Security Enhencement & Solution for Authentication Frame work in IEEE 802.16

A.K.M. NAZMUS SAKIB

Chittagong University of Engineering & Technology

sakib425@yahoo.com

ABSTRACT

WIMAX- Worldwide Interoperability for Microwave Access is going to be an emerging wireless technology for the future. Wireless networking market is thriving because of increasing popularity of Broad Band internet. Wireless network is not completely secure because of rapid release of new technologies, lack of physical infrastructure and market competition. It is (WiMAX) a new technology; not deployed widely to justify the evidence of threats, risk and vulnerability in real situations. Although authentication process is a key to secure access in wireless network, the security sub layer of IEEE802.16 employs an authenticated client server key management protocol in which the Base Station (Server), controls the distribution of keying materials to the Mobile Station(the client). In this paper, an overview of authentication framework is first discussed and several threats on authentication process is later interrogated. Finally, possible solutions to overcome them are inaugurated.

KEYWORDS

Authentication, PKM, Time stamp, Hash, digital signature, visual cryptography

1. INTRODUCTION

WIMAX- Worldwide Interoperability for Microwave Access opens the door to thousands of applications that make use of the solid wireless backbone to connect people together. Due to high data rate, applications will include voice calls, video transfer and many other services. These types of applications will require a solid secure medium to exchange and operate information safely. This is what the IEEE decided to add to the WiMAX standard in its both versions - mobile and fixed broadband wireless access. WiMAX security process is divided into three steps:

01 .Authentication
02. Data Key exchange
03. Data Encryption

Authentication of users and equipments in the BWA network is done as part of the admission control process. The authentication phase is carried out while execution of handoffs in mobile BWA networks. The authentication and service authorization process is carried out at the privacy sub layer, embedded in the WiMAX protocol stack [2], [4]. A complete protocol ensuring secure distribution and management of keying data between network entities are incorporated in this layer, known as Privacy and Key Management protocol (PKM) [2]. Launch of 802.16d in 2004 and 802.16e in 2005 suggests that the standard is in the initial phase of implementation and several dormant issues and short comings will be highlighted with progress in deployment and service provisioning.

In this paper; I present different security vulnerabilities on authentication process and possible solutions to solve them. Rest of the paper is organized as follows: Section 2 introduces the existing authentication frameworks while section 3 describes the attacks on authentication. In Section 4, several possible solutions are presented and Section 5 accomplishes the topic.

DOI : 10.5121/ijcsit.2010.2607

2. AUTHENTICATION FRAMEWORK

2.1 Privacy & Key Management Protocol version 1

The PKM v1 protocol complies with the 802.16d-2004 standard and is operating in the Fixed WiMAX networks [2[. This protocol is a 3-step protocol which involving 1-way authentication. The figure 1 shows the PKM v1 authentication model and messages involved. The detailed operation of PKM v1 can be found in [2], [5] and [6]. PKM v1 is based on X.509 certificate based Public Key Infrastructure (PKI). Figure 1 shows the information flow between Subscriber Station and Base Station. The individual components of the message have been addressed in [2] and [6]. A nonce (NSS) is shown in Step 2 which is a 64-bit number generated randomly to be used as a message linking token [5]. Basic Connection Identity Code (BCID) is used to identify a particular node in the network .It is assigned to the node during the admission control process.

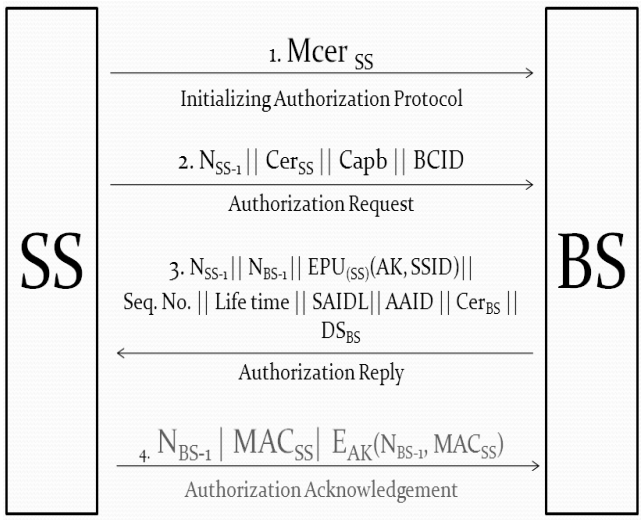

Figure 1: Privacy Key Management Protocol v1

2.2 Privacy &Key Management Protocol version 2

PKM v2 protocol was defined in 802.16e-2005 and is implemented in Mobile WiMAX networks [2]. This protocol is not essentially a variant of PKM v1. PKM v1 and v2 share a common service authorization structure. PKM v2 is a 4-step, 3-way authentication protocol. The operational mechanism of PKM v2 is illustrated in [3] and [7]. Figure 2 shows the PKM v2 authentication framework. The major enhancements in PKM v2 are the inclusion of digital certificates and authorization acknowledgement step. Except step 1, a nonce (NSS or NBS) has been incorporated with each message to link successive steps of the protocol.

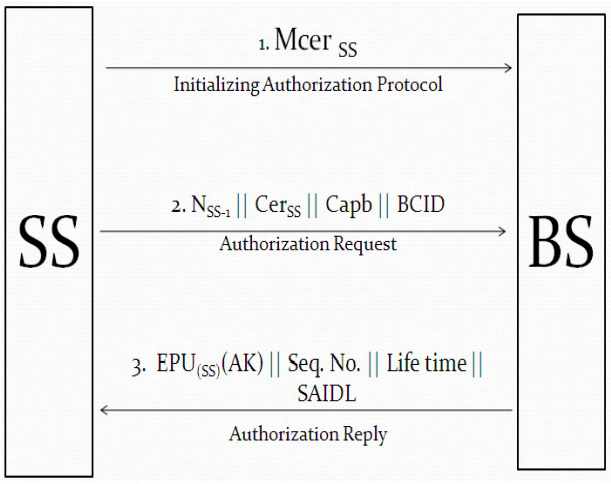

Figure 2: Privacy Key Management Protocol 2

3. ATTACK ON AUTHENTICATION

We can describe the Attacks on authentication by the way which a network can be intruded and the privacy of the users be compromised. The secure access of network services is becoming an important issue in the present communication infrastructures. Any attempts of an intruder to get registered with the network illegitimately or to create chaos in it, is possible; if the user authorization and authentication is compromised. The ways to breach the authentication frameworks are termed as attacks on privacy and key management protocols and their variants.

3.1 Water-Torture Attack

Water-Torture attack is aimed to perturb the network's operation by causing flooding. Some messages are used to initiate cyclic processes when received on any node. Transmission of such type of message can be seen in figure 2 and figure 1 as McerSS. McerSS is the manufacturer's X.509 certificate which is used by the Subscriber Station to show its presence in the network and to initiate the authentication protocol [6]. In the admission control process, the reception of this message at Base Station initiates the cyclic authentication procedure. In Water-Torture attack, these triggering messages are captured and are transmitted in a loop to cause trigger flooding thus, employing one-way authentication [13]. Time Stamping model and the PKM v1 model are vulnerable to this type of infringement attempt. The reason for this is one-way authentication i.e., Base Station authenticates Subscriber Station but vice versa does not occur. This attack is aimed to compromise the security of the users and poses severe threats in case of Employment of BWA infrastructure in security and defense installations for any realm.

3.2 Interleaving Attack

It is a sub-class of Man-in-the-Middle attacks and is specifically aimed for PKM v2. In this attack, an adversary interleaves a communication session by maintaining connections with the Base Station and Subscriber Station, pertaining as SS to BS and vice versa. All the information on route passes through the adversary node and thus an information leakage point is built [10]. Backbone of interleaving attack is the re-transmission of a set of messages from the same session. The HA model proposes an approach to cater the interleaving attack by introducing transmission and storage overheads in the network [8].

3.3 Suppress Replay Attack

This method of gaining forged access to the network services takes advantage of the fact that perfect synchronization must be maintained to protect the authentication session from intrusion [7]. Due to the loss of synchronization in the clocks of the entities, an intruder can gain control on the authentication framework by capturing the messages and transmitting them with added delays, thus causing forward message replay [7]. This class of attack is difficult to counter and it is also vulnerable for the Timestamp Authentication model. The Hybrid Authentication model is also manipulated by this attack.

3.4 Interception

It is a passive attack on confidentiality where an intruding entity is able to read the information that is sent from the source entity to the destination entity. We take eavesdropping and sniffing as an example of interception attack, in this attack; gathering information about the network (such as the SSID, the MAC address of the Access Point (AP), and information about whether WEP is enabled) is getting easier with the release of several products [4]. Interception can occur far outside the user's working range by using high-gain antennas (many of which are standard offerings from some vendors) [5].

3.5 Fabrication

It is an active attack on authentication where an intruder pretends to be the source entity. Fake e-mails and Spoofed packets are examples of a fabrication attack. Man-in-the-Middle Attacks is an example of fabrication, in order to execute a man-in-the-middle attack [14], two hosts must be convinced that the computer in the middle is the other host [6]. Spoofing, Brute-Force Password Attacks and Insertion Attacks are the examples of fabrication attacks [6].

3.6 Modification, Replay and Reaction Attacks

It is an active attack on integrity where an intruding entity changes the information that is sent from the source entity to the destination entity .The insertion of a Trojan horse program or virus is an example of a modification attack [7]. Virus Infection is another issue that affects both wireless and wired networks. Two of these are VBS/Timo-A and the LoveBug [7]. Replay is an active attack on integrity where an intruding party resends information that is sent from the source entity to the destination entity [7]. Examples of Replay attacks are Traffic Redirection, Resource Stealing and Invasion. Reaction is an active attack where packets are sent by an intruder to the destination and the intruder monitors the reaction [7].

3.7 Interruption

It is an active attack on availability, where an intruding entity blocks information sent from the originating entity to the destination entity. Examples are DoS attacks and network flooding. The intruder may try to exhaust all network bandwidth using ARP flooding, ping broadcasts, Transmission Control Protocol (TCP) SYN flooding, queue flooding, smurfs, synk4, and other utilities [6] Examples of Interruption Attack are Denial of Service attacks and Rogue Networks. Rogue Networks and Station Redirection a rogue AP is one owned by an attacker that accepts station connections and then intercepts traffic and might also perform man-in-the-middle attacks before allowing traffic to flow to the proper network[6]. The goal of a rogue is to move valid traffic off the WLAN onto a wired network for attacking (or to conduct the attack directly within the rogue AP) and then reinsert the traffic into the proper network [3].

3.8 Denial of Service attack

DoS attacks such as unprotected network entry, unprotected management frame, unencrypted management communication, weak key sharing mechanism in multicast and broadcast operations and Reset-Command message [13]. Some DoS attacks are include the following:

DoS attacks based on Ranging Request/Response (RNG-REG/RNG-RSP) messages:

This attacker can forge a RNG-RSP message to minimize the power level of M.S to make M.S hardly transmit to BS, thus triggering initial ranging procedure repeatedly. An attacker can also perform a water torture DoS by maximizing the power level of M.S, effectively draining the M.S's battery [14].

DoS attacks based on Mobile Neighbor Advertisement (MOB_NBR_ADV) message:

MOB_NBR_ADV message is sent from serving B.S to publicize the characteristics of neighbor base stations to M.Ss searching for possible handovers [14]. This message is not authenticated. Thus it can be forged by an attacker in order to prevent the M.Ss from efficient handovers downgrading the performance or even denying the legitimate service [14].

DoS attacks based on Fast Power Control (FPC) message:

FPC message is sent from B.S to ask a M.S to adjust its transmission power [14]. An attacker can intercept and use FPC message to prevent a M.S from correctly adjusting transmission power and communicating with the B.S. He can also use this message to perform a water torture DoS attack to drain the M.S's battery.

DoS attacks based on Authorization-invalid (Auth-invalid) message:

The Auth-invalid is sent from a B.S to a M.S when AK shared between BS and M.S expires or B.S is unable to verify the HMAC/CMAC properly [13]. This message is not protected by HMAC and it has PKM identifier equal to zero and it can be used as DoS tool to invalidate legitimate SS.

DoS attacks based on Reset Command (RES-CMD) message:

This message is sent to request a M.S to reinitialize its MAC state machine, which allows a B.S to reset a non-responsive or mal function M.S. This message is protected by HMAC but is still potential to be used to perform a DoS attacks. In order to prevent DoS attacks, first need to fix the vulnerabilities in the initial network entry & secure authentication technique [13].

3.9 Man In The Middle Attack:

A simple man-in-the-middle attack toward this protocol is described in following Figure:

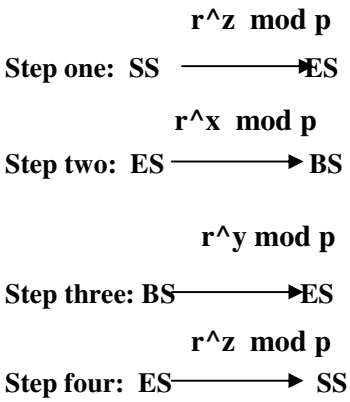

Figure : Man-In-the-Middle attack

Victim SS's public key *PKss* is captured by Evil Station (ES). The ES camouflages as SS and sends its own public key *PKES* to BS, then the severing BS sends back its public key *PKBS*, at this time, the ES could establish a shared key with BS. Finally, ES sends its own public key *PKES* to victim SS, and establishes a shared key with SSe [14]. Consequently, all the messages that the victim SS sends to BS are relayed by ES and the encryption keys are known by ES. Thus, ES could eavesdrop and tamper all these messages. To resist man-in-the-middle attacks in this procedure we need a secure authentication process.

4. PROPOSED SOLUTIONS

4.1 Secure Authentication process by using Timestamp model

Time stamping (T.S) is the process of securely keeping track of the creation and modification time of a document. Here security means that once the document has been recorded, no one can be able to change it, provided that the time stamper's integrity is never compromised. The technique is based on hash functions and digital signature. First a hash is calculated from the data which is aA hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed, hash will also change. Anyone trusting the time stamper can then verify that the document had not been posed after the date that the times tamper vouches and also it can no longer be repudiated that the requester of the time stamp was in possession of the original data at the time given by the time stamp.

Steps are given bellow:

1. M.S sends communication request to B.S.

2. B.S generates the hash (H1) of the data & sends it to the M.S.

3. M.S now adds the T.S to H1 and generates hash H2.Then H2 is encrypted with the private key of M.S. Now encrypted H2 and T.S of M.S are to be sent to B.S.

4. B.S has to add its data with the T.S of M.S and to generate hash H3. Now H2 (Which was encrypted by private key of M.S) should be decrypted by the public key of M.S. If H3=H2 then further communication is continued, otherwise the communication should immediately be ceased.

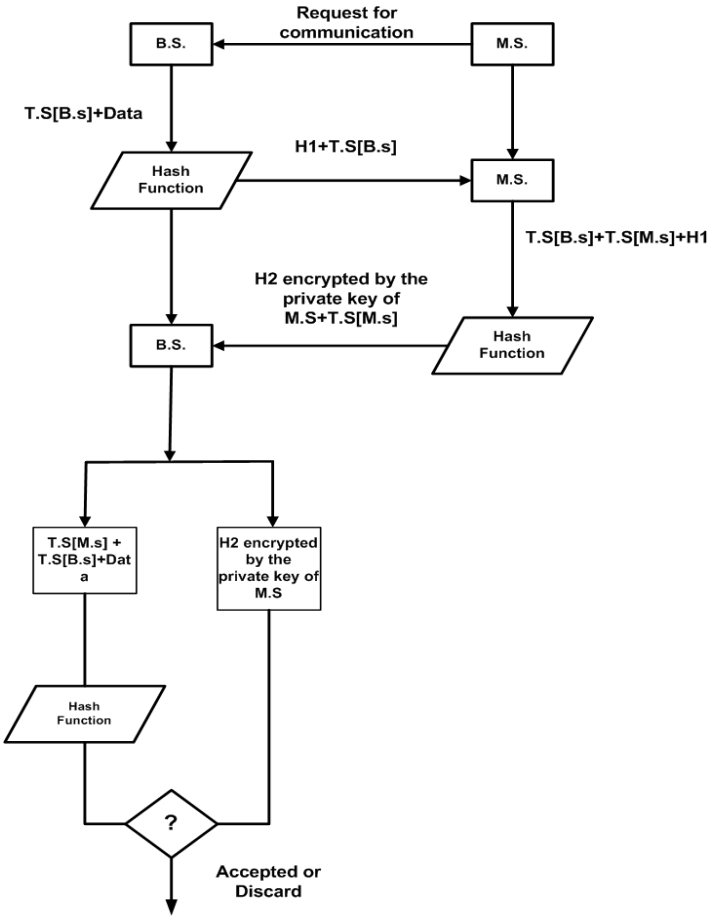

Figure 3: Secure Authentication process by using Time Stamp model

4.2 Hashed based Authentication Model:

The steps are as follows:
Step1: M.S requests for communication and sends out a string as a challenge to B.S.
Step2: B.S. also sends out a string as a challenge to M.S.
Step3: M.S. calculates the message digest of the string by applying hash algorithm and sends the challenging string value and its ISSI number to B.S.
Step4: B.S. also calculates the message digest for the corresponding string and send to the M.S. Only the legitimate B.S. and M.S. know the hash algorithm. But the evil M.S. is not able to produce correct value for the given string. Now B.S and M.S compare the corresponding message digest value. If it matches then farther communication is continued. Otherwise, the communication should immediately be ceased**.** This is illustrated in figure 4.

4.3 Hybrid Authorization (HA) Model:

Ayesha Altaf et al., in [7], propose a model which employs a hybrid approach involving time stamps and nonce to prevent the attacks on privacy and key management protocols. This proposal claims to cater the effect of interleaving attacks discussed in [8] and [9] which may occur on PKM v2. The approach is presented for mobile WiMAX networks and enhances the PKM v2 authentication framework [8]. Hybrid authentication model is described in figure 5.

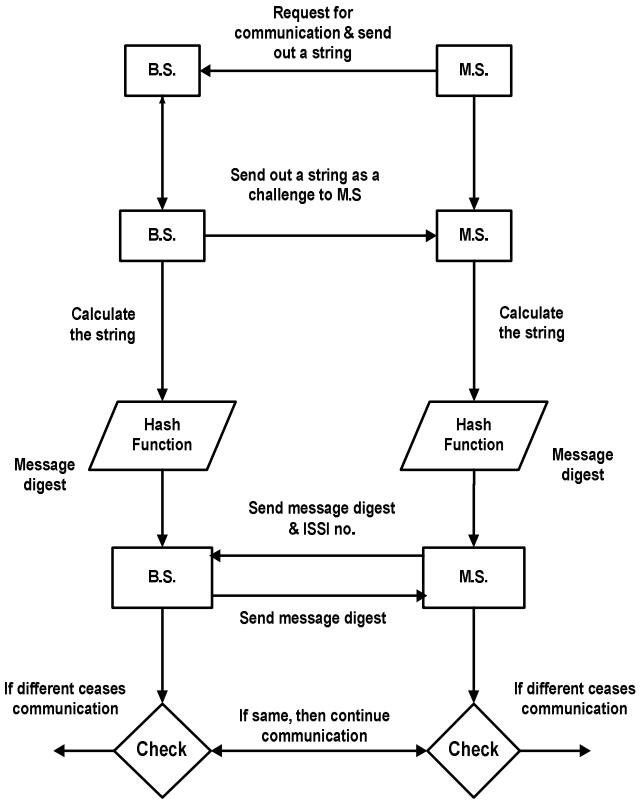

Figure 4: Hashed based Authentication model

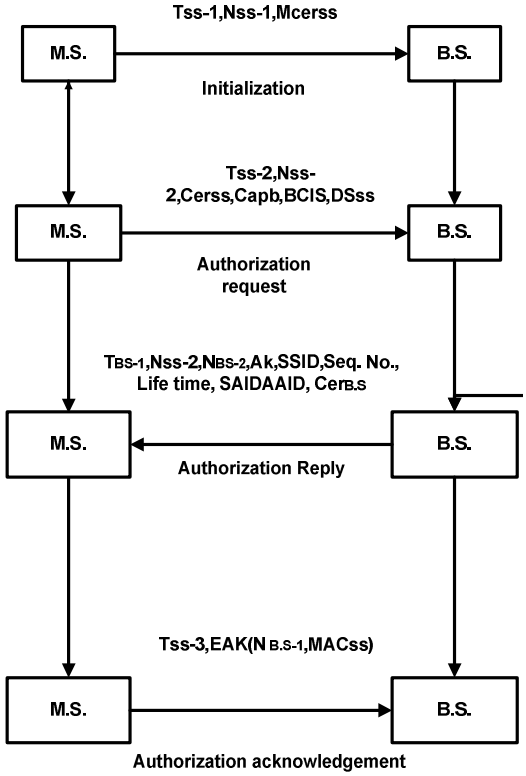

Figure 5: Hybrid Authentication Model

4.4 Authentication process by using Visual Cryptography:

Moni Naor and Adi Shamir is the pioneer of visual cryptography. They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image. While any *n-1* shares revealed no information about the original image. Each share was printed on a separate transparency and the decryption was performed by overlaying the shares. When all *n* shares were overlaid, then the original image would appear. It involves secret sharing with images. Any secret data is taken in the form of image which is a collection of black and white pixels. This image is encoded into *n* random looking images called shadows or shares one for each participant. The secret can only be recovered when *k* or more participants stack their shares together whereas any *k-1* participants' shares reveal no information about the image when stacked. By using visual cryptography how secure authentication can be achieve is describe as follows:

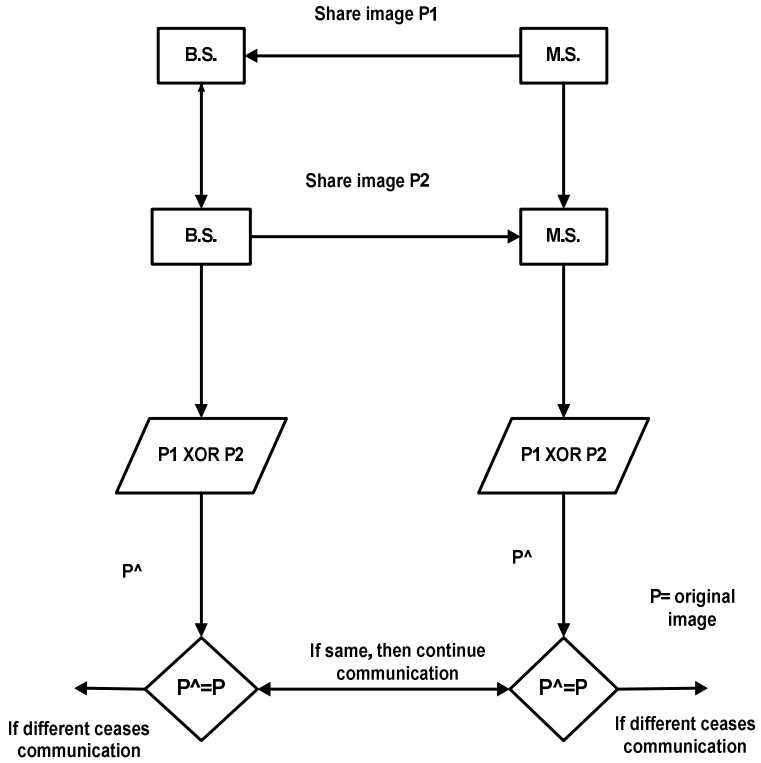

Figure 6: Authentication process by using visual cryptography

4.5 Authentication process using Digital Signature:

A digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and it cannot be altered in transit. Although messages may often include information about the entity sending a message and that information may not be accurate. Digital signatures can be used to authenticate the source of messages and when ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. How secure authentication can be achieved by using digital signature is describe as follows:

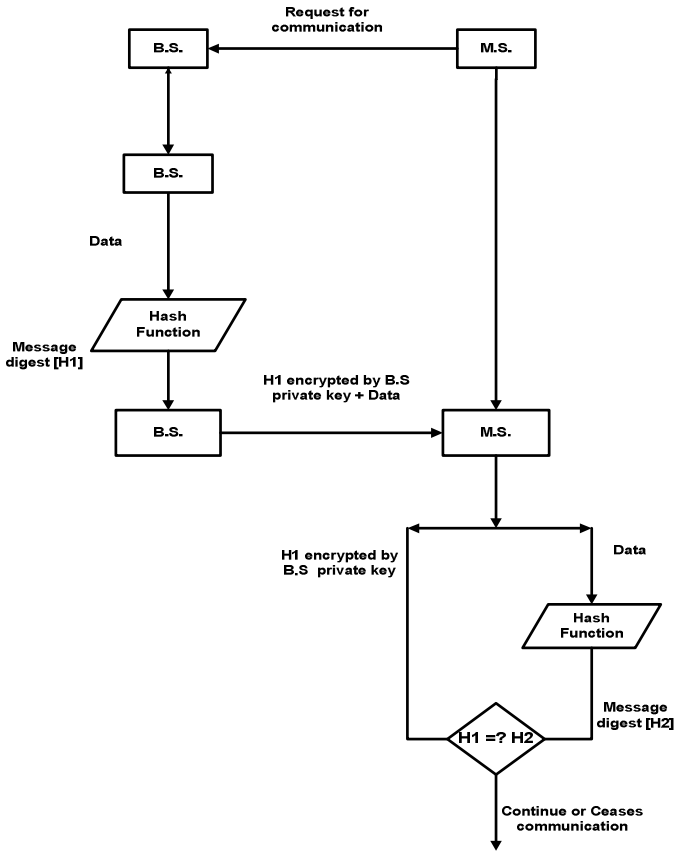

Figure 7: Secure Authentication process using Digital signature

5. CONCLUSION

The IEEE 802.16e based WiMAX network provides better security architecture as compared to 802.16d and basically secures the wireless transmission using different components such as X.509 certificates, PKMv2, the security associations, encryption methods and the encapsulation protocol. However, it still lacks complete security solution due to certain unsecured MAC management messages and several attacks on authentication protocol. Moreover, the mess network is not analyzed clearly. In this paper I present several solutions related to the authentication vulnerability based on time stamping, hash function, digital signature, Hybrid (Time stamp and Nonce) and visual cryptography.

In WiMAX, both layers are attacked by the threats. Interleaving and Man-In-The-Middle attack are considered as the major threats to PHY layer while eavesdropping of management messages, masquerading, management message modification or DoS attacks are treated as principal threats to MAC layer. Some of these issues have been fixed with the adoption of recent amendments and security solutions in IEEE 802.16 but some still exist. Which need to be considered carefully. WiMAX does offer much more strong security solutions in comparison with other wireless technologies such as Bluetooth or Wireless Fidelity; but it is still under development and need more research on its security vulnerabilities.

REFERENCES

[1] A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, "IEEE 802.16e Security Vulnerability : Analysis & Solution" October 2010, Volume 10 Issue 13 Version 1.
[2] IEEE Computer Society and the IEEE Microwave Theory and Techniques Society," 802.16TM IEEE Standard for local and metropolitan area networks," Part 16: "Air Interface for Fixed Broadband Wireless Access Systems", June 2004.

[3] 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.

[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] R. M. Hashmi et, "Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16", Proceedings of 3rd IEEE International Conference on Information and Communication Technologies, August 2009.

[6] Sen Xu,Manton Matthews, Chin-Tser Huang. "Security issues in privacy and key management protocols of IEEE 802.16",44th annual Southeast regional conference, pp. 113-118, ISBN 1- 59593-315-8, 2006.

[7] Ayesha Altaf, M. Younus Javed, Attiq Ahmed, "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005", 9th ACIS International Conference on software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 335-339, 2008.

[8] Sen Xu,Chin-Tser Huang,"Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions", Computer Science and Engineering Department, University of South Carolina, Columbia, September, 2006.

[9] Gavin Lowe,"A Family of Attacks upon Authentication Protocols", Department of Mathematics and Computer Science, University of Leicester, January 1997.

[10] Michel Barbeau,"WiMax/802.16 Threat Analysis", School of Computer Science Carleton University, Ontario, Canada, October 2005.

[11] Hao Zhou, Amaresh V. Malipatil and Yih-Fang Huang "Synchronization issues in OFDM systems", Circuits and Systems, IEEE-APCCAS, pp. 988 – 991, 2006.

[12] Li Gong ,"A Security Risk of depending on Synchronized Clocks", ORA Corporation and Cornell University, September 24, 1991. David Johnston, Jesse Walker, "Overview of IEEE 802.16 Security," IEEE Security & Privacy, June 2004.

[13] Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Anand Srinivasan," Analysis on Mobile WiMAX Security", IEEE TIC-STH 2009.

[14] Mir Md. Saki Kowsar, Muhammad Sakibur Rahman: WiMAX Security Analysis and Enhancement,Department of Computer Science and Engineering Chittagong University of Engineering and Technology Chittagong-4349, Bangladesh.

Authors

A.K.M. NAZMUS SAKIB
B.Sc in Computer Science & Engineering;
Chittagong University of Engineering & Technology;
Bangladesh.
Email: sakib425@yahoo.com,sakib425@gmail.com
Research area: Wireless security