Investigation of Security Issues in WiMAX Networks

Avni Khatkar
UIET, MDU, Rohtak
avnikhatkar@gmail.com

Yudhvir Singh
UIET, MDU, Rohtak
dr.yudhvirs@gmail.com

Raj Kumar
MRK IET, Rewari
raj.indya2000@gmail.com

Abstract: In today's era of communication where wireless media is replacing wired media, security is of utmost concern. The WiMAX technology was developed after the analysis of security failures in IEEE 802.11 technology. As WiMAX has a very high coverage area, security becomes one of the most important issues. Both mobile and fixed WiMAX has many striking features like connection-oriented MAC layer, prerequisite QoS for different applications, efficient mobility, and power-saving features. Needless to say, all these striking features must be protected against malevolent actions by security mechanisms. This paper focuses on discussing security vulnerabilities in WiMAX networks and addressing them by using required security mechanisms

Key Words: WiMAX, Security threats, Jamming, Security Mechanism.

Introduction:

Wired Systems are secure but being a wireless system, WiMAX has security vulnerabilities [1]. Security is of utmost concern in the real world and WiMAX was developed after the security failures were analyzed from IEEE 802.11 networks [2]. When the wireless network technology has a higher coverage area as high as in WiMAX, security becomes one of the most important issues. WiMAX, both mobile and fixed, has many attractive features such as connection-oriented MAC layer, provision of the QoS for different applications, efficient mobility, and power-saving features. Needless to say, all these attractive features must be protected against malicious activities by security mechanisms.

The lowest layer i.e. PHY layer, is open to PHY layer attacks such as jamming and rushing. Jamming is done by introducing a source of strong noise to significantly lower the capacity of the channel, therefore, denying services to all stations. However, jamming is detectable with radio analyzer devices [3]. Rushing or scrambling is another type of jamming, but it takes place for a short interval of time aimed at particular frames. The PHY layer is not protected from being interfered or even catastrophic failures. So, it is essential to include technologies to secure PHY layer and higher layers for a converged routable network and devices within the system and thus follow a cross-layer approach.

1. Survey of Relevant Literature:

There has been a quick growth in different wireless networks. To meet up the increasing demand and in order to provide better service, a lot of research is carried out in this field. With this growth in demand it becomes impervious for the service providers to endow their services with security. As the IEEE 802.16 standard is emerging and maturing, QoS and Security issues have been addressed by many researchers from all across the globe. In this section, a brief summary of current work in this field is presented in tabular form in table 1, for various security techniques.

Table 1: Literature Review of Security in WiMAX

Authors (Year)	Paper Concept/Idea	Contribution and Remarks
Chung-Kuo Chang, Chin-Tser Huang (2007) [9]	Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks	Fast key exchange and fast authentication procedures are introduced to reduce authentication time during network re-entry. The effects of latency reduction by fast authentication are compared with results of other solutions.
Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki	Security Vulnerabilities and Solutions in Mobile WiMAX	Analyzed the security of Mobile WiMAX and propose some possible security improvements and solutions to eliminate the vulnerabilities.

Tanaka (2007) [10]		
Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuanan Liu(2008) [11]	Analysis of mobile WiMAX security: Vulnerabilities and solutions	Modified and eliminated existing weaknesses in DH key exchange protocol to fit it into mobile WiMAX network.
Chin-Tser Huang, J.M.Chang (2008) [2]	Responding to Security Issues in WiMAX Networks	Introduced security protocols used in WiMAX networks and discuss deficiency of protocols in terms of anti-replay, efficiency, scalability, and forward and backward secrecy, as well as how they can be enhanced to address these issues for real applications.
Po-Wen Chi, Chin-Laung Lei (2009) [12]	A prevention approach to scrambling attacks in WiMAX networks	WiMAX is exposed to a special kind of DoS attacks which can target a specific victim connection without influencing the others, authors explain this with a prevention approach.
Chen-Hua Shih, Yaw-Chung Chen (2009) [13]	A Cross-Layering IPv6 Fast Handover Scheme for Real-Time Applications in IEEE 802.16e Network	Proposed a cross-layering IPv6 fast handover scheme which features integrated layer 2/layer 3 messages and fast network re-entry methods which reduce the service disruption time by about 93.6% for downlink and 89.7% for uplink so that the quality of service (QoS) for real-time applications can be improved significantly.
J. Brown, Du Xiaojiang (2009) [14]	Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks	Proposed a general tree-based rekeying scheme, which is more efficient than the MBRA and can significantly reduce communication overhead.
Yonghui Zhang, Xinhua Jiang, Wang Lei, Zhangxi Lin (2011) [15]	Key technologies overview on mobile Internet access and mobility support	Current progressing wireless access technologies were valued on their strengths and weaknesses and the newest mobility support researches and progresses over IP layer, such as MIP, NEMO, SIP and DTN, was introduced.
Junwoo Jung, Jaemin Jeung, Jaesung Lim (2011) [16]	Control channel hopping for avoidance of scrambling attacks in IEEE 802.16 systems	Proposed an approach to prevent the disruption of the control channel from this scrambling attack in IEEE 802.16 systems.
Bo Zhou (2011) [17]	An intrusion detection system based on WiMAX	Designed and realized an intrusion detection system based on improved WEP algorithm with full consideration of the vulnerabilities, characteristics and performance of WiMAX network.
C. Kolias, G. Kambourakis, S. Gritzalis (2013) [18]	Attacks and Countermeasures on 802.16: Analysis and Assessment	Provided a comprehensive taxonomy of attacks and countermeasures on 802.16.
A. Bhatele, R. Parajuli, B.K. Chaurasia (2013) [19]	Traffic Analysis for WiMAX	Traffic analysis at different packet length is also presented over IEEE 802.16(e) network so as to give a clear picture of traffic flow in a WiMAX network.
R. Yaramasu, S.Qureshi, S.B. Lande (2014) [20]	A Quality of Service Based Resource Allocation in Wireless Communication Networks	Proposed solution efficiently enhances performance and utilizes resources and it dynamically changes the bandwidth allocation based on the traffic characteristics and service demands using different techniques.

1. WiMAX Protocol Architecture and Security

The WiMAX protocol architecture has two main layers i.e. Physical layer and Medium Access Control (MAC) layer as shown in figure 1. The MAC Layer is further subdivided into Service Specific

Convergence Sub layer, which is responsible for interfacing with upper layers, MAC common part sub layer which provides core functionality for system access, allocation of bandwidth and connection establishment and maintenance. The third sublayer is MAC security sublayer. The main goal of the security sub-layer is to police PDUs and ensure confidentiality of information exchanged between the BS and MT. This layer provides functionalities such as encryption, secure key exchange, integrity control and authentication.

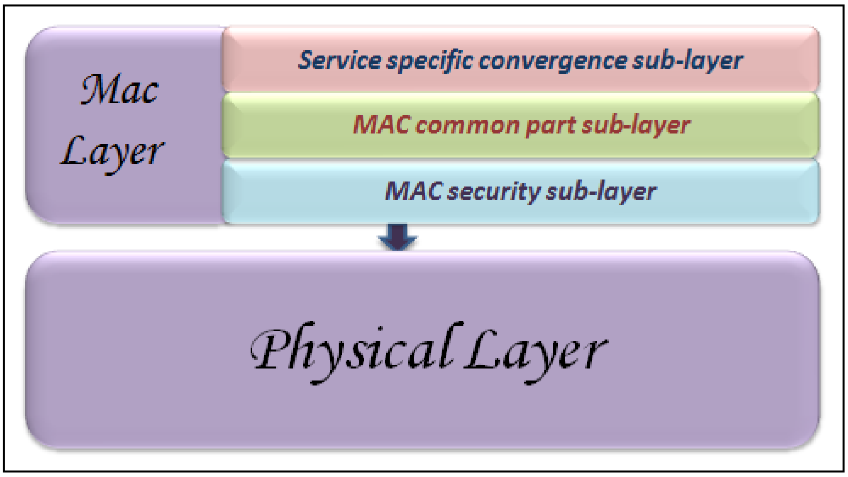
Mac Layer
Service specific convergence sub-layer
MAC common part sub-layer
MAC security sub-layer
Physical Layer

Figure 1: IEEE 802.16 PHY and MAC Layers

2. Security Goals

Two main goals of security in WiMAX are to provide privacy and access control. Due to wireless nature of the network, privacy is an important issue and is achieved by encrypting connections between the base station (BS) and SS in the network. To provide privacy across the air interface, the WiMAX standard has introduced the concept of security associations (SAs). SA is a group of information about authentication and encryption algorithms and their associated keys. There are three types of SAs: primary, static, and dynamic. Both BS and SS share the security information at the initial authorization stage through a primary SA. Static SAs do not change. Actually, the BS is provided with a set of encryption and authentication algorithms in the form of static SA for which the SS has subscribed. Dynamic SAs are assigned to each service flow and their lifetime is equal to the lifetime of the corresponding flow. In other words, each service flow requires a different set of security capability, therefore, dynamic SAs serve this purpose [4].

3. Security Issues

In WiMAX networks, the main security issues used for the protection of information of the users from malicious attacks from the intruders follow different ways. These security issues are described as under:

i. Authentication

In WiMAX, each subscriber station (SS) must have a X.509 certificate that will uniquely identify each subscriber in 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 [5]. A key breach in the authentication mechanism used by WiMAX's privacy and key management (PKM) protocol is the missing concept of BS or service provider authentication. This sometimes leads to man-in-the-middle attacks, subjecting subscribers to various confidentiality and availability attacks. Amendments to IEEE 802.16e lead to supporting Extensible Authentication Protocol (EAP) in WiMAX networks.

ii. 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 as well as other crucial characteristics of network [5].

iii. Availability

WiMAX uses licensed radio frequency spectrum which provides some protection from unintentional interference. But it is not difficult for an attacker to jam the spectrum for all planned WiMAX deployments. 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 de authentication of flood attacks applied against wireless LAN networks [5].

iv. WiMAX Threats

WiMAX security is implemented in the security sub-layer which lies above PHY layer [6], so the physical layer is an unsecure layer [15] 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 mobility also makes it more vulnerable to attacks because the attackers do not need to be at a fixed location and this makes network monitoring process more difficult [6]. These attacks are as described below:

a. Jamming attack

Jamming is done by introducing a source of strong noise to significantly lower the capacity of the channel, therefore, denying services to all stations [3]. Performing a jamming attack is not difficult.

Solutions: Jamming attack can be prevented by increasing [3] signal power or bandwidth using techniques such as frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS). Moreover law enforcement agencies can also help, in addition radio spectrum monitoring equipments detect jamming as well as radio direction finding tools can identify sources of jamming.

b. Scrambling attack

Scrambling is that type of jamming which happens for short intervals of time and is targeted [3] to specific WiMAX frames at PHY layer. It is up to the attacker to selectively scramble control or management information which affects the functionality of network in normal mode. Scrambling attack, attacker requires to interpret control information and to send noise during specific intervals [3].

Solutions: Anomalies monitoring beyond performance norm (or criteria) can detect scrambling and scramblers [3].

c. Water torture attack

In this an attacker forces [7] a subscriber station to drain its battery or consume computing resources by sending a series of fake frames. This attack is more dangerous than Denial-of-Service (DoS) attack because the subscriber station is a portable device and it carries limited resources.

Solutions: 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.

d. Other Threats

IEEE 802.16 is also vulnerable to different types of attacks like forgery attack in which an attacker with sufficient radio transmitter can write to a wireless channel [7]. Mesh mode in 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: While dealing with such security flaws, mutual authentication [8] comes into picture to curb such types of attacks.

Conclusion:

This paper described in depth the current trends in WiMAX networks for securing these networks from malicious attacks and outlined the solutions which can be used to deal with the different types of security flaws encountered in these networks. Different mechanisms which are required to be followed to get rid of the attacks are explained. In current paper, security vulnerabilities in WiMAX networks are discussed and solutions are provided to address them by using required security mechanisms.

References:

1. E.B. Fernandez, M. VanHilst, ‘‘An overview of WiMAX security,’’ in WiMAX Standards and Security, M. Ilyas, Ed. Boca Raton, FL: CRC Press, 2008, pp.197–204.
2. C.T Huang, J.M. Chang, “Responding to Security Issues in WiMAX Networks” *IEEE Magazine IT Professional*,Volume:10 Issue:5, September-October 2008, pp-15-21.
3. M. 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, pp.8-15.
4. M. Bogdanoski, P. Latkoski, A. Risteski, B. Popovski, “IEEE 802.16 Security Issues: A Survey,” *16th Telecommunications Forum, TELFOR*, 25-27 November 2008, pp. 199-202.
5. J. Wright, “WiMAX security issues” *Wireless Security, NetworkWorld.com*, 11 December, 2006.
6. T. Nguyen, “A survey of WiMAX security threats,” *Thesis Report*, nguyent@seas.wustl.edu, 2009, pp. 1-15.
7. D. Johnston, J. Walker, "Overview of IEEE 802.16 Security", *IEEE Security and Privacy*, vol. 2, issue 3, May-June 2004, pp. 40-48.
8. H. Jin, L. Tu, G. Yang, Y. Yang, “An Improved Mutual Authentication Scheme in Multi-Hop WiMAX Network”, *IEEE International Conference on Computer and Electrical Engineering*, 20-22 December 2008, pp. 296-299.
9. C.K. Chang, C.T. Huang, “Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks,” *IEEE Parallel Processing Workshops*, 10-14 September 2007, pp. 46.
10. A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka, “Security Vulnerabilities and Solutions in Mobile WiMAX,” *International Journal of Computer Science and Network Security,* vol. 7, no 11, November 2007, pp.7-15.
11. T. Han, N. Zhang, K. Liu, B. Tang, Y. Liu, “Analysis of mobile WiMAX security: Vulnerabilities and solutions,” *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 29 September 2008-2 October 2008, pp.828 – 833.
12. P.W. Chi, C.L. Lei "A prevention approach to scrambling attacks in WiMAX networks", *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops,WoWMoM,* 15-19 June 2009, pp.1 - 8.
13. C.H. Shih, Y.C. Chen, “A Cross-Layering IPv6 Fast Handover Scheme for Real-Time Applications in IEEE 802.16e Network,” *IEEE Fifth International Joint Conference on INC, IMS and IDC*, 25-27 August 2009, pp. 2056-2061.
14. J. Brown, D. Xiaojiang "Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks,” *IEEE Global Telecommunications Conference, GLOBECOM,* 30 November 2009-4 December 2009, pp.1 – 6.
15. Y. Zhang, X. Jiang; W. Lei, Z. Lin "Key technologies overview on mobile Internet access and mobility support", *IEEE Second International Conference on Mechanic Automation and Control Engineering (MACE),* 15-17 July 2011, pp. 5014 – 5017.
16. J. Jung, J. Jeung, J. Lim "Control channel hopping for avoidance of scrambling attacks in IEEE 802.16 systems", *Military Communications Conference, MILCOM 7*-10 November 2011, pp. 1225 – 1230.
17. B. Zhou "An intrusion detection system based on WiMAX", IEEE *International Conference Computer Science and Network Technology (ICCSNT),* vol. 4, 24-26 December 2011, pp. 2448 – 2451.
18. C. Kolias , G. Kambourakis, S. Gritzalis, “Attacks and Countermeasures on 802.16: Analysis and Assessment,” *IEEE Communications Surveys & Tutorials,* vol.15, Issue 1, First Quarter 2013, pp. 487-514.
19. A. Bhatele, R. Parajuli, B.K. Chaurasia, "Traffic Analysis for WiMAX", IEEE *5th International Conference on Computational Intelligence and Communication Networks (CICN),* 27-29 September 2013, pp.138 – 140.
20. R. Yaramasu, S. Qureshi, S.B. Lande, “A Quality of Service Based Resource Allocation in Wireless Communication Networks,” *International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC),* 9-11 January 2014, pp. 444 – 449.