A.K.M. NAZMUS SAKIB, Tanvir Mahmud, Mountain Munim, Samiur Rahman, Muhammad Mushfiqur Rahman/ International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.490-496

Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties

A.K.M. NAZMUS SAKIB[1], Tanvir Mahmud[2], Mountain Munim[3], Samiur Rahman[4], Muhammad Mushfiqur Rahman[5]

[124](Department of Computer Science & Engineering, Chittagong University of Engineering & Technology, Bangladesh)
[3](Programmer, Affiliation: Bangladesh Computer Society, Bangladesh)
[5](United International University, Dept. of CSE, Bangladesh)

ABSTRACT

Many sophisticated authentication and encryption techniques have been embedded into IEEE 802.16 but it still facing a lot of challenging situations. 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 (client) . In this paper, an overview of security scheme of IEEE 802.16 is present. We identify different security vulnerability that found in initial network entry process. Also, we proposed secure authentication framework by using different function library & cryptographic properties like digital signature, digital envelope.

Keywords – Authentication, Key exchange, WiMAX, DoS, Digital Signature, Digital Envelope, Function

I. INTRODUCTION

1. Introduction

The Mobile WiMAX system based on the IEEE 802.16 include more improved security features than previous IEEE 802.16d-based WiMAX network system [2] . Almost all the security issues in Mobile WiMAX are considered in security sub-layer and are shown in Fig 1.

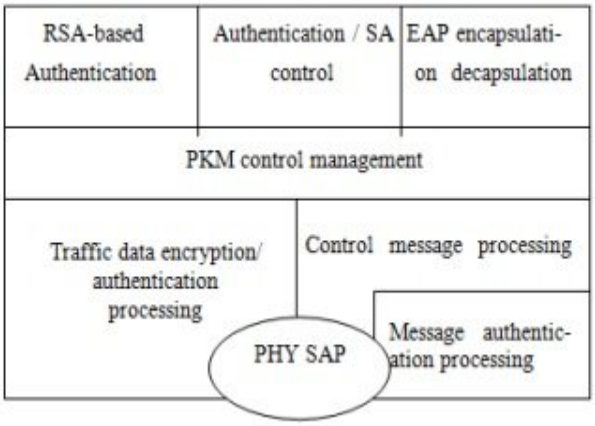

Figure 1: security sub-layers

The security sub-layer encompasses three essential functions: authentication, authorization & encryption [1]. The PKM protocol uses, strong encryption algorithm and RSA public key algorithm, X.509 digital certificates, to carry out key exchanges between B.S and M.S [2][3] . This Privacy protocol has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC [2][3]. The main purpose of the privacy sub layer is to protect service providers against theft of service, rather than guarding network users. Privacy sub layer is above the physical layer, so it only guards data (data link) But does not protect physical layer from intercepted. But It is very much important to secure the physical layer.

2. Initial network entry process

Initial network entry contains four processes: initial Ranging process, M.S Basic Capability negotiation process, PKM authentication process and registration process [2] . It is the most security sensitive processes in IEEE 802.16 [WiMAX] network not only because it is the first phase to establish a connection to the network, but also because many parameters, performance factors and security contexts between B.S & serving M.S are determined during this process [2]. The initial network process is illustrated in Figure 2. After initial network entry, the management communication remains unencrypted [2] and all management information exchanged between B.S & M.S can be accessed by a adversary [2]. The only messages which are encrypted are key transfer messages. But in this case only the key is encrypted, all other information is still sent in the clear. An intruder collecting management information can create detailed profiles about M.S's including capabilities of devices, security settings, associations with base stations & all other information described above[2]. Using the data offered in power reports, registration, ranging and handover messages, an attacker is able to determine the movement and approximate position of the M.S as well. Monitoring the MAC address sent in ranging or registration messages reveals the mapping of connection identifier (CID) and MAC address, making it possible to clearly relate the collected information to user equipment [2].

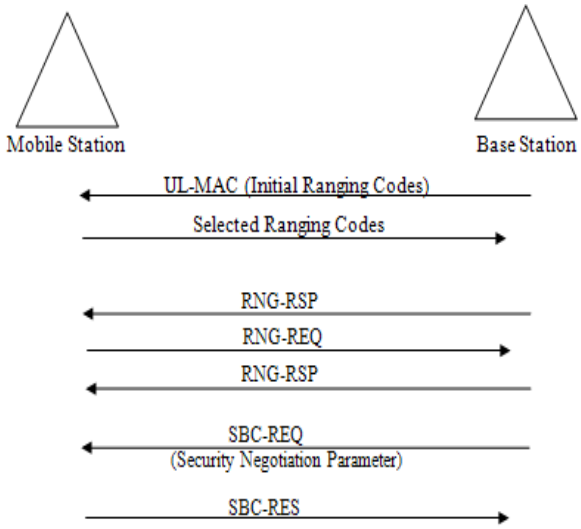

Figure 2: WiMAX initial network entry procedure

3. Vulnerabilities in IEEE 802.16e

This section explains vulnerabilities found in Mobile WiMAX by analysis. These vulnerabilities are:

3.1 Unauthenticated messages

There are some unauthenticated Messages include in Mobile WiMAX. Their forgery can interrupt or constrict the communication between M.S and B.S [2] [3]. First it has to be mentioned that a couple of management messages are sent over the broadcast management connection. Broadcasted management messages authentication is difficult since there is no common key to generate message digests. A common key would not completely protect the integrity of the message as M.S sharing the key can forge these messages and generate valid authentication digits [2][3].

3.2 Initial network entry vulnerability

3.2.1 RNG-RSP vulnerability

In RNG-RSP vulnerability, the attacker modifies the RNGRSP message and sets the status as failed and re-sends it to M.S [2][5]. So the M.S has to go for initial ranging again. If the attacker continuously sets the RNG-RSP status as failed, it (M.S) accesses the

network. This leads to the DoS attack. This RNG-RSP vulnerability is solved by Diffie-Hellman (D-H) key agreement [2][5], which is discussed in the later part of this thesis.

3.2.2 Auth-Request vulnerability

In Auth-Request and Invalid vulnerability, the intruder captures the auth-request message and re-sends it to B.S continuously [4]. So the B.S is confused with the continuous request and sets the Auth-Response as failure. Some time the attacker may captures Auth-Response message from B.S and re-sends to M.S [5][4]. This issue can be solved by either introducing time stamps model. By adding time stamp, B.S and M.S identifies if the authorization message is proper [4]. So the attacker unable to modify the messages.

3.2.3 Rogue BS

For rogue BS attack, the M.S cannot verify that any authorization protocol messages it receives were generated by an authorized B.S. So any rogue BS can create a response [4]. To solve this issue; the M.S has to authenticate to the B.S.

3.3 Denial of Service attack (Dos)

DoS attacks such as unprotected network entry, unprotected management frame, weak key sharing mechanism in multicast & broadcast operations, unencrypted management communication and reset-command message [5][4]. Some DoS attacks are include the following:

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

An intruder can forge a RNG-RSP message to minimize the power level of M.S to make M.S hardly transmit to B.S, thus triggering initial ranging procedure repeatedly [4][5]. An intruder can also perform a water torture DoS by maximizing the power level of M.S, effectively draining the M.S's battery [4].

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

This message is sent from serving B.S to publicize the characteristics of neighbor base stations to M.Ss searching for possible handovers [4][5]. This message is not authenticated and 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 [4].

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

This message is sent from B.S to ask a M.S to adjust its transmission power [5]. This is also one of the management messages which are unprotected. An intruder 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 [4] [5].

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

The Auth-invalid is sent from a B.S to a M.S when Authorization key (AK) shared between B.S and M.S expires or B.S is unable to verify the CMAC/HMAC properly [4][5]. This message is unprotected by HMAC and it has PKM identifier equal to zero [4][5]. Thus, it can be used as DoS tool to invalidate legitimate M.S.

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

This message is sent to request a M.S to reinitialize its MAC state machine, it allows a B.S to reset a non-responsive or malfunction M.S [4]. This message is protected by HMAC but is still potential to be used to perform DoS attacks [4].

4. Solution Suggested

4.1 Secure Authentication process

The steps are as follows (Fig 3) :

Step 1.	MS request for communication & send out a number as a challenge to B.S.

Step 2.	BS also sends out a number as a challenge to MS.
Step 3.	MS calculates the value of the number by applying function and sends the challenging value and its ISSI number to BS.
Step 4.	BS also calculates the value for the corresponding number & send to the M.S. Only the legitimate BS & M.S knows the function. But the evil MS is not able to produce correct value for the given number. Now B.S & M.S compare the corresponding value. If it match then continue farther communication .Otherwise, ceases the communication immediately**.**

Function Generation Process

To use function as a seal or mark of an authenticate M.S [4]; a process must be needed to generate unique functions for a large numbers of SS under each vendor. Although, there are infinite numbers of functions but it must be assigned in a systematic way to ensure that each M.S gets a unique function. A systematic way of generating functions for 10,000 M.Ss is described as follows:

Suppose a vendor wants to assign such functions to 10,000 M.Ss. For that the vendor makes a table for functions which consists C =5 columns and each column has R =100 functions of same characteristics. So there are total (C×R) =50 functions in the table. Now, the vendor will assign a function to a M.S by combining two functions of two columns. So, there are total $R^2 \times \{C (C-1)\}/ 2$ =100,000 numbers of possible functions are available to use. This process is explained in the following example

Table:1

Polynomial Function	Log Function	Trigonometric Function	Exponential Function
$X^{12}+3X$	Log2X-33X	Cos5X/2	e^{5X+44}
190X +1/X	$2X^{11}+LogX$	Sin2X -21X	$e^{X}+e^{1/X}$
$X^3/5X$	$X^3/123Log2$	Tan33X- X^2	$e^{44X+177}$
$44/X^{12}$	Log4X-230	2SinX +33TanX	$1/e^{x}$
X^2 - 1X+55X	$3+LogX^2$	CotX –Sec2X	$e^{\sqrt{X}}$

4.2 Digital Envelope

Digital signatures are computed based on the documents (information) that need to be signed and on some private information held only by the sender.

In practice, instead of using the whole message; a hash function is applied to the message to obtain the message digest. A hash function, in this context; takes an arbitrary-sized message as input and produces a fixed-size message digest as output. Among the commonly used hash functions in practice are MD-5 (message digest 5) & SHA (secure hash algorithm). These algorithms are fairly sophisticated & ensure that it is highly improbable for two different messages to be mapped to the same hash value. There are two broad techniques used in digital signature computation— symmetric key cryptosystem and public key cryptosystem (cryptosystem broadly refers to an encryption technique). In the symmetric key system; a secret key known only to the sender and the legitimate receiver is used. There must be a unique key between any two pairs of users. Thus, as the number of user pairs increases; it becomes extremely difficult to generate, distribute & keep track of the secret keys. A public key cryptosystem, on the other hand, uses a pair of keys: a private key, known only

to its owner and a public key; known to everyone who wishes to communicate with the owner. For confidentiality of the message to be sent to the owner, it would be encrypted with the owner's public key; which now could only be decrypted by the owner; the person with the corresponding private key. For purposes of authentication, a message would be encrypted with the private key of the originator or sender, who we will refer to as B.S.

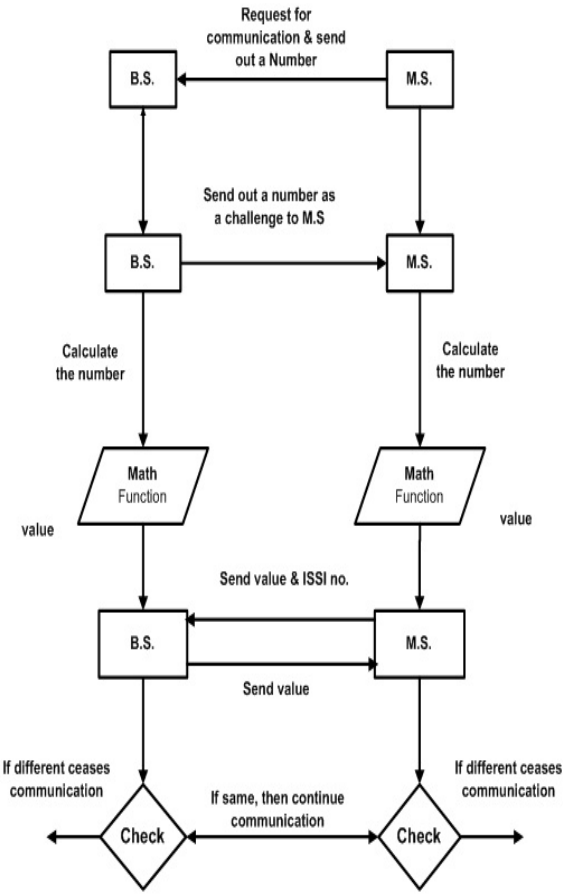

Figure 3: authentication in secure way

This message could be decrypted by anyone using the public key of B.S. If this yields the proper message, then it is evident that the message was indeed encrypted by the private key of B.S and thus only B.S could have sent it.

4.3 Creating and verifying a digital signature

A simple generic scheme for creating and verifying a digital signature is shown in Figs. 4 and 5, respectively. A hash function is applied to the message that yields a fixed-size message digest.

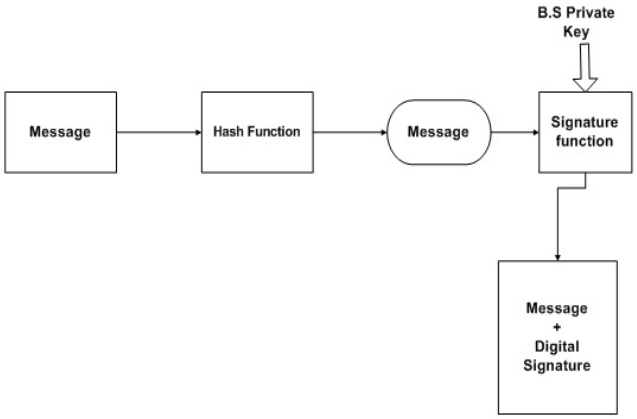

Figure 4: creating a digital signature

The signature function uses the message digest and the sender's private key to generate the digital signature. A very simple form of the digital signature is obtained by encrypting the message digest using the B.S's private key. The message and the signature can now be sent to the recipient. The message is unencrypted and can be read by anyone. However, the signature ensures authenticity of the B.S (something similar to a circular sent by a proper authority to be read by many people, with the signature attesting to the authenticity of the message). At the M.S end, the inverse signature function is applied to the digital signature to recover the original message digest. The received message is subjected to the same hash function to which the original message was subjected. The resulting message digest is compared with the one recovered from the signature. If they match, then it ensures that the message has indeed been sent by the (claimed) B.S and that it has not been altered.

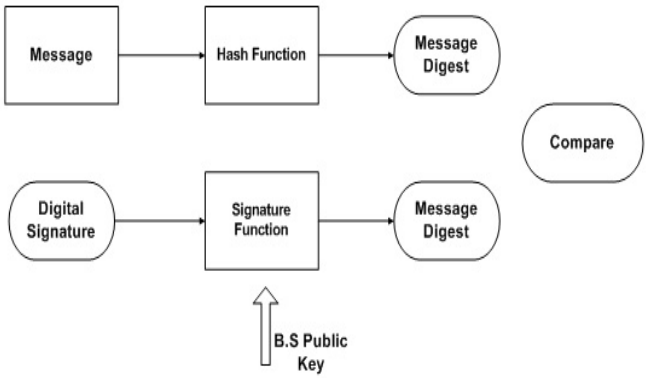

Figure 5: verifying a digital signature

4.4 Creating and opening a digital envelope

A digital envelope is the equivalent of a sealed envelope containing an unsigned letter. The outline of creating a digital envelope is shown in Fig. 6. The message is encrypted by the sender using a randomly generated symmetric key.

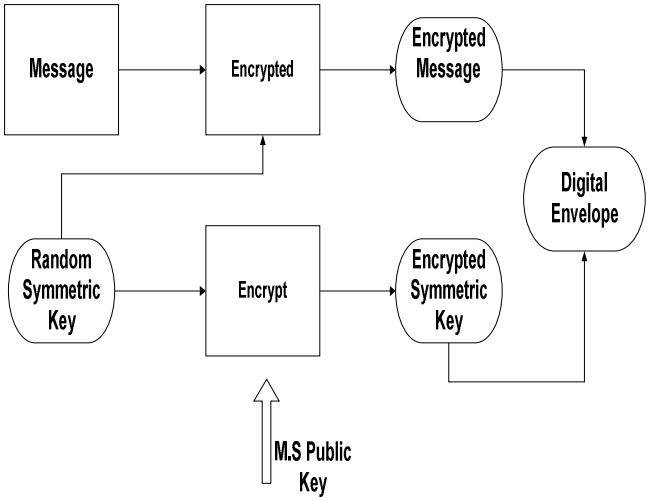

Figure 6: Creating a digital Envelope

4.4 Creating and opening a digital envelope

A digital envelope is the equivalent of a sealed envelope containing an unsigned letter. The outline of creating a digital envelope is shown in Fig. 6. The message is encrypted by the sender using a randomly generated symmetric key.

The symmetric key itself is encrypted using the intended recipient's public key. The combination of the encrypted message and the encrypted symmetric key is the digital envelope. The process of opening the digital envelope and recovering the contents is shown in Fig. 7.

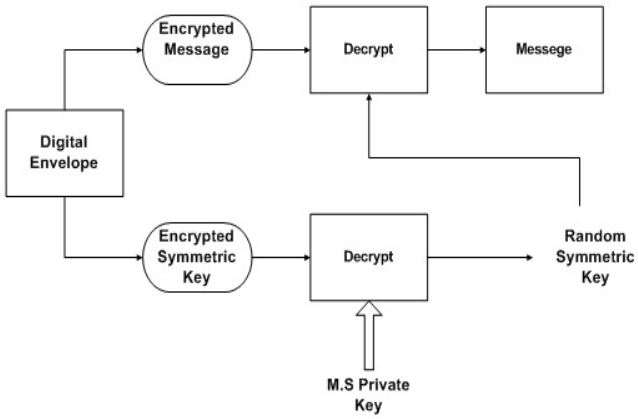

Figure 7: Opening a Digital Envelope

First, the encrypted symmetric key is recovered by a decryption using the recipient's private key. Subsequently, the encrypted message is decrypted using the symmetric key.

4.5 Creating and opening digital envelopes carrying signed messages

The process of creating a digital envelope containing a signed message is shown in Fig. 8.

A digital signature is created by the signature function using the message digest of the message and the B.S's private key. The original message and the digital signature are then encrypted by the B.S using a randomly generated key and a symmetric-key algorithm. The symmetric key itself is encrypted using the M.S's public key. The combination of encrypted message and signature, together with the encrypted symmetric key, form the digital envelope

containing the signed message. Figure 9 shows the process of opening a digital envelope, recovering the message, and verifying the signature.

First, the symmetric key is recovered using the M.S's private key. This is then used to decrypt and recover the message and the digital signature. The digital signature is then verified as described earlier.

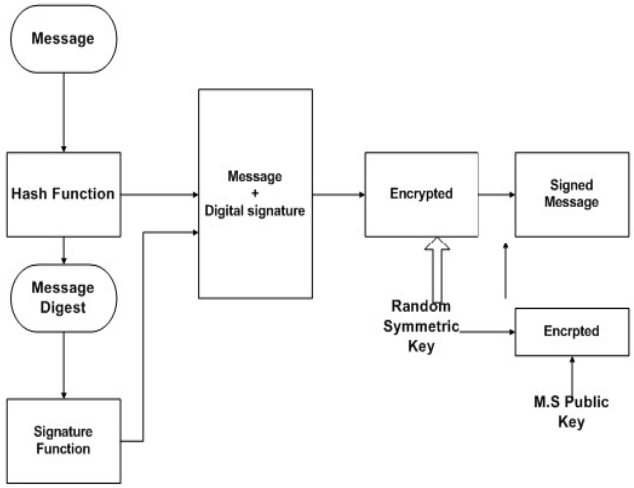

Figure 8: Creating a Digital Envelope carrying a signed messege

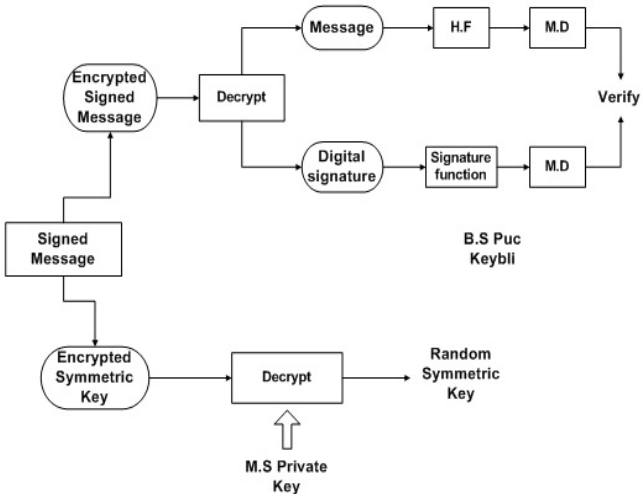

Figure 9: Opening a Digital Envelope & Verifying a Digital Signature

5. Conclusion

In this paper, an overview of security scheme in IEEE 802.16 is presented. Attacks on authentication can be described as the ways by which a network can be intruded and the privacy of the users is compromised; if the user authentication & authorization stage is compromised. Therefore, the ways to breach the authentication frameworks are termed as attacks on privacy & key management protocols. But our proposed authentication protocol will protect this type of interception. Just as signatures facilitate validation and verification of the authenticity of data, digital signatures serve the purpose of validation and authentication of information.

References

[1] Lang Wei-min, Wu Run-sheng, Wang jian-qiu : A Simple Key Management Scheme based on WiMAX: *PLA Institue of Communication Command, Institute of Physics and Communication & Electronics.*

[2] 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, ICCIT 2009*

[3] Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, Andreas Deininger :Security Vulnerabilities and Solutions in Mobile WiMAX, *KDDI R&D*

Laboratories, 2-1-15, Ohara, Fujimino-shi, Saitama 356-8502, Japan.

[4] Trung Nguyen, Prof. Raj Jain : A survey of Wimaxsecurity threats.

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

[6] "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16"- A.K.M. NAZMUS SAKIB, *Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology] Vol2, No 6, 2010.*

[7] "Security Vulnerability in IEEE 802.16 : Analysis & Solution"- A.K.M. NAZMUS SAKIB, Dr Muhammad
Ibrahim Khan, Mir Md Saki Kawsor, *Global Journal of Computer Science & Technology, Vol 10, Issue 13, Ver 1,*
2010.

[8] "Security Improvement of IEEE 802.11i (Wi-Fi Protected Access 2)"- A.K.M. NAZMUS SAKIB, Fariha
Tasmin Jaigirdar, Muntasim Munim, Armin Akter, *International Journal of Engineering Science & Technolo*