



WIMAX: An Overview, Security Issues and Security Threats

¹Er. Ujwal Parmar, ²Er. Sharanjit Singh

¹Research Scholar, ²Assistant Professor,
Computer Science & Engineering,

Guru Nanak Dev University, Regional Campus, Gurdaspur, Punjab (INDIA)

Abstract: WIMAX stands for Worldwide Interoperability for Microwave Access which is also known as IEEE 802.16 wireless metropolitan area network. It basically an alternative to wired technologies such as cable modems, DSL (Digital Subscriber Line), T1/E1 lines and provides broadband access over long distances. [10] It has many advantages like high data rates, Quality of service, scalability, security, mobility. In this paper, I have discussed about the most concerned issue of security in broadband wireless network access i.e. WIMAX. The security in WIMAX is involved with certain vulnerabilities, threats and risks or attacks. The various threats have been occurred at the Physical and MAC layer. The WIMAX communication protocols involve certain security mechanisms which are also discussed in this paper which helps to reduce some attacks.

Keywords: WIMAX, IEEE, WIMAX Network System Architecture, WIMAX Security Mechanism, Security Threats

I. INTRODUCTION

In today's life, broadband services and applications has become the necessary for internet users for the continuous connection with high bandwidth while accessing different mobile and roaming devices. The IEEE 802 committee has set some networking standards such as Ethernet (802.3) and Wifi (802.11) and some other set of standards which defines WIMAX. There are two main types standards i.e. IEEE 802.16d which supports the fixed bandwidth access in which the end devices is not able to move between base stations (BS) but can enter into network at different locations IEEE 802.16e is the revised version which supports mobility (both the fixed and mobile broadband wireless access system) which allows Mobile stations to move between different base stations while communicating. WIMAX is used in many numbers of applications such as "the last kilometer" broadband connections, hotspots and high-speed connection as used in business purposes. WIMAX is- "A telecommunication technology that provides wireless transmission of data using a variety of transmission modes i.e. point-to-multipoint links to portable and fully mobile internet access".

Based on the IEEE 802.16 standard, WIMAX is called IEEE Wireless MAN due to its Broadband Wireless Access Metropolitan Area Network (BWA-MAN) technology. It is the new interface standard with different frequency ranges-2.5 GHz, 3.5 GHz and 5.8 GHz which also provides scalability, high data rates and strong QoS (quality of service) guaranteed for data, voice, video etc. WIMAX has the distance range up to 30 miles and speed of 70 Mbps.

	802.16	802.16a	802.16e
Spectrum	10-66 GHz	2-11 GHz	2-6 GHz
Channel bandwidth	20, 25, and 28 MHz	1.5 to 20 MHz	1.5 to 20 MHz with UL sub channels
Modulation	QPSK, 16QAM, 64 QAM	OFDM 256 sub carriers QPSK, 16QAM, 64 QAM	OFDM 256 sub carriers QPSK, 16QAM, 64 QAM
Bit rate	32-134 Mbps (28 MHz)	75 Mbps (20 MHz)	15 Mbps (5 MHz)
Channel conditions	LOS	Non-LOS	Non-LOS
Typical cell radius	2-5 Km	7-10 Km, max 50 Km	2-5 Km
Application	Fixed	Fixed and portable	Mobility

Table 1: IEEE 802.16 standards[3].

II. WIMAX (IEEE 802.16) PROTOCOL STRUCTURE: MAC and PHY layer

Before concerning about the security issues of WIMAX, we need to have knowledge about the WIMAX protocol architecture which provides the detailed information about the various specifications for securities in the sub-layer [1].

The IEEE802.16 protocol architecture consists of two main layers: The MAC(Medium Access Control) layer and The PHY (Physical) layer. [2][1]The MAC layer further consists of three sub-layers: First, Service Specific Convergence Sub-layer(CPS) is the first sub-layer in the protocol structure which provides high level data services, data flow and connections. Second, Common part Sub-layer which provides rules and mechanism for connection management and bandwidth allocation. Third, Security Sub-layer which lies between the CPS layer and the PHY layer which addresses the security specifications such as the authentication, key establishment and exchange , encryption ,and decryption of data between the MAC and the PHY layer. The PHY(physical) layer provides the mapping between the MAC protocol data units and the data frames of the PHY layer which is received and transmitted with the coding and modulation done on the radio frequency signals.

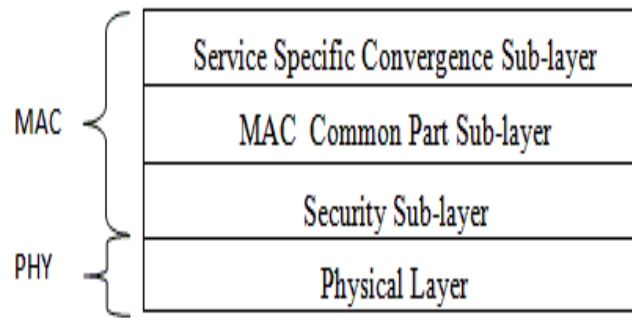


Figure 2: The IEEE 802.16 protocol structure [2]

III. WIMAX NETWORK SYSTEM ARCHITECTURE

The Wimax Network System is based on IP Service model. The WIMAX network system is of three parts:

A. Connectivity Service network

- IP (Internet Protocol) connection to WIMAX users.
- It provides all core network functions: user authentication, network administration, tunneling between CSNs for roaming service, provides interface to other networks.
- It provides the IP address management, Qos (quality of service) and security [11].

B. Access Service network

- Wireless access to WIMAX users
- It includes one or more base stations and ASN gateways which provides the radio access network. Base Station is connected with the Mobile stations (MS) provides the flexible arrangements between and configuration of sub-channels, upgrades and expands the network based on the requirement of the users. The base station functions the tunnel establishment, Qos service policy establishment, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management and session management [11].
- Transfers AAA (Authentication, Authorization and Accounting) messages to WIMAX subscribers.

C. Mobile station

- used by end users to access the network

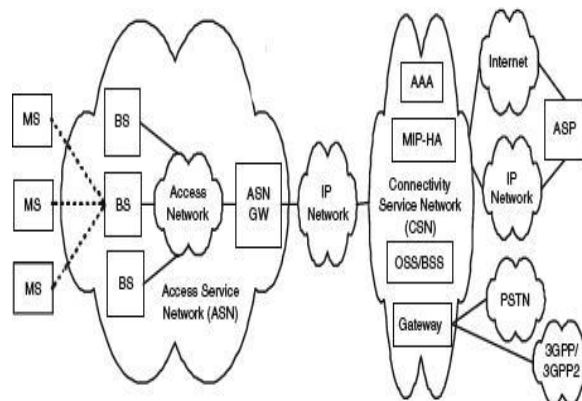


Figure 3: IP-Based WIMAX Network Architecture.

IV. WIMAX SECURITY MECHANISMS

For WIMAX security, there are different mechanisms that are deployed over the transmission channel through WIMAX communication protocol.

A. DATA SA (SECURITY ASSOCIATION)

Data Security Association has a 16 bit SA identifier. During the transmission of data over the channel, DES in CBC (cipher) mode helps to protect the data and there are two Traffic Encryption Keys (TEKS) i.e. Current operational key and TEK which are used for data encryption. There are three types of Data SA: Primary SA, Static SA, and Dynamic SA. The primary SA is shared between MS and BS and is used for link initialization. Static SA is shared among different MS (Mobile Station). Dynamic SAs are used for transport connections.

B. AUTHORIZATION SA (Authentication)

Authorization state is shared between the BS (Base Station) and SS (Subscriber Station). It has 60 bit Authorization Key (AK) and 4 bit quantity to identify AK. It uses X.509 certificate for RSA Encryption. 3DES (112 bit) key used in Key Encryption key for distributing TEK (Temporal Encryption Key). It uses HMAC (Hash function-based message authentication code) which is used to provide authenticity to key distribution messages from BS to SS and SS to BS respectively. AK provides the authorization token which is encrypted by the public key of RSA cryptography. Authentication is completed when both BS and SS possess Authorization Key (AK) [4].

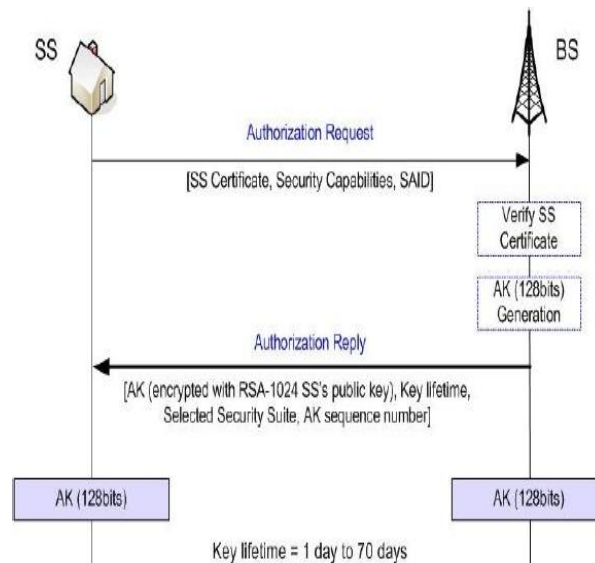


Figure: IEEE 802.16 Authentications.

C. DATA KEY EXCHANGE

Transport Encryption Key is used for data encryption. In authentication process, it uses AK to derive Key Encryption key and HMAC key.

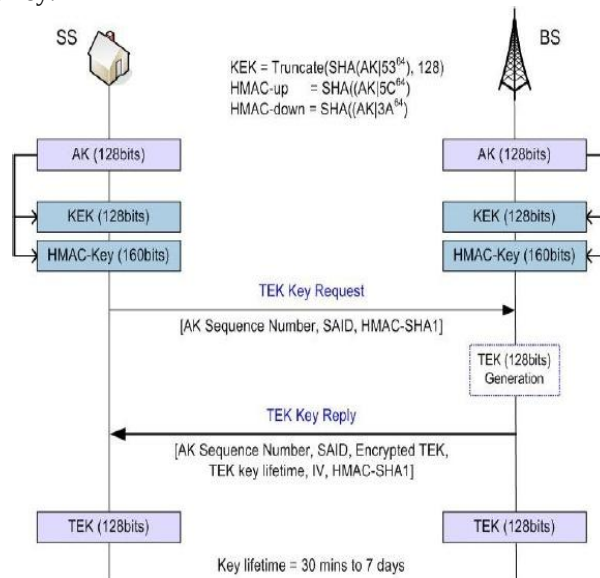


Figure: 4 IEEE 802.16 Data Exchange Key[5]

TEK is encrypted with 3DES (112bits), RSA and AES (128 bits) and is generated by BS. Key Exchange message is authenticated by HMACSHA1 which provides Message Integrity [5].

V. SECURITY THREATS AND VULNERABILITIES

A. ROGUE BASE STATION

Rogue base station acts as an attacker which duplicates the original or legitimate base station. It steals the original access point identity and confuse the subscribers or users that whether they are getting service from the legitimate one or fake. It creates long term disturbance of service. In WIMAX network, it uses the Time Division Multiple Access. The attacker steals the legitimate identity of the base station and starts creating fake messages. The attacker can send those messages only at the time when the time slots is provided for transmit of messages. This threat can be mitigate with no such technical issues i.e. through EAP (Extensible Authentication Protocol) which provides Mutual Authentication. The BS and the subscriber should be mutually authenticated to each other before transmission of messages.

B. MAN IN THE MIDDLE ATTACK

The attacker performs eavesdropping. The attacker used to interfere between the conversation of the sender and receiver and replays the messages [6]. The intruder intercepts and sends its own public key to the victim and to which the victim does not get to know that the person to whom he is talking to is not a legitimate user and the victim sends the public key to the hacker. Thus, to mitigate this attack the security mechanism is provided with Three-Way handshake Scheme that supports re-authentication mechanism [7].

C. DOS (DENIAL OF SERVICE) ATTACK

In DOS attack the attacker used to attack on the first connection which is established between the BS and MS in the Initial Ranging Process. In initial network entity, the request and response messages have been sent between the MS (Mobile station) and the BS(base station) to join the network. MS used to send the RNG-REQ message to the BS and BS used to respond with RNG-RSP message to the MS which contains the CID (Connection Identifier) which is not encrypted and is vulnerable to attack. The attacker used to modify it with the status failed. The MS again try for the ranging process. But the attacker continues to intercept response between the MS and BS. Thus, the MS does not allow to join the connection and triggers initial ranging process again and again which leads to the DOS attack [8].

D. THREATS TO THE PHYSICAL ATTACK

The Physical layer of the IEEE 802.16 is most vulnerable to attack and it is insecure as it is not protected from various attacks. The various attacks on the PHY layer are:

D.1 Jamming Attack

It is similar to the DOS attack which adds noise to the responded message of the BS. It can be done intentional or unintentional. It is detected by radio analyzer detector which only indicates that steps should be taken to recover the threat [6].

D.2 Scrambling Attack

Scramble attack is for short period of time, it is targeted only some slots of data frames. The attacker used to scramble the uplink slots of MS and make it unreadable for BS. This attack is difficult for the attacker to perform [9][6].

CONCLUSION

In this paper we have studied that, in the Global internet, WIMAX is now become the future network that provides the high speed with low cost. It provides the wireless network with better services to Mobile devices. WIMAX has many more advantages while accessing an Internet. Due to such reasons, Security of the WIMAX is most important. Thus, this paper have main focused on the security issues on WIMAX. The various threats are discussed, so that precautions or certain measures should be taken to these possible attacks. Even though the WIMAX has such Security solutions or Security mechanisms but still some issues are unsolved. So, WIMAX needs a further research to resolve these security issues.

REFERENCES

- [1]. http://www.asee.org/activities/organizations/zones/proceedings/zone1/2008/Professional/ASEE12008_0022_paper.pdf
- [2]. <http://www.cse.wustl.edu/~jain/cse574-08/>
- [3]. IEEE 802.16: Broadband Wireless MANs [online]. Available: <http://standards.ieee.org/about/get/802/802.16.html>
- [4]. Johnston, D., Walker, J. (2004). Overview of IEEE802.16 Security. URL:http://mia.ece.uic.edu/~papers/WWW/Bubbles/segment/WiMax_Security.pdf. [5]Wongthavarawat, K. (2005). IEEE 802.16 WiMax Security. URL:http://www.nectec.or.th/nac2005/documents/20050328_SecurityTechnology-05_Presentation.pdf.
- [6]. N. Beacham, "Man in the Middle (MITM) Attacks," Technology and More, 28 June 2008.
- [7]. J. M. Hartley, "WiFi and WiMax Protocols of Security," December 2008. <http://softwarecommunity.intel.com/articles/eng/3708.htm>.
- [8]. A.K.M. NazmusSakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, "IEEE 802.16e Security Vulnerability: Analysis and Solution", Global Journal of Computer Science and Technology Vol. 10 Issue 13 (Ver. 1.0), October 2010.
- [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, <http://portal.acm.org/citation.cfm?id=1089761.1089764>
- [10]. http://www.tutorialspoint.com/wimax/what_is_wimax.htm
- [11]. http://www.tutorialspoint.com/wimax/wimax_network_model.htm
- [12]. M.Barbeau, "Threats: Threats to WiMax," <http://www.freewimaxinfo.com/physical-layer.html>