A New Classification Based on IEEE 802.16 for Wireless Access

Noudjoud Kahya-Abbaci, Nacira Ghoualmi
Network and Security Laboratory
Department of Computer Engineering
Badji Mokhtar University
Annaba, Algeria
Kahya.noudjoud@gmail.com, Ghoualmi@yahoo.fr

ABSTRACT: *Recently the most accepted standard for wireless broadband access is termed as Wimax which ensures effective and seamless technology. By realizing this value we in this work, propose a new innovative security solution for wireless access in a long range. We have studied in depth the issues in the communication layers and hence we classified these limitations in the protocols. The two identified attacks are man-in-the-middle attacks and denial of service attacks. This classification is effective as it considers un-authentication, unencryption.*

Keywords: WiMAX, Security, Vulnerabilities, Attacks

Received: Received 1 September 2011, Revised 18 November 2011, Accepted 23 November 2011

1. Introduction

IEEE 802.16, commonly known as Worldwide Interoperability for Microwave Access (WiMAX), is a recent wireless broadband standard that has promised high bandwidth over long-range transmission.

In the past few years, the IEEE 802.16 working group has developed a number of standards for WiMAX. First published in 2001, the IEEE 802.16 standard specified a frequency range of 10–66 GHz with a theoretical maximum bandwidth of 120 Mb/s and maximum transmission range of 50 km. However, the initial standard only supports line-of-sight (LOS) transmission and thus does not seem to favor deployment in urban areas. A variant of the standard, IEEE 802.16a-2003, approved in April 2003, can support non-LOS (NLOS) transmission and adopts OFDM at the PHY layer. It also adds support for the 2–11GHz range. These two standards were further revised in 2004 (IEEE 802.16-2004). Recently, IEEE 802.16e has also been approved as the official standard for mobile applications.

In the IEEE 802.16 technology, security has been considered as the main issue during the design of the protocol. However, several design and security vulnerabilities were found in this technology. These vulnerabilities are the main cause to introduce unauthenticated messages which are susceptible to forgery, the unencrypted management communication which reveals important management information and it does not have perfect mechanism for mutual authentication.

This article presents an analysis of the security threats to Wimax security that reflects to most recent work of the IEEE and Wimax

Forum and performed based on the following questions.

- What are the Vulnerabilities and Security threats of the Wimax Technology?
- What are the attacks at the Physical Layer then at the MAC layer?

The reminder of this paper is organized as follow: Section 2 provides background and detailed information about Wimax architecture and securities specifications in the security sublayer. In Section 3 the literature is reviewed. Then vulnerabilities in Wimax security will be discussed in section 4. In this section we analyze DoS attacks and man-in-themiddle attacks, based on unauthenticated message, encryption management and the absent of mutual authentication. The last section concludes the paper.

2. WIMAX Overview

In order to understand Wimax security issues, we first need to understand Wimax architecture and how securities specifications are addressed in this technology.

2.1 Wimax Architecture

The protocol architecture of Wimax/802.16 is structured into two main layers: the Medium Access Control (MAC) layer and physical layer see Figure 1.

The MAC layer consists of three sublayers: the service specific convergence sub-layer (CS), MAC common part sub-layer (MAC CPS), and security sub-layer.

The service specific Convergence Sub-layer (CS) maps higher level data services to MAC layer service flows and connections. There are two type of CS: ATM CS which is designed for ATM network and service, and packet CS which supports Ethernet, point to-point protocol (PPP), both IPv4 and IPv6 internet protocols, and virtual local area network (VLAN).

The MAC Common Part Sub-layer (MAC CPS) is the core of the standard. 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.

The Security Sub-layer lies between MAC CPS and PHY layer. This sub-layer is responsible for encryption and decryption of data traveling to and from the PHY layer, and it is also used for authentication and secure key exchange.

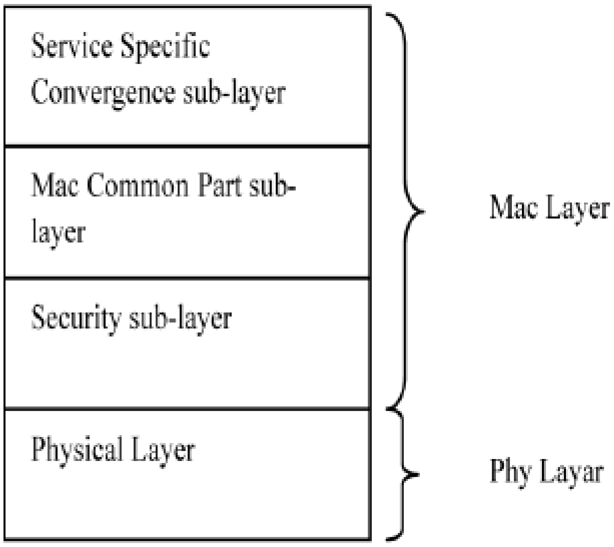

Figure 1. The IEEE 802.16 Protocol Structure

2.2 Security Scheme

Compared to Wi-Fi, security has been included in the design of WiMAX systems at the very start. In both IEEE 802.16- 2004 and IEEE 802.16e-2005 standards, MAC layer contains a security sub-layer. To provide secure distribution of sensitive data from the BS (Base Station) to the SS (Subscriber Station) and protect network services from attacks, Wimax applies strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization. The most of security issues as described in the following figure:

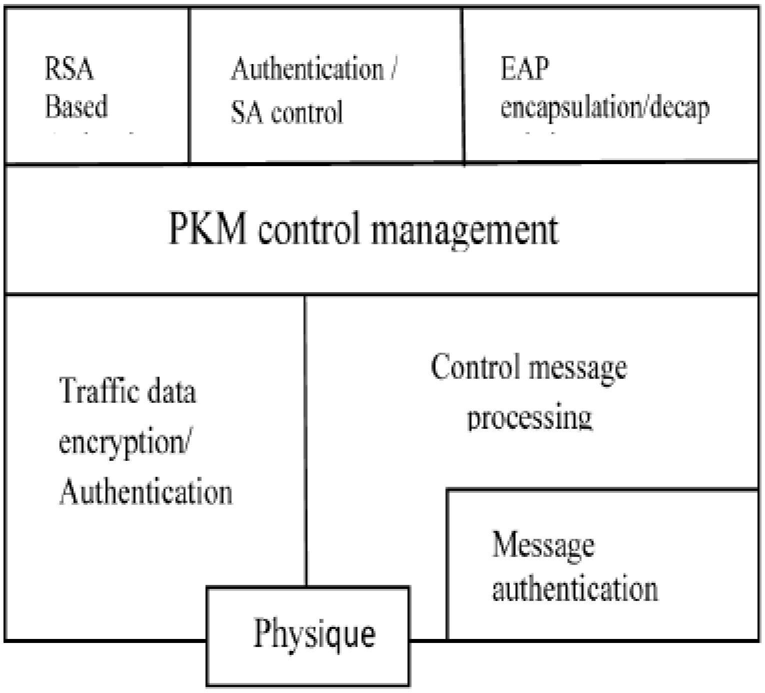

Figure 2. MAC Security Sub-

This sub layer basically performs three functions: Authentication, Authorization and Encryption.

1- Authentication: Authentication is achieved using a public key interchange protocol that ensures not only authentication but also the establishment of encryption keys. 802.16e basedon Mobile Wimax defines Privacy Key Management (PKM) protocol in security sub-layer, which allows three types of authentication:

*The first type is RSA based authentication**:*** RSA based authentication applies X.509 digital certificates together with RSA encryption. In this authentication mode, a BS authenticates the SS through its unique X.509 digital certificate that has been issued by the SS manufacturer. The X.509 certificate contains the SS's Public Key (PK) and its MAC address. When requesting an Authorization Key (AK), the SS sends its digital certificate to the BS, and then BS validates the certificate, uses the verified Public Key (PK) to encrypt an AK and sends back to the SS. All SSs that use RSA authentication have factory installed private/ public key pairs together with factory installed X.509 certificates [1].

The second type is EAP (Extensible Authentication Protocol) based authentication: In the case of EAP based authentication, the SS is authenticated either by an X.509 certificate or by a unique operator-issued credential such as a SIM or by user-name/ password. There are three types of EAP: the first type is EAP-AKA (Authentication and Key Agreement) for SIM based authentication; the second type is EAP-TLS (Transport Layer Security) for X.509 based authentication; the third type is EAP-TTLS (Tunneled Transport Layer Security) for SS-CHAPv2 (Microsoft- Challenge Handshake Authentication Protocol) [1].

The third type is RSA based authentication followed by EAP authentication.

2- Authorization: This process follows the authentication process. SS requests for an AK and a SAID (Security Association ID) from BS by sending an Authorization Request message. This message includes the SS X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS interacts with an AAA (Authentication, Authorization and Accounting) server to validate the request from the SS, and sends back an Authorization Reply which includes the AK encrypted with the SS's public key and a lifetime key and an SAID [1] [2].

3- Encryption: The previous authentication and authorization process results in the assignment of and Authorization Key (AK), which is 160 bits long. The Key Encryption Key (KEK) is derived directly from the AK and it is 128 bits long. The KEK is not used for encrypting traffic data; so SS require the Traffic Encryption Key (TEK) from BS. TEK is generated as a random number generating in the BS using the TEK encryption algorithm where KEK is used as the encryption key. TEK is then used for encrypting the data traffic.

3. Literature Review

Few of relevant papers tackle the security issues of WIMAX network. T.Han and all [1], M.Rahman and M.Kowsar [3], M.Barbeau [4], M.Nasreldin and all [5], they give the most complete analysis of WIMAX security; they focused on the problem of IEEE 802.16.mechanisms for this technology and his security threats which are described in certain papers by different authors.

Table 1 contains the tabular format of a summarized review of the literature. What are the challenges to the WiMAX? & what are the solutions for these challenges. Every author has its own view.

Author	Summary	Problems/Challenges	Solution
Michel Barbeau 2005 [4]	An analysis of the security attacks on the wimax and architecture has been conducted. Main focus is on the threats analysis of physical and Mac layer.	- Jamming, - screambling, - DDOS, - Rouge BS, -X.509 digital certificate	Communication keys should be secure mutual authentication needed.
Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El-Hennawy. 2008 [5]	An analysis of threats according to the level of risk to IEEE 802.16. These threats were classified.	- Eavesdropping of management message. - Rouge BS. - DOS. - Jamming attack.	Strong authentication technique for SS and mutual authentication for BS. Spread spectrum scheme. Intrusion Prevention System.
Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu 2009 [1]	The paper is an overview of security architecture of mobile WiMAX network. He investigate man-in-the-middle attacks and Denial of Service (DoS) attacks toward 802.16ebased Mobile WiMAX network.	- Man-in-the-middle attacks. - RNG-RSP DoS attack. - DoS attacks.	propose Secure Initial Nenvork Entry Protocol (SINEP) based on DiffieHellman (DB) key exchange protocol to enhance the security level during network initial.
Muhammad Sakibur Rahman, Mir Md. Saki Kowsar 2009 [3]	This article shows security vulnerabilities found in WiMAX (man-in-the-middle attack) and gives possible solutions to eliminate them.	- Man-in-the-middle attacks. -Description of some unauthenticated and unencrypted management messages which threat system reliability.	Propose modify DH protocol to fit mobile WiMAX to eliminate man-in-the-middle attack by using cryptographic sealing function.
John Hong Kok Han, Mohamad Yosoff Aias and Goi Bok Min. 2009 [8]	This paper presents one of the possible attacks namely the denial of service attacks on the IEEE 802.16e-2005 mobile wimax networks.	- DoS attacks on IEEE 802.16e.	The authors Simulation of DoS attacks and they show that a DoS attack exploiting the design of RNG-RSP messages is devastating the overall service levels of the wimax network.

Table 1. Summarized table of the review

An analysis of the security attacks on the WiMAX and architecture has been conducted. Main focus is on the threats analysis of Physical and MAC layer. Jamming, Scrambling, DDoS, Rouge BS creation, compromising of X.509 digital certificates are some the common attacks on WiMAX technology. The techniques used to countermeasure these attacks/threats are spread spectrum scheme, Strong Encryption techniques. Communication keys security and Mutual Authentication but still the threats are there. Three options for authentication are discussed, but all the three can be compromised by an attacker.

4. Vulnarablities in WIMAX

In this paper, we give also an overview of security scheme in IEEE802.16. We investigate man-in-the-middle vulnerabilities and DoS vulnerabilities in Wimax, we analyze how the man-in-the-middle attacks based on unauthenticated, unencrypted message and unmutual authentication are launched.

Wimax has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack.

A-Physical layer threats:
WIMAX/802.16 is vulnerable to physical layer attacks such as jamming and scrambling:

A-1 Jamming: Is archived by introducing a source of noise strong enough to significantly reduce the capacity of the channel. Jamming is either unintentional or malicious, jamming segments of bandwidth, once detected, can also be avoided in spread spectrum [6].

A-2 Scrambling: It is targeted to specific frames or parts of frames. Scramblers can select what they want to scramble, control information or management information to affect the normal operation of the network. Scrambling becomes a major problem when the network deals with time sensitive messages which cannot tolerate delay such as channel measurement report requests or responses [1][2].

B- Mac Layer Threats:
We analyze vulnerabilities contained in Mac layer and we categorize these weaknesses in the protocol into two kinds: they are man-in-the-middle vulnerabilities and denial of service vulnerabilities.

B-1 Man-in-the-middle vulnerabilities: In this kind of attack, the attacker intercepts messages during the process of communication or a public key exchange and then retransmits them, tempering the information contained in the message, so that the two original parties still appear to be communicating with each other.

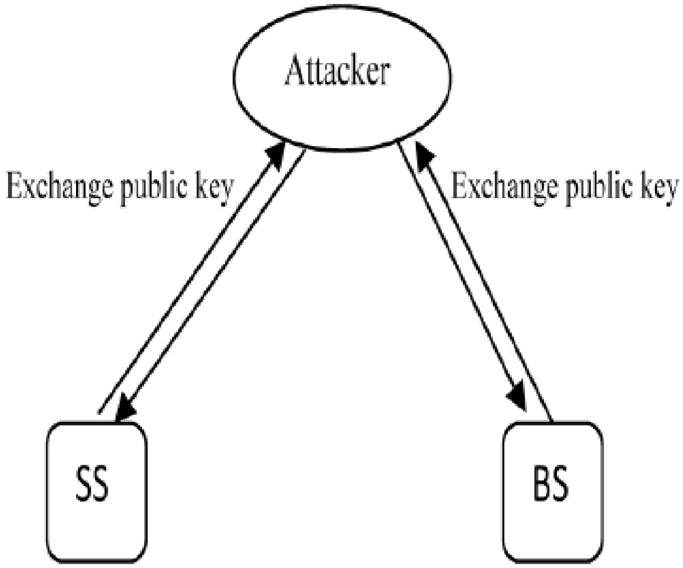

Figure 3. Man-in-the-middle attack

In Wimax, three kinds of vulnerabilities give a possibility of man-in-the-middle attack to BS and SS.

Unauthenticated messages: Some management messages are not covered by any authentication mechanism like hash based message authentication code (HMAC), this introduces some vulnerability. A couple of management message are sent over the broadcast management connection. Since in Wimax security architecture, there is no common key which can be used as the authentication of broadcasted management message. So the authentication of these messages is difficult. Furthermore, a common key would not completely protect the integrity of the message as Subscriber Station sharing the key can be generated by unauthenticated Base Station.

Unencrypted management communication: Initial network entry contains four processes: Initial Ranging Process, SS Basic Capability (SBC) negotiation process, PKM authentication process, and Registration Process. A most of the management message remains unencrypted, the only messages which are encrypted are key transfer messages. In the initial network entry procedure, there exist the possibilities that, through intercepting and capturing message in this entry procedure, attacker camouflages himself as the legitimate SS and send tamped SBC-RSP message to serving BS while interrupting the legitimate SS's communication with the legitimate BS, The spoofed message may contain false message about the security capabilities of the legitimate SS. For instance, the attacker may send messages to inform the BS that the SS only supports low security capabilities or has no security capabilities. In this situation, if the BS supports this kind of SS, the communication between the SS with the serving BS will not be encrypted [1]. As a result, the attackers would wiretap and tamper all the information transmitted.

Lack of mutual authentication: The lack of mutual authentication between the SS and BS is the main reason of the presence of the man-in-the-middle attack. The SS authenticates itself through its certificate but the BS attacker forces to authenticate itself and tries to initiate a session by transferring an AK. The attacker generates his own Authorization Reply Message containing its own self generated AK. And hence the attacker can register himself as a BS with the victim SS. There is a provision of mutual authentication in user networks in IEEE 802.16. It is based on the already discussed EAP. The authentication occurs after scanning, acquisition of channel description and ranging etc. The WiMAX EAP methods can be actually implemented using the EAP-TLS method [2].

B-2 Denial of Service vulnerabilities:

Denial of Service (DoS) attack is an incident in which a subscriber is deprived of the service of a resource they would normally expect to have.

Maximum DoS vulnerabilities stem from unprotected management messages.

Ranging Request (RNG-REQ) message: The Ranging Request (RNG-REQ) message is the very first message sent by an SS seeking to join a network. The message announces the SS's presence and is a request for transmission timing, power, frequency and burst profile information. The message is also sent periodically to allow for adjustments on the part of the SS. The RNG-REQ also allows the SS to inform the BS of its preferred downlink burst profile [7]. An attacker can intercept the message to change the reported most preferred burst profile of SS to the least effective one, hence downgrading the service.

Ranging Response (RNG-RSP) message: As it receives, the RNG-REQ message from an entering SS, the BS responds with a RNG-RSP message. The BS uses this message to change up- and downlink channel of the SS, transmission power level, reinitialize the MAC or even terminate communications with the SS. BS also uses the RNG-RSP message to modify the settings of the transmission link to improve the quality and efficiency of its services. This message, like the RNG-REQ, is unauthenticated, unencrypted. An Attacker can forge a RNG-RSP message to alter the power level of the SS to transmit at minimum power. The effect of this setting is that the SS transmit at a power so low, it can barely reach the actual BS and triggers the initial ranging procedure repeatedly [8]. Alternatively, a water torture attack can also be performed by the attacker in which the RNG-RSP message will tell the SS to increase its power levels to maximum to effectively and quickly drain its battery life.

The last points describe a possible DoS attack in mobile WIMAX.

DoS attacks based on Mobile Neighbor Advertisement (MOB_NBR_ADV) message: MOB_NBR_ADV message is used only in IEEE 802.16e, is sent from serving BS to publicize the characteristics of neightbor base stations to SSs searching for possible handovers. This message is not authenticated. Thus it can be forged by an attacker in order to prevent the SSs from efficient handovers downgrading the performance or even denying the legitimate service.

Sleep control messages: Mobile Wimax introduces sleep mode to minimize MS's power usage and reduce usage of BS air interface resources. Sleep mode is a state in which an SS conducts pre-negotiated periods of absence from the BS air interface. The SS can set the sleep mode in the bandwidth request and uplink sleep control messages that are not authenticated. The attacker can send the bandwidth request and uplink sleep control message with the identifier of victim SS [1]. As a result, the BS will stop transmitting messages to that SS, so performing a DoS attack.

5. Conclusion

After studying the Wimax architecture and their security measures, we came to an end that a lot of security services are provided to secure the communication but, several design and security vulnerabilities were found in this technology. These vulnerabilities are the main cause to introduce unauthenticated messages which are susceptible to forgery, the unencrypted management communication which reveals important management information and it does not have perfect mechanism for mutual authentication;

A lot of security concerns should be provided, so future work is needed in this area to secure the communication and countermeasure the security threats/attacks.

References

[1] Han, T., Zhang, N., Liu, K., Tang, B., Liu, Y. (2008). Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Networks. Atlanta, USA.

[2] Hasan, S.,Qadeer, M. (2009). Security Concerns in WiMAX" India ISCIT IEEE.

[3] Sakibur Rahman, M., Saki Kowsar, M. (2009).WiMAX Security Analysis and Enhancement. 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December, Dhaka, Bangladesh.

[4] Barbeau, M. (2005). Wimax /802.16 Threat analysis". ACM in workshop on quality of service and security in wireless and mobil networks.

[5] Nasreldin, M., Aslam., El-Hennawy, M. (2008). Wimax Security. 22h international conference on advanced information networking and application, IEEE.

[6] Yang, H., Riccato, F., Lu, S., Zang, L. (2006). security wireless word, published by IEEE commun.

[7] Naseer, S.,Younus, M., Ahmed, A. (2008). Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks: A Survey. ACIS International Conference on Software Engineering,Artificial Intelligence, Networking, and Parallel/Distributed Computing Ninth. IEEE.

[8] Han , J.,Yusoff Alias, M., Min, G. (2009). Potential Denial of Service Attacks in IEEE802.16e-2005 Networks. ISCIT. Published by IEEE.