Volume 2, Issue 1, January 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A SURVEY OF ROGUE BASE STATION ATTACKS IN WIMAX/IEEE802.16

Deepti
Department of ComputerScience
Indo Global College of Engineering Engineering

Deepika Khokhar
Department of Computer Science Science
Indo Global College of Engineering PTU, Jallandhar (India) PTU, Jallandhar(India)

Satinder Pal Ahuja
Department of Computer
Indo Global College of PTU, Jallandhar (India)

***Abstract* - WIMAX (Worldwide Interoperability for Microwave Access)/ IEEE 802.16 is a very promising technology. It is based on Wireless MAN technology. With the growing popularity of WIMAX, the security risks have increased many folds. WiMax is an appealing alternative to wired networks but there exist critical threats including jamming, eavesdropping and modification of management messages, masquerading as BS, and DoS attacks. In this paper we will give an overview of the security architecture of WIMAX. Then we will give an overview of the various kinds of threats viz. Physical Layer and MAC Layer threats, then lists the security requirements of a WIMAX system. Then we address to problem of a rogue base station (BS) in WIMAX/802.16 wireless access networks.**

***Keywords:* - WIMAX, Protocol Layer Architecture, Security Architecture, Types of Threats, Rogue BS in WIMAX.**

I. INTRODUCTION

WIMAX, short for Worldwide Interoperability for Microwave Access, is the name for 802.16 families of wireless services. WIMAX Technology is one of the emerging wireless technologies that provide us high speed mobile data and telecommunication services. WIMAX Technology works same as Wi-Fi does but it is more improved and efficient then Wi-Fi. In other words we can say that IEEE 802.16 or WIMAX is an excellent successor to Wi-Fi/ IEEE 802.11 It provides higher speed connection up to 70 Mbps over the area of 30 miles. Security has become a primary concern in order to provide protected communication in Wireless environment. Since WIMAX uses air interface for the transmission medium, both the PHY and MAC layers are readily exposed to security threats. The various classes of wireless attacks are interception, fabrication, modifications, interruption and repudiation. Two main entities in WiMAX are Base Station (BS) and Subscriber Station (SS). A rogue base station attacks can also be conducted due to absence of efficient security mechanism. These types of attacks occur due to absence of mutual authentication mechanism between the Subscriber Stations (SS) and the Base Stations (BS). These type of threats are also known as identity theft threats.It never offers a mean for the SS to verify the genuineness of a BS through the messages received from the BS. Thus, a rogue BS can generate and transmit any message to the SS. The wireless networks carry all sorts of confidential data, so security is a highly important part of any wireless network structure. WiMAX is open to more security threats than other wireless systems.

II. WIMAX ARCHITECTURE

A. Protocol Layer Architecture

The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer.. The PHY layer provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals. MAC layer further comprises of three sub-layers described as follows.

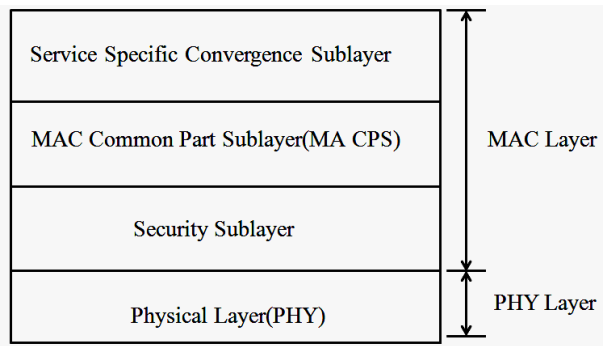

Fig. 1 Protocol Layer Architecture

i. Service Specific Convergence Sub-layer (CS):- It maps higher level data services to MAC layer service flow and connections.

ii. Common Part Sub-layer (CPS):- It is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocation and connection management. The MAC protocol data units are constructed in this sub-layer.

iii. Security Sub-layer:- It lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers.

B. Security Architecture

The security sub layer performs three main functions i: e authentication, authorization and encryption. The Security sub-layer has two main component protocols. A data encapsulation protocol for securing packet data across fixed BWA network. A key management protocol (PKM) providing the secure distribution of keying data from the BS to the SS. The architecture of security sub layer is shown in figure.

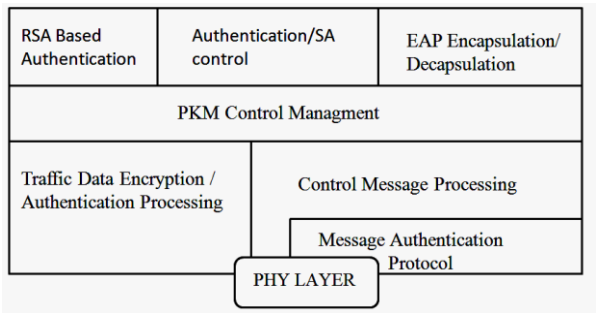

Fig. 2 WIMAX Security Architecture

The main components of security architecture of IEEE 802.16 are as follows:

i. Security associations: – A context to maintain the security state relevant to a connection between a base station (BS) and a subscriber station (SS).

ii. Certificate profile: – X.509 is used to identify communicating parties. These certificates are used by base stations to identify the identity of Subscriber Stations

iii. RSA authentication**: -** This protocol is based on X.509 certificates.

iv. EAP authentication: - The EAP uses particular kinds of credential (subscriber identity module, password, token-based, X.509 certificate or other) depending on the EAP method implemented.

v. HMAC/CMAC authentication: - The 802.16 standard security includes the use of a Hashed Message Authentication Code (HMAC) for some message authentication and integrity control. 802.16e added the possibility of using CMAC as an alternative to HMAC.

vi. PKM authorization: – An authorization protocol to distribute an authorization token to an authorized SS.

vii. Privacy and key management**: –** A protocol to rekey the SA. Once authorized to the network, the SS can now establish a data SA between it and the BS, for that it again uses the PKM protocol.

viii. Encryption**: –** A payload field encryption using DES-CBC in 802.16d, DES-CBC and AES-CCM in 802.16e.

III. THREATS TO WIMAX

WIMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack. There are many types of attacks in WIMAX such as Rouge Base Station Attacks, DoS (Denial of Service), Data Link Layer, Application Layer, Physical Layer, Privacy Sub Layer, Mutual Authentication, Key Management, Threat of Identify Theft, Water Torture, Black Hat Threat. The overview of the various kinds of threats viz. Physical Layer and MAC Layer threats are discussed as follows.

A. 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. Scrambling and jamming is two principal threats for WIMAX physical layer.

i. Jamming or Blocking - It is an attack achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel, therefore denying services (DoS) to all stations.

© 2011, IJARCSSE All Rights Reserved

ii. Scrambling or Rushing - It is a kind of jamming but it takes place for short intervals of time and targeted to specific WIMAX frames or parts of frames at the PHY layer.

iii. Water torture attack - It 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.

B. *Threats to the MAC layer*

There are a lot of defects or flaws in WIMAX security solutions at the MAC layer. It is a connection oriented layer.Identity threats are severe threats to WIMAX. They are also known as masquerade threats in which one system assumes the identity of another system. A rogue base station is an attack in which attacker station that duplicates a legitimate base station. The rogue BS makes the SSs believing that they are connected to the legitimate BS, thus it can intercept SSs' whole information. The lack of mutual authentication between the SS and BS is the main reason behind this kind of attack.

There are some other serious attacks that can exploit vulnerabilities in many aspects of the MAC layers. Two of the most destructive attacks can be classified as Man-In-The-Middle attacks (MITM) and Denial of Service attacks (DoS).

Man-in-the-middle attacks occur when attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. Denial-Of-Service (DOS) occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed.

IV. SECURITY REQUIREMENTS

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems.Well designed security architecture for a Wimax and other wireless communication networks should support the following essential requirements:

i. Privacy :- Provide protection from eavesdropping as the user data traverses the network from source to destination.

ii. Data integrity:- Ensure that user data and control/management messages are protected from being tampered with while in transit.

iii. Authentication: - Have a mechanism to ensure that given user/device is the one it claims to be. Conversely, the user/device should also be able to verify the authenticity of the network that it is connecting to. Together, referred to as mutual authentication.

iv. Authorization: - Have a mechanism in place to verify that a given user is authorized to receive a particular service.

v. Access control: - Ensure that only authorized users are allowed to get access to the offered services.

V. ROGUE BASE STATION IN WIMAX

These are commonly known as identity theft attacks. The rogue BS (base station) makes the SS (subscriber station) believing that they are connected to the legitimate BS, thus it can intercept SSs' whole information. SS can be compromised by a forged BS which imitates a legitimate BS. They are also known as Masquerade attack in which one system assumes the identity of another. A rogue BS is a malicious station that impersonates or duplicates legitimate base station. The rogue base station puzzles a set of subscribers who try to get service which they believe to be a legitimate base station. The attacker generates his own Authorization Reply Message containing its own self generated AK. Hence attacker can register himself as a BS with victim SS. The attacker has to capture the identity of legitimate BS. Then it builds messages using the stolen identity. The attacker must transmit while achieving a RSS (receive signal strength) higher than the one of the fake base station.

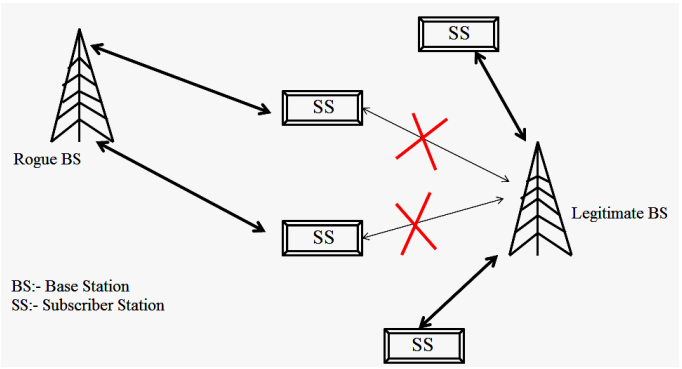

Fig. 3 Working of Rogue Base Stations

© 2011, IJARCSSE All Rights Reserved

WiMax/802.16 supports two models of authentication at network entry: unilateral (MS only) and mutual (BS and MS). The lack of mutual authentication between the SS and BS is the main reason behind this kind of attack. There are two types of certificate are categorize by WIMAX standard: one is for Subscriber Station (SS) certificates and other is for manufacturer certificates but there is no provision for Base Station (BS) certificates. A manufacturer certificate identifies manufacturer of WIMAX device. It can be self signed certificate or subjected to any third party. The SS certificate is used by BS to determine whether the SS is legitimate or not. Manufacturers normally create and sign Subscriber Station certificates. The major drawback of the WiMax security design is the lack of a Base Station (BS) certificate**.**

VI. CONCLUSION

Worldwide Interoperability for Microwave Access (WIMAX) is going to be an emerging wireless technology for future. With increasing popularity of Broadband internet wireless networking market is thriving. As the popularity of WIMAX increases, so will the threats to it. Some of the issues have been dealt with and no longer pose a problem, but some still persist and need to be considered carefully as WiMax becomes more prevalent. Malicious elements are working round the clock to break the security of the various networks. In a WIMAX system, data are transmitted via wireless link, so the security is becoming the hot topic of research. The scope of research in wireless security grows and makes the research more and more interesting due to rising security problems. It is therefore recommended for further studies, the various techniques to secure wireless networks. The scenarios with respect to behaviour of Rogue BS is unpredictable and dynamic in nature therefore the scenarios to detect such threats will require up gradation and change in scenarios as the technology with respect to wireless communication or networking changes. It is therefore recommended for further studies, the various techniques to identify and detect Rogue BS.

REFERENCES

[1] “Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations” Jie Huang, Chin-Tser Huang, Department of Computer Science and Engineering,University of South Carolina Columbia, South Carolina, USA,2011 IEEE.

[2]“Defending against Rogue Base Station Attacks using Wavelet Based Fingerprinting” Alaaedine CHOUCHANE, Slim REKHIS, and Noureddine BOUDRIGAalaaedine.ch@gmail.com,slim.rekhis@isetcom.rnu.tn,nab@supcom.rnu.tn Comm” Networks and Security Research Lab. University of 7th of November at Carthage. Tunisia. 2009 IEEE.

[3] “A Simple Key Management Scheme Bsaed on WiMAX” Lang Wei-min, Department of Information Warfare PLA Institute of Communication Command Wuhan, China E-mail: wemlang@sina.com, Wu Run-sheng, Wang jian-qiu, Institute of Physics and Communication & Electronics Jiangxi Normal University Nanchang, China E-mail: wurunsheng1980@163.com 2008 IEEE.

[4] “Research on the Authentication Scheme of WiMAX” LANG Wei-min, ZHONG Jing-li, LI Jian-Jun, Department of Information Warfare, PLA Institute of Communication Command, Wuhan, China E-mail: wemlang@sina.com , QI Xiang-yu, Armored Force Engineering Institute, Beijing, China E-mail: wmlang76@tom.com 2008 IEEE.

[5] “Authentication Scheme in Multi Hop WiMAX Network” in Proc International Conference on Computer and Electrical Engineering, Huixia Jin, Li Tu, Gelan Yang et.al , “An Improved Mutual December 20-22, 2008.

[6] “Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX” ,Sanjeev Dhawan IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications,2007.

[7] “Fundamentals of WiMAX: Understanding Broadband Wireless Networking”, New Jersey: Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, Pearson Education Incorporation, 2007.

[8] “WiMAX: A Wireless Technology Revolution” Boca Raton: G. S. V. Radha Krishna Rao, G. Radhamani, Auerbach Publications, 2007.

[9] “WiMAX/802.16 threat analysis”, M. Barbeau, Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, pp. 8–15, October 2007.

[10] “Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks” La détection de fausses stations de base dans les réseaux d’accès sans fil WiMax/802.16 Michel Barbeau School of Computer Science, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6 Jean-Marc Robert1 Alcatel, CTO Security Research and Competence Center, 600 March Rd., Ottawa,2006.

[11] “Rogue AP Detection in the Wireless LAN for Large Scale Deployment” Sang-Eon Kim, Byung-Soo Chang, Sang Hong Lee KT 17 Woomyeon-dong, Seocho-gu, Seoul 137-792, Korea and Dae Young Kim Department of InfoComm Engineering,2006

[12] “Securing a Wireless World”, IEEE Comm. Mag., vol. 94, Hao Yang, Fabio Ricciato, Songwu Lu, and Lixia Zhang, no.2, pp 442-454, Feb 2006.

[13] “IEEE Standard for Local and Metropolitan Area Networks. Air Interface for Fixed and mobile Broadband WirelessAccess Systems” IEEE Std 802.16e. New York: IEEE Press, 2006.

[14] “Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential”, GHOSH (A.), WOLTER (D.R.), ANDREWS (J.G.), CHEN (R.), *IEEE Communications Magazine*, 43, no. 2, pp. 129-136, February 2005.

[15] “Overview of IEEE 802.16 Security,” D. Johnston, J. Walker, Published by IEEE Computer Society, 2004.

[16] “Security Issues in Privacy and Key Management Protocols of IEEE 802.16,” X. Sen, M. Matthews, H. Chin-Tser, Department of Computer Science and Engineering - University of South Carolina Columbia, SC 29208, USA,2004.

[17] www.wimaxforum.org/resources/featured-research

[18] www.wimax industry.com/wimaxwhitepapers.html

[19] http://4g-wirelessevolution.tmcnet.com

[20]www.freewimax.com

© 2011, IJARCSSE All Rights Reserved

© 2011, IJARCSSE All Rights Reserved