds of up to 1 Gbps and 500 Mbps, respectively, can be achieved.[8]

3.4. Wimax success factors

Motivation for deploying WiMAX has come through by seeing growing demand for broadband connectivity, specifically in areas inadequately served by existing broadband networks[9]. Service operators of Wimax have identified a Big opportunity in their respective markets & chosen a competitive broadband technology that is available today i.e. the fastest one & one that is less expensive also.
Other factors driving operators to deploy WiMAX are:

3.4.1 Speed to market:

Wireless network connectivity can be offered in a very short time as compared to fixed networks. While deploying the network, it is not required for operator does to acquire rights of way, which could take significant amounts of time. Also when we talk about those growing markets which lack good planning of cities, in that case wireless networks may be the best way to provide connectivity [9].

3.4.2 Network deployment opportunities:

Through WiMAX network, operators can design their networks as they want to design. Therefore through this approach, operators have been able to focus on those areas where there is strong demand, which helps them to generate a higher return on investment and to grow their business of subscribers[9].

3.4.3 Mobility and multiple-use scenarios:

The key reason of differentiating Wimax from DSL is the mobility feature of Wimax through IEEE 802.16e,Through three modes of Wimax network i.e. ixed, portable and mobile, the operators can provide different applications thereby expanding their business possibilities provided that price of these services is affordable.

3.4.3.1 IP architecture:

Due to IP-based technology of Wimax, new services can be added in less time which leads to generating more revenue for service providers and since IP core is, therefore if required different technologies can be deployed in the last mile[9].

3.4.3.2 Cost of spectrum: If we compare the spectrum cost of Wimax, it is less in comparison with 3G.

4. WIMAX SECURITY ISSUES

WiMAX is considered a very good wireless access mechanism when dealing with long distance high spedd connectivity, which makes it suitable for Internet service providers [3].

Designed Promoted by standard of IEEE 802.16 committee, WiMAX was developed after the security failures were analyzed fromIEEE 802.11 networks[17].
When security ws recognized as a ery impornt factor, the 802.16 group developed mechanisms to protect service provider from theft of service, and to protect customer from unauthorized uncovering of their information[6].

4.1. Authentication

The 802.16 networks works with a key principle which is that each subscriber station (SS) must have a X.509 certificate that will uniquely identify each subscribersin the network. Implementing X.509 certificates makes it challenging for an attacker to spoof the identity of subscribers,giving generous protection against theft of service[6]. A key breach in the authentication mechanism used by WiMAX's privacy and key management (PKM) protocol is the missing concept of base station (BS) or service provider authentication. This sometimes leads to man-in-the-middle attacks, subjecting subscribers to various confidentiality and availability attacks. Amendment to IEEE 8012.1e lead to supporting Extensible Authentication Protocol (EAP) in WiMAX networks.

4.2. Encryption

Also the amendment of 802.16e provided support for the Advanced Encryption Standard cipher leading to confidentiality of data traffic. Like Wireless Lan standard management frames are not encrypted which gives support to an attacker to collect information about subscribers in the arearange as well as other and other crucial characteristics of network[6].

4.3. Availability

Deployment of Wimax will make use of licensed radio freqency spectrum which will enable come giving them some protection from unintentional interference.By making use of avaialable tools, it is although not difficult for and attacker to jam the spectrum for all planned WiMAX deployments.Moreover in addition to physical layer denial of service attacks, an attacker can use legacy management frames to forcibly disconnect legitimate stations. This is just like deauthenticate flood attacks applied against Wireless Lan networks[6].

4.4. Wimax threats

WiMAX security is implemented in the security sub-layer in protocol architecture which is above the PHY layer[1], so the Physical layer is an unsecure layer[9] and it is not capable to work against attacks which target inherent vulnerability of wireless links such as jamming, scrambling or water torture attack. WiMAX supports mobility, this feature is regarded as best one but it also makes the networ more vulnerable to attacks because the attackers do not need to be at fixed location which make network monitoring process more difficult[1].

4.4.1 Jamming attack

Jamming is an attack done by introducing a Some noise which is capable to to reduce the capacity of the channel[9]. Performing a jamming attack is not difficult because any concerned information as well as reqired devices are easy to acquire and even enough material is available in a book by Poisel [10] which teaches jamming techniques.

Solutions: We can prevent jamming attack by increasing[9] power of signals or by increasing the signal bandwidth using techniques such as frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS).

Moreover law enforcement agencies can also help in this regard, in addition to that radio spectrum monitoring equipment to detect jamming as well as radio direction finding tools to identify sources of jamming are very helpful for the same.

4.4.2 Scrambling attack

Scrambling is that type of jamming which happens for short intervals of time and targeted[9] to specific WiMAX frames at PHY layer. It is upto the attacker to selectively scramble control or management information which affects the functionality of network in normal mode. Scrambling attack is not s easy to perfome like jamming attack because in this case attacker requires to interpret control information and to send noise during specific intervals [9].

Solutions: We can use anomalies monitoring beyond performance norm (or criteria) to detect scrambling and scramblers[9].

4.4.3. Water torture attack

It is a type of attack in which an attacker forces[11] a sbsciber station to drain its battery or consume computing resources by sending a series of fake frames. This kind of attack is considered taken as more dangerous than Denial-of-Service (DoS) attackbecause the subsciber station is a portable device and it carries limited resources.

Solution: In order to get rid of this type of attack, such type of mechanism is required which can discard fake frames, thereby avoiding running out of battery or computational resources.

4.4.4. Other threats

IEEE 802.16 is also vulnerable to different types of attacks like forgery attack in which an attacker with a sufficient radio transmitter can write to a wireless channel [11] .When we consider mesh mode in network, the 802.16 can be affected by replay attacks in which an attacker sends valid frames multiple times, which he has intercepted in the middle process of forwarding (relaying).

Solutions:

When dealing with the above type of security flaw, concept of mutual authentication [13] comes into picture to deal with such types of attacks.

5. AUTHENTICATION AND AUTHORIZATION SOLUTION IN WIMAX

Wimax Security scheme deals with main issues of authentication and confidentiality.IEEE 802.16 security features have very good impact due to their design approach [12] and security options are prioritized from beginning by Wimax standard bodies.Wimax authentication and authorization techniques are used to prevent spying of the user ID, denial of service (DoS), offline dictionary attack, man-in-the-middle attack, authentication method down-grading attacks etc[12]. In this regard the authentication protocol has to ensure collecting information about the user before protocol selection as well as to ensure that both sides are equally authenticated(mutual authentication).

Extensible Authentication protocol was introduced to offer authentication scheme to fo for avoiding the problems related to authentication. It works by integrating various methods of authentication for matching with the nature of the communication channel. Various techniques specified by IEEE under EAP are EAP-PKM, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-SIM and EAP-AKA[12]. Wimax networks make use of use of EAP-PDM as well as EAP-TLS. EAP-Transport Layer Security is an Internet Engineering Task force open standard which is well-supported among wireless vendors. It provides good level of security because of it being considered the successor of the Secure Socket Layer standard. It uses PKI for securing communication to the RADIUS authentication server. The strength of EAP-TLS in terms of authentication is its requirement for client side certificate[14] thereby illustrating classic convenience versus security[15] trade-off. In case of EAP transport layer security mechanism even if the password by some means is known to the hacker, still he will not be able to break into the system because client side certificate is required. Through the concept of incorporating these certificates into smart cards, authentication becomes more secure because without having the smart card in possession, it is not possible to recover any user’s private key. Moreover any theft of the same will be noticed immediately to get a new one[12]. On the other side EAP-PKM has both types of authentication mechanism i.e. one way as well as mutual authentication.PKM-EAP of WiMAX offers more secure & robust way, the following enhancements have been addressed [12]:

1. To avoid Man in the middle attacks, PKM2 offers Mutual authentication.
2. Each Subsciber station is assigned unique X.509 certificate which can’t be easily forged.
3. There is a different SAID assigned to each service, therefore if one is service is compromised, it will not affect the other ones.
4. Authentication key has a limited lifetime which provides periodic reauthorization and key refresh, thereby avoiding the attackers to have large amount of data to perform cryptanalysis.
5. In order to prevent replay attacks, one of the mechanisms is to add a random value from the Base station and Subscriber station to authorize SA.
6. DES 3 & AES are two encryption standards which are considerd secure when we talk about Wimax security [15].
7. Subscriber station can attempt to use a handover-transferred Master Key for avoiding full re-authentication.
8. Every base station in WiMAX is equipped with a dedicated security processor, thereby helping in implementing mutual authentication system in Wimax. Or we can say that designing of an authentication protocol can be done in a way in which most of the computational procedures are done inside base station [12].

When looking at the security architecture [15] of Wimax, some know an issue comes into picture.

Some ways are defined for securing wireless communication at MAC layer, but it has not focused on the threats from any attacks targeting the physical layer, like radio jamming, or continuously sending packets.

Continous sending of packets may lead lead to overwhelmed receiver, and eventually cause Denial of Service (DoS) or fast battery consumption.

Even after seeing these shortcomings, both the mechanisms of authentication and authorization applied in WiMAX are still best suitable for it[12].

6. CONCLUSION

This research paper started by explaining what Wimax is and we also discussed Various Wimax standards, their security issues and specified the solutions. We also analyzed various threats to wimax security and discussed available solutions for authentication & authorization in Wimax. From this analysis, we are able to consider different issues pertaining to security aspect of Wimax technology. When discussing the security of such technologies, there are several possible perspectives. Different authentication, access control and encryption technologies all fall under the umbrella of security. As future technology of broadband is wireless communication, in that WIMAX will play a major role after clearing all its security problems.

7. REFERENCES

[1] A survey of WiMAX security threats, Trung Nguyen, nguyent@seas.wustl.edu.

[2] Security issues and proposed solutions concerning authentication and authorization for WiMAX(IEEE 802.16e) Bart Sikkens, University of Twente, the Netherlands sikkensb@cs.utwente.nl

[3] Wikipedia,WIMAX,http://en.wikipedia.org/wiki/WiMAX, accessed: 11-12-07.

[4] Introduction to mobile WiMAX Radio Access Technology: PHY and MAC Architecture, Dr. Sassan Ahmadi, Wireless Standards and Technology, Intel Corporation, Dec 7, 2006.

[5] Prakash Iyer, Nat Natarajan, MuthaiahVenkatachalam, Anand Bedekar, Eren Gonen,Kamran Etemad, Pouya Taaghol, All-IP Network Architecture for Mobile WiMAXTM, IEEE MobileWiMAX Symposium, Mar 2007, pp. 54 – 59

[6] WiMAX security issues Wireless Security By Joshua Wright, NetworkWorld.com Dec 11, 2006.

[7] http://www.tutorialspoint.com/wimax/wimax_network_model.htm

[8] http://www.ict-pulse.com/2011/07/edge-wimax-3g-4g-what is-the-difference

[9] Michel Barbeau, "WiMax/802.16 Threat Analysis", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Quebec,Canada,2005.

[10] R. Poisel, "Modern Communications Jamming Principles and Techinques", Artech House Publishers, 2003.

[11] David Johnson and Jesse Walker, "Overview of IEEE 802.16 Security", Intel Corp, IEEE Security and Privacy, 2004
http://portal.acm.org/citation.cfm?id=1009288

[12] http://rswcyyw.blogspot.in/2007/06/authentication-authorization-and.html

[13] Huixia Jin1 Li Tu2 Gelan Yang2 Yatao Yang3,” An Improved Mutual Authentication Scheme in Multi-Hop WiMax Network”, 2008 International Conference on Computer and Electrical Engineering IEEE 2008 .

[14] Ergang Liu, Kaizhi Huang and Liang Jin,” The Design of Trusted Access Scheme Based On Identity For WiMAX Network” First International Workshop on Education Technology and Computer Science IEEE 2009.

[15] Cătălin-Teodor Dogaru,” WiMAX Network Security Plan”, 8th International Conference on Communication IEEE 2010.

[16] Deepti, Deepika Khokhar, Satinder Pal Ahuja, A Survey of rogue base station attacks in Wimax. Vol. 2 Issue 1, International journal of advance research in computer science and software engineering, January 2012.

[17] Responding to Security Issues in WiMAX Networks,Chin-Tser Huang, University of South Carolina, J. Morris Chang, Iowa State University. IT Pro September/October 2008 Published by the IEEE Computer Society.

[18] A Survey of Mobile WiMAX IEEE 802.16m Standard, Mr. Jha Rakesh, Mr. Wankhede Vishal A.,Prof. Dr. Upena Dalal, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 1, April 2010.