An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile Wimax

Deepak Kumar Mehto, Rajesh Srivastava

Abstract— Security is amongst one of the major issues in Broadband Wireless Access (BWA) Networks. After the launch of the IEEE 802.16 standard (WiMAX), a number of security issues were reported in several articles. Ever since the beginning, work has been in progress for the neutralization of these identified threats. In this paper, the analysis of the authentication protocols implemented in WiMAX has been presented along with the description of the threats posed to them. An approach has also been presented for the prevention of these threats like the avoidance of replay; suppress replay and man-in-the-middle attacks. The proposed approach enhances the network security.

Index Terms— Mobile Wimax,Authentication , Privacy & Key Management.

I. INTRODUCTION

As much as the wireless networks have brought about major development in the way the information is shared between individual-to-individual, individual-to-business and business-to- business scenarios, they still face challenges, which are yet to be solved. 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: *Confidentiality*- Allowing only that the intended legitimate recipients to read encrypted messages (information). *Integrity* is referred to as ensuring that another party has not altered messages after it has been sent. *Authentication*- This is making sure that parties sending messages or receiving messages are who they say they are, and have the right to undertake such actions. On wired networks it has been exhaustively researched and there are many mechanisms available to provide confidentiality, integrity and authentication of information (CIA).

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. The major problem when securing the wireless signal is in its mode of transmission [1]. The wireless signal is transmitted through electromagnetic waves, which cannot be physically contained. Being communicated through the air makes them easy to intercept by anyone with the right equipment. WiMAX builds on the experience of security problems of 802.11 (Wi-Fi)wireless networks and was developed to solve most of the wireless LAN shortcomings especially security, and also quality of service, high-speed data rates and long distance connectivity coverage [2]. WiMAX (World-wide Interoperability for Microwave Access) also known as IEEE 802.16 is the BWA standard for Metropolitan Area Networks [13]. First published in 2002, 802.16 gives the specifications for the air interface allowing Point-to-Point and Point-to-Multipoint Broadband Wireless Access in the 10–66 GHz frequency band under LOS conditions [13]. In 2004, IEEE 802.16d was published to address the requirements of fixed BWA under NLOS conditions in 2–11 GHz [14]. An amendment to IEEE 802.16d was published to address the provision of mobility in 2005 under the title Mobile WiMAX or IEEE 802.16e which also operates in 2-11 GHz band under NLOS conditions [15]. The architecture of WiMAX is based on the MAC and PHY Layer. The MAC layer is further divided into three parts: convergence sub-layer, common-part sub-layer and privacy sub-layer [4]. Physical layer is divided into two parts: transport sub-layer and physical sub-layer [4]. The convergence sub-layer moulds the network layer packets into MAC Service Data Units (SDUs). Common part sub-layer implements the services of the MAC layer and transforms the SDUs to MAC Protocol Data Units (PDUs). The privacy sub-layer implements the security using two protocols: encapsulation protocol for encryption of payload and "Privacy and Key Management" protocol for distribution of keying data among network entities [12]. Two Versions of PKM have been implemented in WiMAX (PKM v1 & v2). Following are the PKM authentication methods [5]:

1) RSA based authentication: using X.509 certificates with RSA encryption.

2) EAP based Authentication (EAP-AKA/ EAP-TLS/ EAP-TTLS): using user credentials.

3) RSA-EAP: RSA based Authentication followed by EAP authentication.

The authentication phase arrives and is handled by the PKM protocol. Two versions of PKM protocol have been presented till date: PKM v1 and PKM v2. The PKM protocol basically manages the key distribution and exchange between SS and BS. For this purpose, X.509 digital certificates and RSA public-key encryption algorithm are utilized. The keys include Authorization Key (AK), Key Encryption Keys (KEKs) and Traffic Encryption Keys (TEKs).

Manuscript received May 30, 2011.

Deepak Kumar Mehto, M.E. (S.S.), ShriRam Institute of Technology, Jabalpur (M.P.), India, (e-mail: deepak_mtech@rediffmail.com**).**

Rajesh Srivastava, Asst . Professor, Comp. Sci. & Engg. Dept.,ShriRam Institute of Technology, Jabalpur(M.P.), India, (email: rajesh_5479@rediffmail.com).

II. BACKGROUND STUDY

The security of Fixed WiMAX was analyzed in several papers, especially in [16] where a lot of security vulnerabilities are outlined. With the publication of the Mobile WiMAX amendment, most of these vulnerabilities were solved. The security of IEEE 802.16e was only analyzed by a few papers, such as in [7] that examined the 3-way TEK exchange and the authorization process and could not find any security leak. Also [8] analyzed the key management protocol using protocol analyzing software and did not detect any problem. The multicast and broadcast service was examined in [9], by applying a protocol analyzing tool. He found out that security of the MBS is based on a few parameters which need to be implemented properly for complete protection. It is also pointed out that the interoperation with other protocols could be a security problem if these protocols have lower security characteristics.

III. MOBILE WIMAX (IEEE 802.16E)

The development of IEEE 802.16 was started by the IEEE in 2001. After that it was revised several times and ended in the final standard IEEE 802.16-2004 which is often called Fixed WiMAX [4]. This standard defines Wireless Metropolitan Broadband access for stationary and nomadic use. This means end devices can not move between base stations (BS) but they can enter the network at different locations. This specification was extended by the development of IEEE 802.16e which is known as Mobile WiMAX [12]. This standard supports mobility so that mobile stations (MS) can handover between BS while communicating. On the link layer, Mobile WiMAX introduces new features like different handover types, power saving methods and multicast and broadcast support. Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its predecessors [6]. It uses EAP-based mutual authentication, a variety of strong encryption algorithms and packet numbers to protect against replay attacks and reduced key lifetimes.

A. Initial Network Entry Procedure

For initial network entry, a MS has to pass some steps. The first step is to search for a downlink map message of the BS which is broadcasted periodically. This frame includes information about the initial ranging connection identifier (CID) which is associated with a timeslot in where the initial ranging process can be performed. Access to this common used timeslot is by standard random access channel. The MS then increases its transmission power with each ranging request it sends on the initial ranging slot until it receives a response from BS. This response includes ranging adjustments and the basic and primary management CIDs which reserve particular time intervals for the MS to send and receive management messages. After initial ranging is completed the basic capabilities for the connection are negotiated. Then the authentication process follows. IEEE 802.16e provides simple RSA-authentication or EAP-based authentication. EAP-based authentication includes higher layer authentication and therefore can be considered as the most secure method. After the authentication process, the MS and BS set up a common authorization key (AK). Then a key encryption key (KEK) is derived from the AK which is used to securely transfer further keys. Also the keys for message authentication in the uplink and downlink are derived from AK. After this, the 3-way TEKexchange for each data connection is executed. This means MS and BS exchange the keys which are finally used for data traffic encryption. Here, each message is integrity protected via a MAC digest and the transferred traffic encryption key (TEK) is encrypted by the KEK .

Key management: In the 3-way TEK exchange processed at initial network entry, the MS sets up a security association (SA) for each data communication it may wants to establish. Such a security association manages the keys for data encryption (TEKs), their lifetimes and other security related parameters of this connection.

Optional sleep mode: To save stations battery capacity and reduce the load on the channel, an optional sleep mode was defined in Mobile WiMAX. It allows the MS to be absent from the serving BS for certain time periods and may power down its transmitter. Therefore IEEE 802.16e specifies three different sets of power saving classes. Services with common demand properties should be mapped to the same set of power saving class. Each power saving class defines time periods when the MS should be in active state, listening for transmissions, and periods where it is allowed to change to sleep mode.

Multicast and Broadcast Service (MBS):

IEEE 802.16e alsointroduces a service for Multicast and Broadcast communications. This enables the BS to distribute data simultaneously to multiple MSs. To secure the broadcast communications, the IEEE 802.16e uses a common group traffic-encryption key (GTEK) for traffic encryption/decryption. Every group member must know this key. To share the GTEK between MS and BS, two algorithms are used: The mandatory key request/reply mechanism and the optional Multicast and Broadcast rekeying Algorithm (MBRA). In the standard request/reply mechanism a MS has to manage the GTEK update by itself. This means it has to request new keying material if the current key is going to expire. An optional alternative to distribute keying material is the Multicast and Broadcast rekeying algorithm (MBRA). Here the keys are managed by the BS. If a key lifetime is going to expire, the BS broadcasts one Key Update Command message to all MSs. This saves a lot of bandwidth as GTEKs are updated very frequently.

B. Security Flows in IEEE 802.16e

This section explains the flaws found in Mobile WiMAX. These flaws are analyzed as follows:

C. Unauthenticated Messages

Most of the management messages defined in IEEE 802.16e are integrity protected.

This is done by a hash based message authentication code (HMAC) [10], or alternatively by a cipher based message authentication code (CMAC) [11]. However, some messages are not covered by any authentication mechanism. This introduces some vulnerability. Also, a couple of management messages are sent over the broadcast management connection. Authentication of broadcasted management messages is difficult since there is no common key to generate message digests.

D. Unencrypted Management Communication

In Mobile WiMAX management messages are still sent in the clear. When a MS performs initial network entry, it negotiates communication parameters and settings with the BS. Here a lot of information is exchanged like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information and MS capabilities etc. Currently the complete management message exchange in the network entry process is unencrypted and the above mentioned information can be accessed just by listening on the channel. After initial network entry, the management communication over the basic and primary management connections remains unencrypted. Non-authenticated management messages sent on the primary or basic management connection can easily be authenticated using a HMAC or CMAC digit.

IV. ISSUES IN WIMAX

A. Privacy Protection

Privacy protection for mobile users during the roaming process has been in increasing concern for people that care their privacy. Given the open nature of radio media used in wireless access networks, privacy protection is even more meaningful and demanding in such an environment. A mobile user's privacy like movement pattern, network usage habit etc. should be protected from potential adversary intending to break user's privacy [3].

B. Interruption Attack

Interruption is an active attack on availability where an intruding entity blocks information sent from the originating entity to the destination entity. Examples are Denial of Service (DoS) attack and network flooding. DoS attack is an incident in which a subscriber is deprived of the service of a resource they would normally expect to have. A considerable amount of denial of service attacks implement across the Internet by flooding the propagation medium with noise and forge messages. The victim is overwhelmed by the sheer volume of traffic, with either its network bandwidth or its computing power exhausted by the flood of information. Almost all the DoS vulnerabilities in Mobile WiMAX standard are due to unauthenticated or unencrypted management messages. Here optional sleep mode is concerned.

Mobile WiMAX introduces an optional sleep mode to save the MS's power usage and decrease usage of BS air interface resources. It allows the MS to be absent from the serving BS for certain time periods and may power down its transmitter. These periods are characterized by the unavailability of the MS implementation of sleep mode is optional for the MS and mandatory for the BS.

V. ISSUES IN WIMAX

A. Simple authentication protocol

In this subsection, we smoothly apply the public-key cryptography based key-establishment technique to the 802.16 MAC protocol in the simple authentication. Simple means no real authentication for a user. The only modification to the 802.16e standard is a pair wise master key derivation function.

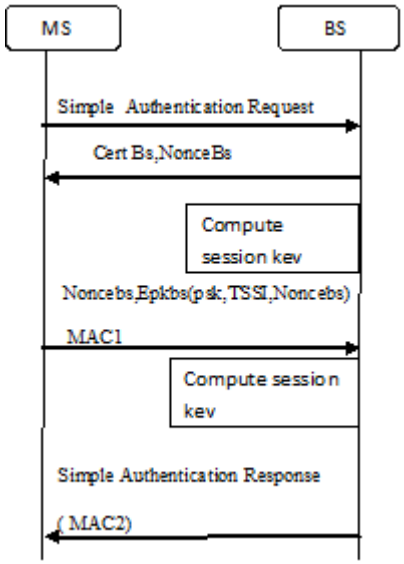

Fig. 1: Simple Authentication Process

In order for a mobile station to use simple authentication, a BS should indicate that it supports simple authentication in its ranging frames. The simple authentication key establishment protocol shown in Figure 2 is the following:

(1) A mobile station sends a simple authentication request to BS.

(2) The BS creates a random number NonceBS, and sends the MS a challenge message which consists of the BS's cert and NonceBS.

(3) The MS receives the BS's cert, verifies the correction of the cert, generates two random numbers as temporal subscriber station identity (TSSI) and pre-share key (psk), and derives temporal keys (pak, pair authentication key and pek, pair encryption key) as the formula (1) and (2) for protecting the succeeding messages, calculates EPKBS (psk, TSSI, NonceBS) by Public Key Encryption algorithm with BS's public key and MAC1 =HMAC (Pak,TSSI|| Noncebs) then sends the BS a response message which consists of NonceBS, EPKBS (psk, TSSI, NonceBS) and MAC1. (4) The BS firstly checks the freshness of NonceBS in the received message, then decrypts the message EPKBS (psk, TSSI, NonceBS) with its private key to obtain psk, TSSI and NonceBS, verifies the consistency of NonceBS in the message by comparing with that saved in local.

Then, BS derives temporal keys (pak, and pek) as the formula (1) and (2) for protecting the succeeding messages, calculates the MAC2 of simpleauthentication response message with the pak and sends the response to the MS.

B. Secure Initial Network Entry Process

The secure initial network entry process is shown in

Figure 2. It has the following stages:

(1) A mobile station sends a service request to the BS, which means the MS alleges that it is a legitimate subscriber.

(2) The BS responds the MS by the UL MAP message which contains the BS's cert and a random number NonceBS.

(3) When the MS receives the BS's cert, he regards the BS as supporting the simple authentication process, then calculates the MAC1 and sends the BS a message which consists of the selected ranging code, EPKBS(psk, TSSI, NonceBS) and MAC1.

(4) The BS handles EPKBS (psk, TSSI, NonceBS) and derives secret keys for the protection of the following messages, calculates the MAC2 of RNG-RSP message and sends the response to the MS.

(5) The MS verifies the correction of the MAC2 in the received message, if the result is valid, the shared key is established and the MS continue to communicate with the BS

Because of the authentication of the BS by the MS has been achieved during the secure initial network entry process, we only need authenticate the MS by the BS in the following Secure Authentication and Key Exchange process as PKM in the 802.16 standard. In order to defend the man-in-the-middle attack between two authentication processes, we advise to bind the previous psk to the PMK derivation process.

B. Key Derivation

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled. In the simple authentication protocol, a temporal pre-share key (psk) is generated to protect the frames exchanged before the EAP authentication is finished. In order to authenticate and encrypt frames with individual secret key, the pak and pek is derived as follows:

Pak : = Dot16KDF(psk,"auth'|| TSSI|| Noncebs,160)(1)

Pek: =Dot16KDF(psk, "enc" ||TSSI|| Noncebs,128)(2)

The key derivation algorithm Dot16KDF is defined in the 802.16 standard.

D. Privacy protection scheme

During the simple authentication process, a random number as a temporal subscriber station identity (TSSI) is assigned to MS. The station can protect its public identity (ids) by the couple <TSSI, pek> as follows:

Cids :=EAES(pek,ids)

The station encrypts its public identity (ids) by a symmetric cryptographic algorithm (such as AES) with the pek as secret key, which may be its certificate or ISMI in the USIM. Then, the station replaces its public identity with the couple of TSSI and cids during the EAP authentication process. Since the TSSI already sent to the BS during the simple authentication process, the BS can find the correct secret key (pek) to decrypt the cids and obtain MS's public identity (ids) by the index of TSSI when BS receives the authentication request message during the EAP authentication process.

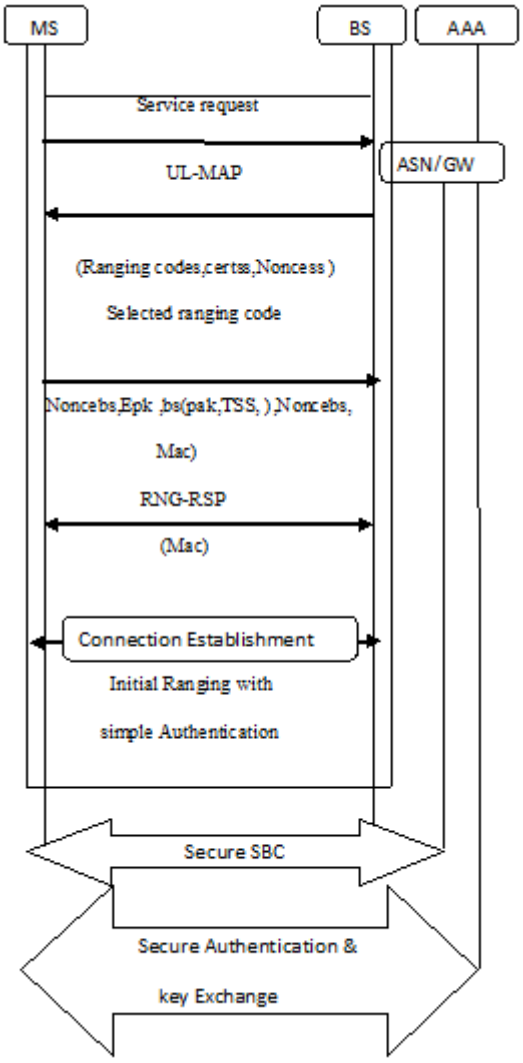

Fig 2 . Secure initial network entry process

E. Frame protection

The existing standard does not protect management and QoS frames, because there are no security schemes between the MS and BS for these frames before the EAP authentication is finished. However, we can apply the general protection scheme to protect these frames by calculating the MIC only. The random number in the previous message is treat as filed plaintext data, even though it is not in the resulting frame, i.e., in this case, even if there is no data to be encrypted, the MIC is different for each frame because of the changing NonceBS. This makes forging and replaying the management frames useless. The MIC only provides weak protection of integrity of both the header and data field of the IEEE 802.16 frame.

There are data protection schemes (for example, AES-CCM, CBC-MAC) in the 802.16e standard, but these protections can only be provided after successful EAP authentication. We can further extend them to data frames sent before and during the EAP authentication process using the temporal key derived in the above. EAP messages and (four-way) handshake messages can be protected by AES algorithm with the temporal key.

The sender encrypts the payload, adds the message integrity check code, and sends the resulting frame. The receiver then checks the originality and integrity of the frame and processes it after decryption.

VI. ANALYSIS AND DISCUSSION

Protocol security:

Because the proposed protocol is an optional supplement for the mobile WiMAX, it does not reduce the security of the original authentication protocol. Thus, we only analyze the security of the simple authentication protocol. The proposed protocol is a one way authentication process, which encrypts the temporal shared key with the BS's public key and protects the initial network entry process.

Freshness:

During the simple authentication process, the calculation of the session keys contains three random numbers which are psk, TSSI and NonceBS provided by the mobile user and the BS. Thus, the session keys are of freshness.

Consistency:

Because the BS and MS calculate the MAC of the messages with the pak derived from the session key and verify the integrity of the messages in the aftermost two messages, they achieve the agreement for the consistency of the session keys.

VII. CONCLUSION

This paper described the security mechanisms present in the WiMAX. We identify and analyze the security issues ignored by the current mobile wireless standard. In [6], the authors proposed completely new protocol for authentication and authorization process which requires complete modification to the standard.Then we propose an efficient simple authentication protocol based on public-key cryptography to address all these issues. Although based on a simple idea, the new method can provide mobile user privacy protection and enhance the security of mobile WiMAX networks.

REFERENCES

1. Griffin "Creating a Secure Network for Your Business", White-Paper, 2005. accessed on 24 June 2006
2. Panagiotis, T. and George, G. 2010. WiFi and WiMAX Secure Deployments," Journal of Computer Systems, Networks, and Communications, vol. 2010.
3. Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan," Analysis on Mobile WiMAX Security", IEEE TIC-STH 2009.
4. Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", Chapter 9: MAC Layer of WiMAX, Pearson Education Prentice Hall, 2007. ISBN (PDF) 0-13-222552-2
5. Yang, Y., and Li, R. 2009. Toward Wimax Security. In Proceedings of Computational Intelligence and Software Engineering, Wuhan, China, pp. 1-5.
6. Dong, H., and Yan, W. 2008. Secure Authentication on WiMAX with Neural Cryptography. In International Conference on Information Security and Assurance, 2008. ISA 2008, pp. 366-369.
7. Datta A., He C., Mitchell J.C., Roy A., Sundararajan M. "802.16e Notes, Electrical Engineering and Computer Science Departments, Stanford University, CA, USA, 2005,
8. Yuksel E. "Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling", Technical University, Denmark, DTU, 2007.
9. Ju-Yi Kuo, "Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol", Stanford University, CA, USA, 2006,
10. Krawczyk H., Ballare M., Canetti R. "HMAC: Key- Hashing for Message Authentication", RFC 2104, http://www.ietf.org/rfc/rfc2104.txt, IETF, 1997.
11. Dworkin M.: Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, NIST special publication 800-38B, National Institute of Standards and Technology (NIST), MD, USA, 2005.
12. Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)", School of computer and Information Science, Edith Cowan University, Australia, 2006. Shon, T., and Choi, W. 2007. An analysis of mobile WiMAX security: vulnerabilities and solutions. In Proc. Of the 1st International Conference on Network-based information systems, Regensburg, Germany, pp. 88-97.
13. IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, 802.16TM IEEE Standard for local and
14. metropolitan area networks," Part 16: Air Interface for Fixed Broadband Wireless Access Systems", June 2004.
15. IEEE Std. 802.16e/D12, "IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005.
16. D. Johnston and J. Walker, "Overview of IEEE 802.16 security", IEEE Security and Privacy, pp. 40–48, May/June 2004.

AUTHORS PROFILE

Deepsk Kumar Mehto: He is pursuing his M.E. from R.G.P.V. Bhopal in Software System. His area of research interest is wireless security & mobile computing.

Rajesh Shrivastava: He has completed his M.E. from R.G.P.V. Bhopal in Computer Science & Engineeting . His area of interest is security in mobile communications. He had published several research journals in international conferences. He is pursuing his P.hD. in mobile communication.