Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A Review on security issues in WiMAX

Ravinder Kumar[1], Veepin Kumar[2]
[1]M. Tech. Scholar, [2]Asstt. Professor
[1,2]*Department of Computer Science & Engineering.*
[1.2]*Om Institute of Technology and Management, Hisar.*

Abstract **–** The IEEE 802.16 standard, commonly known as WiMAX, is the latest technology that has promised to offer broadband wireless access over long distance. Since 2001, WiMAX has evolved from 802.16 to 802.16d standard for fixed wireless access and to the new IEEE 802.16e standard with mobility support. With the growing popularity of WiMAX the security risks have increased many folds. In this paper we will give an overview of security architecture of WiMAX. We propose some possible security improvements and solutions to eliminate the vulnerabilities. Finally, we will have a look at improvement reported in multi hop WiMAX networks.

Keywords **–** WiMAX, IEEE 802.16, security, encryption, security concerns, authentication

I. INTRODUCTION

The IEEE 802.16 or WiMAX is an excellent successor to WiFi/IEEE 802.11. As WiMAX grows, the security concerns over it also increase. We define security as protection of data being transmitted over a wireless networks. It is important to understand the full range of problems that security systems need to address. These needs are confidentiality, integrity and authentication (CIA), and are defined as follows:

A. *Confidentiality* – Allowing only that the intended legitimate recipients to read encrypted messages.

B. *Integrity* – is referred to as ensuring that another party has not altered messages after it has been sent.

C. *Authentication* – This is making sure that parties sending messages or receiving messages are who they say they are.

As WiMAX transitioned from Line of Sight (LOC) and Point to Multi Point (PMP) higher frequency (10-66 GHz) to lower frequencies (2-11 GHz) and NLOS mobile systems the security issues increased tremendously. Also, WiMAX uses radio channels which are open channels and hence pose a very serious security problem for traffic confidentiality and integrity. For transmission, WiMAX uses air as medium which exposes the PHY and MAX layers [1].

Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), Intrusion Detection Systems (IDS) and firewalls are just examples among various security mechanisms that have been proposed to address security issues in wired networks.

As already mentioned above, WiMAX uses radio and anyone with a properly positioned and configured receiver can intercept messages, and if he has a properly configured transmitter, i.e. he poses as a legitimate base station (BS) while actually being a rouge base station [2], he can write on the wireless channel, capture frames, make new ones, modify existing frames from the users.

II. WiMAX SECURITY ARCHITECTURE

A. *Data Link layer security* – The IEEE 802.16 standard consists of well defined interfaces in the protocol stack. The protocol contains MAC layer along with PHY layer. MAC layer includes three sub layers as shown in the figure 1.

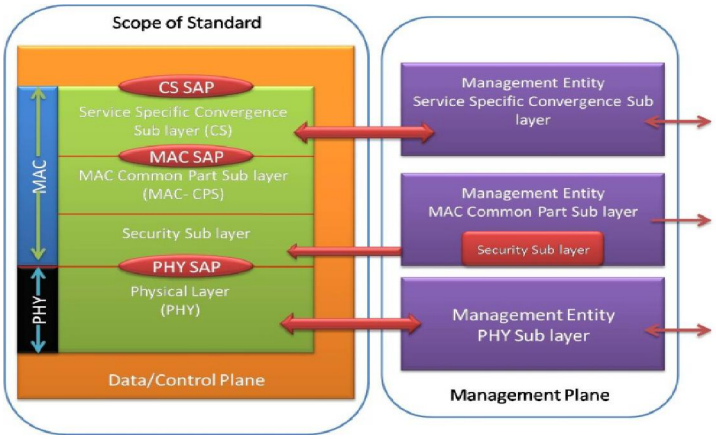

Figure 1: 802.16 Protocol Layering

The figure shows the three sub layers.

1) *Service Specific Convergence Sub Layer* (CS) – This is used for mapping higher level data services to MAC layer service.

2) *MAC Common Part Sub Layer* (MAC-CPS) – MAC CPS defines:
   - The rules and mechanisms for system access, bandwidth allocation, grant connection control etc.
   - Functions like uplink scheduling, bandwidth request etc.
   - The communication between the MAC CPS and CS is handled by MAC SAP

3) *Security Sub layer* – The Security Sub Layer lies between MAC CPS and PHY. This layer is responsible for the encryption and decryption of data travelling to and from the PHY layer. This layer is used for authentication and secure key exchange [3].

B. *Protocol Layer Security scheme* – The IEEE 802.16e standard has better security features than the IEEE 802.16d. Most of the concerns raised with the 802.16d have been addressed in 802.16e. Security sub-layer is shown below in figure 2.

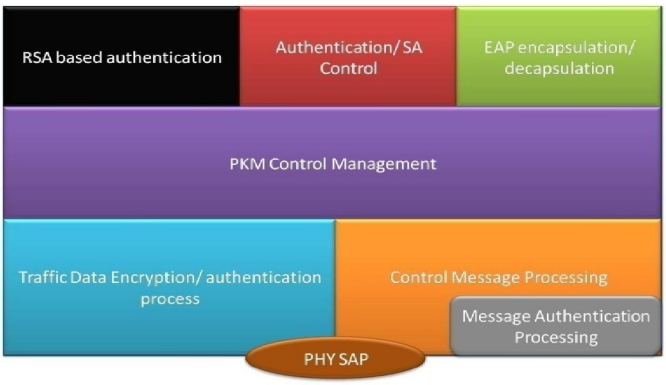

Figure 2: WiMAX security sub layer

This sub layer performs three functions

1) *Authentication* – The following authentication protocols are supported by WiMAX"

RSA Authentication based on X.509 Certificates. The basic use of the X.509 certificates is the determination of the identity of the base station (BS) by the subscriber station (SS). The certificate consists of eleven elements [5].

There are two types of certificates:

- *Manufacturer* is used to identify the third party.

The subscriber station certificate is used by the BS to determine whether the SS is a legitimate one or not.
While granting the AK, the BS verifies the certificate and uses the verified Public Key to encrypt an AK and send it to the SS. The process of RSA authentication is shown in figure 3. The message is encrypted using the public key and the formula at the subscriber station. The cipher text so obtained is then transmitted to the base station where the complimentary operations are performed to obtain the plain text. It must be noted that the decryption is done with the help of the private key at the base station.

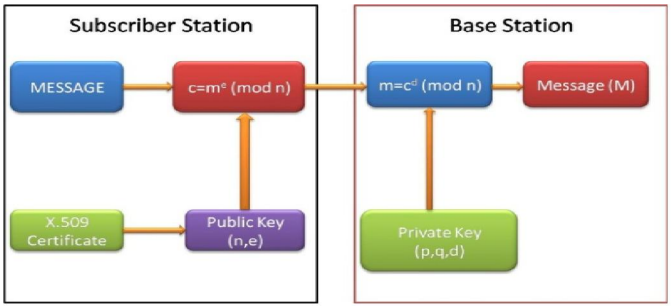

Figure 3: RAS Authentication

- *EAP (Extensible Authentication Protocol)* – is a simple encapsulation that can run over not only on PPP but on any link like the WiMAX. For the case of WiMAX the EAP runs from the Mobile Station (MS) to the BS over the PKMv2. In the case that the authenticator is not in the BS, the BS sends the protocol to the authenticator in the access service network. The EAP is carried, from the authenticator to the authentication, over RADIUS. The EAP framework is shown in figure 4.

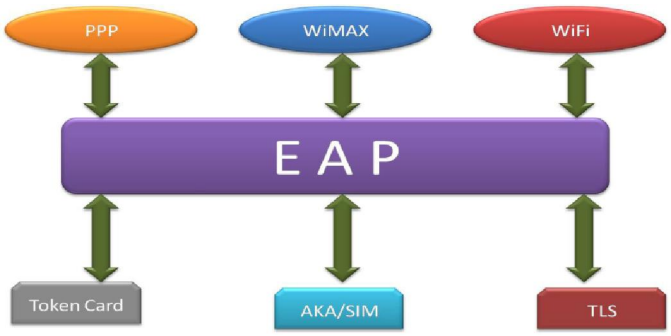

Figure 4: EAP Framework

- *HMAC (Hashed Message Authentication Code)* - The 802.16e standard added the option of using CMAC in place of HMAC. The major advantage of HMAC is that the receiver can verify the identity of the sender. This is possible because while sending the message, the sender creates a HMAC of the message using a key known to the sender and receiver alone. When the message is received, the receiver computes its own HMAC of the message with the same key and compares it with the one received from the sender. If there is a match, the identity is verified.

2) *Authorization* – This process follows the authentication process. In this the SS request an AK along with a SAID (Security Association ID). The authorization message includes the SS's X.509 certificate, encryption algorithms and cryptographic ID. After authorization the BS sends back to the SS a public key, a lifetime key and a SAID.

3) *Encryption* – A Traffic Encryption Key (TEK) is used to encrypt the data traffic [4]. The TEK encryption process is Shown in Figure 5

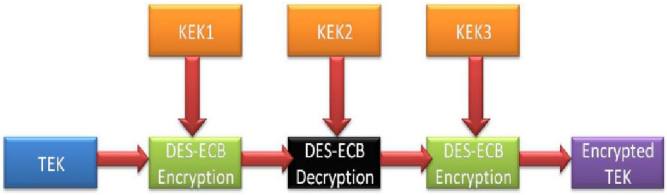

Figure 5: TEK Encryption Process

III. THREATS TO WiMAX

Many of the security threats found in WiMAX have been addressed. These are issues that were found with the deployment of WiFi. This gives WiMAX an advantage. If all, or at least most of the security issues can be addressed before WiMAX's mainstream deployment, it will make it a more accepted network than WiFi. This section of the paper will discuss the known security threats in WiMAX. These include:

- Rogue base stations -
- DoS attacks -
- Man-in-the-middle attacks -
- Network manipulation with spoofed management frames -
- Threats in the physical layer -

- *Rogue base stations* – A Rogue Base Station is defined as an attacker station that imitates a legitimate base station [6]. This kind of attack results in disruptions in service and allows hackers to confuse subscribers. WiMAX uses time division multiple access, therefore the rogue

base station must transmit with a stronger strength at the same time the legitimate station transmits. The authentication protocols used in WiMAX help mitigate this threat. WiMAX uses the EAP protocol as its main protocol for authentication.

- *DoS attacks* – Dential of Service (DoS) attacks is defined as an attempt to make a computer resource unavailable to its intended users [7]. Hackers usually use this type of attack on web servers for banks, credit card payment gateways or DNS root servers. A DoS attack uses the IP address to flood the user's network and obstruct communication between the intended user and the victim. This type of attack is not preventable; however steps can be taken to quickly resolve the attack. Some firewalls have built-in protection from DoS attacks, that monitor the amounts of packets received and the time frame they were received. It has been proposed hat a Shared Authentication Information (SAI) protocol could be sued to offer a defence mechanism against DoS attacks, without incurring overhead at the ASN gateway and base station. This proposal uses the unused upper 64-bits of the 128-bits Cipher Based Message Authentication Code (CMAC) to calculate a CMAC key [8]. This proposal could be the answer to prevention of DoS threats.

- *Man-in-the-middle attacks* – Man-in-the-Middle attacks are forms of eavesdropping. The hacker establishes separate connections between two victims and relays the messages between them [9]. The hacker intercepts the public key from one of the victims and sends his or her own public key to the intended victim. When that victim responds the hacker then has that public key. The use of the RF spectrum in WiMAX allows for vulnerabilities to the man-in-the-middle attack. However, WiMAX uses a three-way handshake scheme that supports re-authentication mechanisms for fast handovers to prevent man-in-the-middle attack [10]. If the base station is constantly changed the public key changes making it almost impossible for hackers to eavesdrop using public key.

- *Network manipulation with spoofed management frames* – The management frames in WiMAX are similar to WiFi's. When WiFi was first deployed vulnerabilities were found in the management frames that allowed DoS attacks by disrupting the wireless session between two nodes. WiMAX has cryptographic protections from spoofed identities, but that does not mean it is safe. Replay DoS attacks still remain a threat to WiMAX, due to the lack of any mechanisms to specifically detect and discard repeated packets [11].

- *Threats in the physical layer* – Blocking and rushing are the major threats located in the physical layer. Blocking or jamming activates a strong frequency to lower the capacity of the channel creating a DoS to all stations. This threat is detectable with a radio analyzer device. This device does not prevent this threat, but it alerts the end user so that steps can be taken to immediately recover. Rushing or scrambling is another type of jamming, but it only activates for short periods of time and only affects certain frames. Jamming can be prevented using an increased signal or using frequency hopping. Control or management messages are not in danger of rushing or blocking. Scrambling the uplink slots is too difficult for hackers [12].

IV. CONCLUSIONS

WiMAX security has been discussed in this paper. The precautions taken with WiMAX were not done for WiFi. IEEE 802.16 is an emerging standard for broadband wireless communications that is receiving a lot of attention from service provider and hardware producers as an alternative to wired broadband access or promising technology to offer broadband wireless access over long distance.

In this paper, we describe different security vulnerabilities found in IEEE 802.16e, such as : Unauthenticated messages which could constrict or interrupt the communication between mobile station and base station which listens to the traffic, he can collect lots of information about both instances; and lastly, shared keys in the multicast and broadcast services in Mobile WiMAX that can cause group members to forge messages or even distribute own traffic keying material, thus controlling the multicast and broadcast content.

REFERENCES

[1] LangWei-min, Zhong Jin-li, Li Jian Jun et.al., "Research on the Authentication Scheme of WiMAX" in Proc 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 12-14 October 2008, Dalian, China PR.

[2] Michel Barbeau Carleton University, Ottawa, Ontario, Canada, "WiMAX/802.16 Threat analysis", Published in: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks pp. 8 – 15, 2005

[3] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang et.al., "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", in Proc 5th IEEE International Conference on Mobile Ad Hoc and Sensor Networks, pp.828-833 2008. September 29 – October 2, 2008, Atlanta, USA.

[4] Lang Wei-min, Wu Rung-shen, Wang, Jian-qiu, "A Simple Key Management Scheme Based on WiMAX" in Proc International Symposium on Computer Science and Computational Technology, (Volume 1) pp. 3-6 20-22 December 2008, Shangai, China

[5] IEEE Standard for Local and Metropolitan Area Networks. Air Interface for Fixed and mobile Broadband Wireless Access Systems, IEEE Std 802.16e. New York: IEEE Press, 2006.

[6] M. Barbeau, J. Hall and E. Kranakis, " Detecting Impersonation Attacks in Future Wireless and Mobile Networks", Secure Mobile Ad-hoc Networks and Sensors, Published in: Proceeding MADNES'05 Proceedings of the First international conference on Secure Mobile Ad-hoc Networks and Sensors, Ottawa, pp. 80-95, 2006.

[7] M. McDowell, "Understanding Denial of Service Attacks," National Cyber Alert System, 1 Aug. Vol.2 No.2 (2010), Article ID:1866, 4 pages pp. 134-137 DOI:10.4236/cn.2010.22020 Received February 23, 2010; revised April 20, 2010; accepted April 29, 2010

[8] K. Youngwook, L. Hyoung-kyu and B. Saewoong, "Shared Authentication Information for Preventing DDoS Attacks in Mobile WiMAX Networks", Proceedings of the 5th consumer communications and networking conference, Las Vegas, Published in: Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE, pp.765-769 10-12 Jan 2008.

[9] N. Beacham, " Man in the Middle (MITM) Attacks," Technology and More, JOURNAL NAME: Communications and Network, Vol.2 No.2, May 31, 2010.

[10] J. M. Hartley, " WiFi and WiMAX Protocols of security," December 2008. http://softwarecommunity.intel.com/articales/eng/3708.htm

[11] R. Millman, "Security Experts See Vulnerabilities in WiMAX." WiMAX.com, 17 oct 2006.

[12] M. Barbean, " Threats: Threats to WiMAX," http://www.freewimax info.com/ physical-layer.html

