Analysis of Security Weaknesses in IEEE 802.16

Noudjoud Kahya-Abbaci, Nacira Ghoualmi
Department of Computer Engineering
LRS laboratory
Badji Mokhtar University
Annaba, 23000, Algeria
Kahya.noudjoud@gmail.com, Ghoualmi@yahoo.fr

ABSTRACT: *The IEEE 802.16 standard, usually known as WIMAX, is the latest technology that has promised to offer broadband wireless access over long distance. In this article we offer an overview of the state-of-the-art of security issue on WIMAX, which is a new and hot research point for telecommunication and computer scientist, we analyze vulnerabilities contained in layers and we categorize these weakness into three kinds: man-in-the-middle, replay and denial of service attacks. We give a classification of the man-in-the-middle attacks based on unauthentication, unencryption message and unmutual authentication. Some of these attacks have been fixed with the adoption of recent amendments and security solutions in IEEE 802.16 but some still persist exist and need to be resolved. In our paper we propose a new authentication protocol more reliable and secure to prevent replay, DOS and man-in-the-middle attacks.*

Keywords: WiMAX, Security, Vulnerabilities, Man-in-the-middle, Replay, DOS, Authentication protocol

Received: 15 September 2011, Revised 30 November 2011, Accepted 1 December 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 of data in a variety of ways, ranging from point-to-point links to full mobile cellular-type access.

In the past few years, the IEEE 802.16 working group has developed a number of standards for WiMAX. First published in 2001[1], 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[2], 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) [3]. To support mobility, the IEEE has defined the IEEE 802.16e amendment [4], the mobile version of the 802.16 standard. In mobile WiMAX battery life and handover are essential issues to support mobility between subnets. This new amendment aims at maintaining mobile clients connected to a MAN while moving around. It supports portable devices from mobile smart-phones and Personal digital assistants (PDAs) and laptop computers. IEEE 802.16e works in the 2.3 GHz and 2.5 GHz frequency bands.

Table 1 review for WiMAX technology standards and versions.

Standard	802.16	802.16a/802.16-2004	802.16e-2005
Date Completed	December 2001	June 2004	December 2005
Spectrum	10-66 GHz	< 11 GHz	< 6 GHz
Modulation	QPSK 16-QAM 64-QAM	OFDM 256 subcarrier QPSK 16-QAM 64-QAM	Same as 802.16a
Channel condition	LOS	NLOS	NLOS
Bit Rate	32-134 Mbps	> 75Mbps	> 15 Mbps
Cell Radius	1-3 miles	3-5 miles	1-3 miles

Table 1. WIMAX standards and revision

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 paper 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 II provides background and detailed information about Wimax architecture and securities specifications in the security sub-layer. In Section III the literature is reviewed. Then vulnerabilities in Wimax security will be discussed in section IV. In this section we analyze replay, DoS and man-in-the-middle attacks which is based on unauthenticated message, encryption management and the absent of mutual authentication. Section V introduces the proposed revised authentication protocol and his analysis. 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 (Figure 1).

In the physical (PHY) layer, IEEE 802.16 supports four PHY specifications for the licensed bands. These four specifications are Wireless-MAN-SC (single carrier), OFDM (orthogonal frequency division multiplexing), and OFDMA (orthogonal frequency division multiple access). In addition, the standard also supports different PHY specifications (SC, OFDM, and OFDMA) for the

unlicensed bands. To support multiple subscribers, IEEE 802.16 supports both time-division duplex (TDD) and frequency-division duplex (FDD) operations.

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 PHYlayer, and it is also used for authentication and secure key exchange.

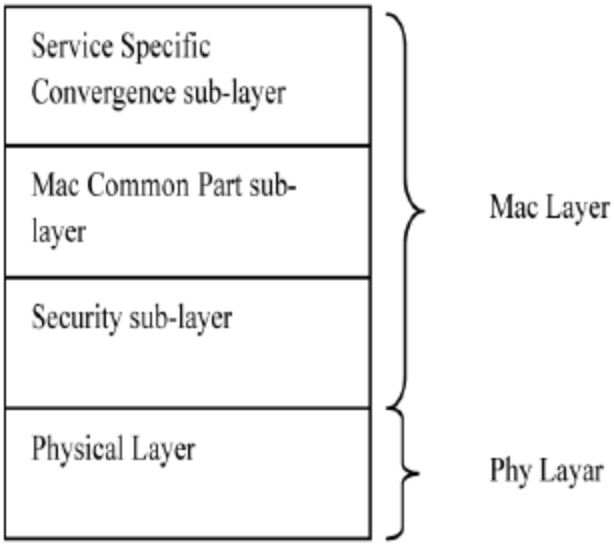

Figure 1. The IEEE 802.16 Protocol

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:

This sub layer basically performs three functions (or Phases): 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 based-on 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 [5].

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) [5].

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

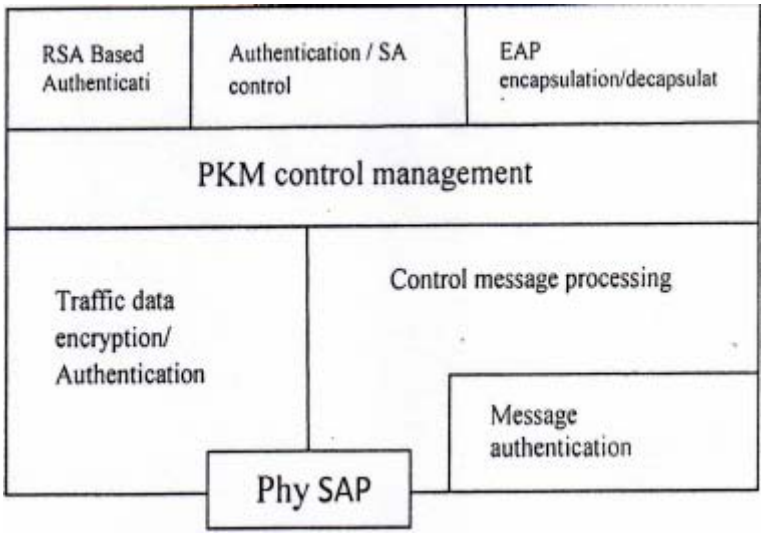

Figure 2. MAC Security sub-layer

2- Authorization: This process follows the authentication process.

Security of connections access in WIMAX is done with respect to the Privacy Key Management (PKM) protocol. PKM is responsible for the authorization of SS's and distribution of key material to them. In the first version of the IEEE 802.16 standard, the authorization protocol used in PKMv1 is basically 3 way handshake protocol between the SS and BS. The SS sends a message to BS, which contains an X.509 certificate (identifying the SS's manufacturer). BS is using this message in order to decide if the particular SS is a trusted device. 802.16 design defines that all devices from a trusted manufacturer can be trusted. SS sends a second message without waiting for an answer from BS. This second message contains the SS's X.509 certificate and its public key, the SS's Security capabilities and its SAID (Security Association Identity). The X.509 certificates are used for the BS to know if the SS is authorized. SS's public key is used by the BS to form the reply message. If BS determines that the SS is authorized then it replies with a third message, which initiates an SA (security association) between the BS and SS. BS generates Authentication Key (AK) which encrypted with the SS's public key, a 4-bit sequence number, used to distinguish between successive generations of AKs, the AK life time and a list of SAIDs which contains the identities and the properties of the SA list the SS authorized to access. If AK is used correctly, then SS gains the authorization to access the WMAN channel. The 802.16 designs assume that BS and SS share the secure AK.

The PKMv1 is shown as follows:

SS → BS: Mancert (SS);

SS → BS: SsCert, Capabilities, SAID;

BS → SS:{ AK}pk(Ss), SAIDlist, AKSeqn, AKlifetime

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 transmitted between SS and BS.

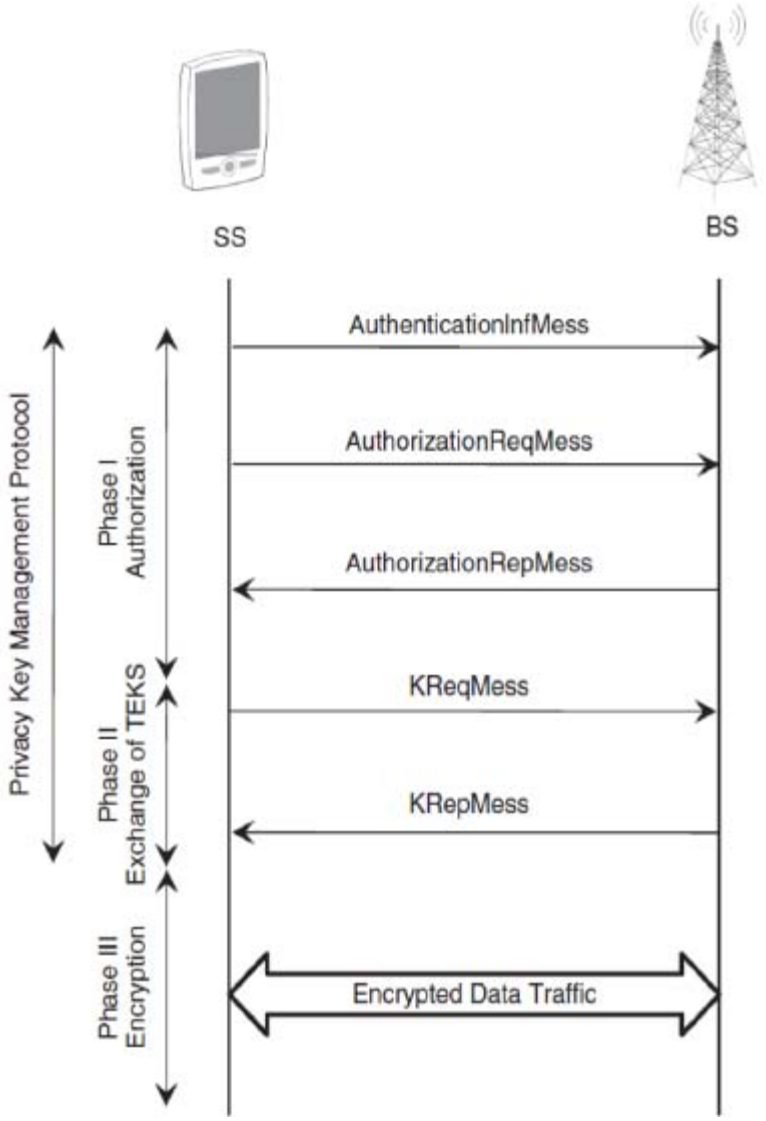

Figure 3. PKM Protocol phases

3. Literature Review

Few of relevant papers tackle the security issues of WIMAX network. T.Han and all [5], M.Rahman and M.Kowsar [7], M.Barbeau [8], M.Nasreldin and all [9], they give the most complete analysis of WIMAX security; they focused on the problem of IEEE 802.16.

The purpose of this literature review is to study the literature of WiMAX/802.16. The review is basically of security mechanisms for this technology and his security threats which are described in certain papers by different authors. Table 2 contains the tabular format of a summarized review of the literature. What are the challenges to the WiMAX and what are the solutions for these challenges. Every author has its own view.

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.

Author	Summary	Problems/Challenges	Solution
Michel Barbeau 2005 [8]	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 [9]	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 [5]	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 [7]	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 [12]	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 2. Summarized table of the review

4. Vulnerablities in Wimax

In this paper, we give also an overview of security scheme in IEEE802.16. We investigate man-in-the-middle, replay 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.

4.1 Physical layer threats

WIMAX/802.16 is vulnerable to physical layer attacks such as jamming and scrambling:

4.1.1 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 [10].

4.1.2 ***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 [5][6].

4.1.3 Water torture*:* is another kind of physical layer attack, is considered even more destructive than a typical Denial-of-Service (DoS) attack. This attack consists of sending a series of bogus frames in order to drain the SS's battery or consume computing resources. In this context, a suitable mechanism for detecting and discarding the bogus frames needs to be employed.

4.2 Mac Layer Threats

We analyze vulnerabilities contained in Mac layer and we categorize these weaknesses in the protocol into tree kinds: they are man-in-the-middle, replay and denial of service vulnerabilities.

4.2.1 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.

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 [5]. 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 it 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 [8].. 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 [6]

4.2.2 Replay Attack

The SS begins with an Authentication Information Message and a subsequent Authorization Request Message, with the aim to transmit all relevant information to the BS. The latter responds to the last message with an Authorization Reply Message. Although the message is transmitted in plaintext, it does not constitute a problem since the information is public anyway. However, the BS can fall victim to a replay attack by which the attacker intercepts an Authorization Request Message from an authorized SS and stores it. Even though he will not be able to derive the AK from the Authorization Response Message (since he does not possess the associated private key), he can repeatedly send the message to the BS, burdening the BS with the effect that this declines the real/authentic SS [13].

4.2.3 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 [11][14]. 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 [12]. 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 [14].

Sleep control messages: Mobile Wimax introduces sleep mode to minimize MS's (Mobil Subscriber) power usage and reduce usage of BS air interface resources. Sleep mode is a state in which an MS conducts pre-negotiated periods of absence from the BS air interface. The MS 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 MS [5]. As a result, the BS will stop transmitting messages to that MS, so performing a DoS attack.

Various vulnerabilities and possible attacks to WiMAX network have been discussed and illustrated. Wimax has security vulnerabilities in both layers. At PHY layers, jamming *and* scrambling can be considered as majors threats. At MAC layer, man in the middle, DoS and replay attacks. Some of these attacks have been fixed with the adoption of recent amendments and security solutions in IEEE 802.16 but some still exist and need to be considered carefully. In that case our responsibility also increase how we can provide maximum data rate with maximum security so we proposed an authentication protocol more reliable and secure.

5. The Proposed Revised Authendication Protocol

As discussed in the previous section, authentication protocol vulnerable to replay, DoS and Man-in-the-middle. Some solutions are introduced to solve those problems in our new revised protocol. To prevent replay and man-in-the-middle attacks we add timestamp. The problem with timestamp is that it requires time synchronization between MS and BS. In the wireless scenario, time synchronization is considered to be difficult (particularly under mobility). But In IEEE 802.16(e), it is assumed that time synchronization is done between MS and BS.

Nonce is a possible alternative to timestamps for use in the authentication protocols. Nonce shows that the request queued were not used before. Timestamp identifies which request are the newer one and also the time sent by the MS and BS.

Nonce will not give any information about the time that was sent. Nonce is also not sufficient to tell the BS that it is the current message received from the MS. There are two problems with the protocol that has timestamps only. An adversary can easily

capture the timestamp of MS by listening to message 2. The time adjustment can be done by the adversary accordingly. Hence the scope of man in middle attack is persists with timestamp added protocol. To prevent security threats like replay attacks, DoS attack and Man-inthe-middle attack, both nonce and time stamp are needed. So the revised protocol has the timestamp attached with the MS message to the BS along with the nonce.

5.1 The protocol is shown as follows

MS sends a message to BS, which contains an X.509 certificate identifying MS's manufacturer. BS is using this message in order to decide if the particular MS is a trusted device or not. MS sends a second message without waiting for an answer from the BS. This second message contains the MS certificate (MsCert) and a nonce (Ns1) used for identification, both are encrypted with the public key of the BS pk(Bs), it also contains the timestamp of MS and generated nonce of MS along with SAID and its security capabilities. MS signs the message ensuring the BS that he is not an adversary with his private key sk(MS), the time stamp addition could bring an extra layer of security since the BS could identify the message as current one. The time stamp could avoid the intruders who are trying to synchronize time with either BS or MS. If BS determines that the MS is authorized it replies with a message. BS sends a generated nonce along with nonce which was sent by the MS. That could ensure MS that message3 is the reply of the request send by MS itself. BS Nonce ensures the MS about the authentication of BS. This mutual authentication gives extra layer of security. BS sends a pre-AK encrypted with the secret key of BS sk(Bs), The AK is derived from Pre-AK. Use of Pre-AK gives the opportunity to avoid AK sending in raw format (though encrypted with the public key). From pre-PAK, the MS generates AK. If AK is used correctly, then MS gains the authorization to access the WMAN channel. The Lifetime of Pre-AK and Sequence no of pre-AK are sent in message3. This protocol using the public key of MS in message3 ensures MS that the message received is from a legitimate BS. As this message sends the BS certificate, the MS is now sure that the message is not copied by the adversaries.MS sends its Timestamp and the nonce of BS previously received to confirm authorization access in message4. MS signs the message with its private key.

The revised authentication protocol is shown as follows:

MS → BS:Mancert(MS);

MS → BS:{{MSsCert,Ns1}pk(BS),Capabilities, SAID,Tms,Ns}sk(MS);

BS → MS:{{prePAK}sk(Bs),SAIDlist,Tms,Tbs,

Ns,Nb,prePAKSeq,prePAKlifetime,BsCert}pk(MS);

MS → BS:{Nb,Tms }sk(MS);

In our proposal protocol, an adversary cannot obtain the unique pre-PAK. Timestamp and nonce are used in the revised protocol to prevent replay, DOS and man-in-the-middle attack. The MS appends the time stamp and nonce. This helps the BS to identify the request as a newer one. The nonce will wipe out the possibility of replay attack.

The nonce helps the BS to identify successive requests and it enhances the BS capacity to reject those requests which was sent by the intruders or adversaries so to prevent DOS attack.

BS, thus, can identify the latest requests and it is able to filter out samples of replay attacks. In stapes authorization reply message, the BS sends the timestamp and nonce of MS. That helps in preventing an adversary from forging a BS. This protocol also provides mutual authentication. The nonce value sent by the BS helps in preventing the man-in-the middle attack

.

The timestamp helps the BS in identifying the latest requests, which prevents reply attacks. It also helps the MS to identify the recent messages, and hence it can identify the AK used by the MS as new or not. The addition of nonce from the BS helps the MS to identify whether the message which he received with pre-AK is a newer one or not. It is better to add more buffers to carry the used nonce values in the previous sessions. This gives more security to the BS and user MS.

6. 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. In our part, a revised authentication protocol is proposed by using nonce and timestamp together. The new solution is efficient to tackling the various security threats such as replay, man in the middle and DOS attacks.

References

[1] 802.16. (2001) IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[2] 802.16a. (2003). IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2–11 GHz.

[3] 802.16. (2004). IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[4] Standard, I – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Band (2005).

[5] 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.

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

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

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

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

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

[11] 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.

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

[13] Evren Eren. (2007). WiMAX Security Architecture – Analysis and Assessment. IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 , Dortmund, Germany

[14] Deininger, A., Kiyomoto, S., Kurihara, J.,Tanaka, T. (2007). Security Vulnerabilities and Solutions in Mobile WiMAX. International Journal of Computer Science and Network Security. 7(11) 88–97.