WIMAX SECURITY ANALYSIS AND ENHANCEMENT

Mir Md. Saki Kowsar [(1)], Muhammad Sakibur Rahman [(2)]

1. Department of Computer Science and Engineering, CUET E-mail: sakikowsar@cuet.ac.bd
2. Department of Computer Science and Engineering, CUET E-mail sakib_cse_cuet@yahoo.com

ABSTRACT

The importance of IEEE 802.16, Worldwide Interoperability for Microwave Access (WiMAX) is growing and will compete with technologies such as 3G. The acceptance and adoption of technologies also depend on security. Therefore, this article shows security vulnerabilities found in WiMAX and gives possible solutions to eliminate them. We find the initial network procedure is not effectively secured that makes man-in-the-middle attack possible. Focusing on this attack, we propose Diffie-Hellman (DH) key exchange protocol to enhance the security level during network initialization. We modify DH key exchange protocol to fit it into mobile WiMAX network as well as to eliminate existing weakness in original DH key exchange protocol. Finally we found that the proposed algorithm shows 2.5 times better performance in comparison with existing systems.

Keywords- WiMAX; Key Generation; Man-in-the-Middle; Sealing Function;

1.0 INTRODUCTION

IEEE 802.16 is the Standard to state the radio frequency of fixed Broadband Wireless Access (BWA). WiMAX is the trade name of “IEEE 802.16 Standard”. IEEE 802.16 was first planned to offer the last mile for Wireless Metropolitan Area Network (WMAN) with the line of sight (LoS) of 30- 50 km. It was designed to facilitate WISP’s (Wireless Internet Service Provider) Backhaul, Broadband internet connectivity to proprietary and standards-based Wi-Fi mesh networks, hotspots, residences and businesses. It is featured with QoS (Quality of Services) for Voice and Video, real-time video conferencing and other services with up to 280 Mbps per base stations. Revised Standard 802.16d, 2004 provides extended support for non-line-of-sight (NLoS) in 2-11GHz spectrum with mesh connections for both fixed and nomadic users. Latest IEEE 802.16e Standard, released on February 28, 2006 intends to facilitate mobility in 2-6GHz spectrum within a range of 2-5 km.

Mobile WiMAX introduces new features like different handover types, power saving methods and multi- and broadcast support. Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its Predecessors[1]. It uses EAP-based mutual authentication, a variety of strong encryption algorithms and packet numbers to protect against replay attacks and reduced key lifetimes.

But in current standard of WiMAX consists some vulnerabilities and these vulnerabilities are the main cause to introduce unauthenticated messages which are susceptible to forgery and the unencrypted management communication which reveals important management information.

In this paper, we present an overview of WiMAX protocol layer and security scheme. We focus the security vulnerabilities found in mobile WiMAX and introduce Diffie-Hellman (DH) key exchange protocol to eliminate these security leaks. Furthermore, we also introduce a new thought to eliminate man-in-the-middle problem arises in DH key exchange protocol.

2.0 WIMAX SECURITY ARCHITECTURE

2.1 IEEE 802.16 Protocol Layer

The IEEE 802.16 WiMAX standard consists of a protocol stack with well-defined interfaces. The WiMAX protocol layer contains MAC layer and PHY layer. MAC layer includes three sub-layers shown in Figure 1: The Service Specific Convergence Sub-layer (MAC CS), the MAC Common Part Sub-layer (MAC CPS) and the Security Sub-layer or Privacy Sub-layer.

Two main protocols work in security sublayer, one is an encapsulation protocol for encrypting packet data across the fixed BWA, and the other is a Privacy and Key Management Protocol (PKM) providing secure distribution of keying data from Base Stations (BS) to Subscriber Stations (SS) or Mobile Stations (MS). Security sublayer is responsible for all security related activities. It also enables BS to impose conditional access to network services.

WiMAX security process is divided into three steps:

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

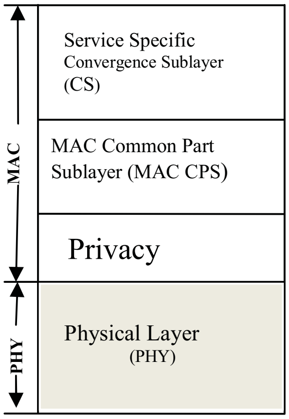

Figure 1. **IEEE 802.16 MAC and Physical Layer.**

The PKM protocol uses, RSA public key algorithm, X.509 digital certificates, and strong encryption algorithm to carry out key exchanges between SS and BS [2]. This Privacy protocol has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC [3].

The main objective of the privacy sublayer is to protect service providers against theft of service, rather than guarding network users. Privacy sublayer is above the physical layer, so it only guards data at the data link layer but does not protect physical layer from intercepted. It is necessary to include technologies to secure physical layer.

3.0 VULNERABILITIES IN IEEE 802.16

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, and [4] examined the 3-way TEK exchange and the authorization process and could not find any security leak. Also [5] analyzed the key management protocol using protocol analyzing software and did not detect any problem. But [6] shows, in mobile WiMAX there are some unauthenticated and unencrypted management messages which threat system reliability. This section explains vulnerabilities found in Mobile WiMAX.

These vulnerabilities are:

- Unauthenticated messages:

Mobile WiMAX includes some unauthenticated messages. Their forgery can constrict or even interrupt the communication between mobile station and base station.

- Unencrypted management communications:

The complete management communication between mobile station (MS) and base station (BS) is unencrypted. If an adversary listens to the traffic, he can collect lots of information about both instances.

3.1 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) [7] or alternatively by a cipher based message authentication code (CMAC). However, some messages are not covered by any authentication mechanism. This introduces some vulnerability. A couple of management messages 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 messages, so the authentication of these messages is difficult. Furthermore, a common key would not completely protect the integrity of the message as mobile stations sharing the key can be generated by unauthenticated BS.

3.2 Unencrypted Management Communication

The topic of unencrypted messages has already been discussed in some papers for Fixed WiMAX. In Mobile WiMAX management messages are still sent in the clear. The risk introduced by the management messages when they sent without encrypted will be discussed in this section.

When a MS performs initial network entry it negotiates communication parameters and settings with the BS, a lot of information is exchanged like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information, MS's capabilities, etc. Since the management messages are unencrypted, so an attacker can be accessed the mentioned information just by listening on the channel.

Initial network entry contains four processes: initial Ranging process, SS Basic Capability (SBC) negotiation process, PKM authentication process, and registration process. Initial network entry is the most security sensitive processes in Mobile WiMAX network not only because it is the first gate to establish a connection to the network, but also because many physical parameters, performance factors, and security contexts between SS and serving BS are determined during this process. The initial network process and MS Basic Capability negotiation is illustrated in Figure 2.

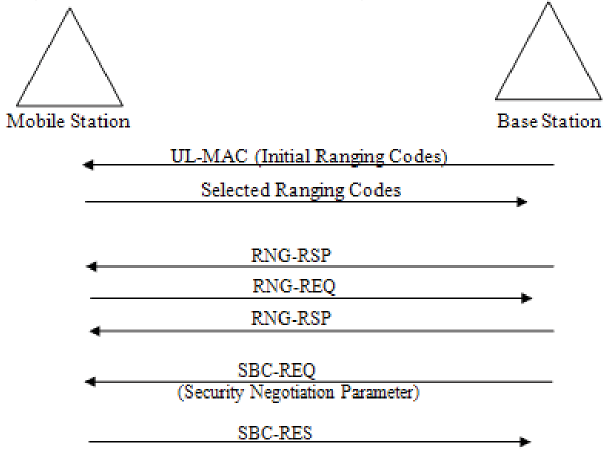

Figure 2. *WiMAX Initial Network Entry Procedure.*

After initial network entry, the management communication over the basic and primary management connections remains unencrypted. As most of the management messages are sent on these connections, nearly all management information exchanged between MS and BS can be accessed by a listening adversary.

The only messages which are encrypted are key transfer messages. But in this case only the transferred key is encrypted, all other information is still sent in the clear. An adversary collecting management information can create detailed profiles about MS's including capabilities of devices, security settings, associations with base stations and all other information described above. Using the data offered in power reports, registration, ranging and handover messages, a listening adversary is able to determine the movement and approximate position of the MS 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.

4.0 SOLUTION AND IMPROVEMENT

There are not appropriate methods to protect these messages. In order to eliminate the security vulnerabilities during initial network entry, we can encrypt the initial management massages based on Diffie-Hellman (DH) key exchange protocol [8]. DH key agreement is a key management method to share an encryption key with global variables known as prime number 'P' and 'G', 'G' is a primitive root of P. 'a' is the private key of MS, and 'b' is the private key of BS.

SS's public key is $PK_{MS} = G^{a}$ mod P, and

BS's public key is $PK_{BS} = G^{b}$ mod P.

The DH key exchange protocol is described as follows where both BS and MS exchange keys:

Step1: MS $\longrightarrow$ BS

Step2: MS $\longleftarrow$ BS

Step3: MS calculate encryption key Ka= (PKBS)a

Step3: MS calculate encryption key Kb= (PKMS)b

Algebraically it can be shown that Ka=Kb. So, the encryption will be symmetric key encryption process. And it is suggested to use 'Vernam Cipher' encryption process rather than DES or AES to encrypt initial management communication where the key will be used as a random number for encryption. Because of the use of symmetric key encryption as well as Vernam Cipher which required only to performed bitwise Exclusive-OR operation [9], it will not introduce any traffic overhead in the network. Encryption process is described as follows:

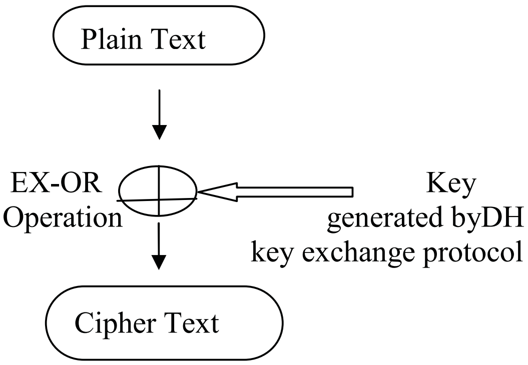

Figure 3. **Encryption Process by using Key, Generated by DH Algorithm.**

4.1 Man-in-the-middle Vulnerabilities

A man-in-the-middle attack is one in which the attacker intercepts messages during the process of communication establishment or a public key exchange and then retransmits them, tampering the information contained in the messages, so that the two original parties still appear to be communicating with each other.

In Diffie-Hellman key exchange process [10], it is possible to man-in-the-middle attack. Figure: 5

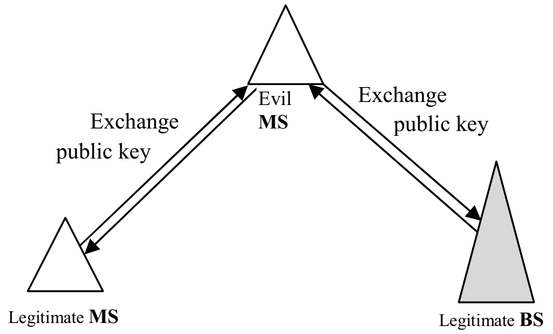

Figure 4. Man-in-the-middle Attack.

It is possible to overcome the man-in-the-middle vulnerability by using cryptographic sealing functions. In this process every MS has an International Subscriber Station Identity (ISSI) and a cryptographic function as a seal of legitimate MS. The security process is as follows:

Step1: MS alleges that it is a legitimate subscriber.

Step2: BS sends a random number, R_{BS} as a challenge to MS.

Step3: MS calculates the value of the function for this random number and sends the value and its ISSI number to BS.

Step4: MS sends a random number, R_{SS} as a challenge to BS that it is a legitimate BS.

Step5: BS calculates the value of the function by this random number for the corresponding ISSI and sends to BS.

Step6: Only the legitimate BS knows the function which is used by the given ISSI but not the evil MS. So the evil MS is not able to produce correct value for the given random number. Then MS checks BS's identity using the response that it receives, if the BS is legitimate, the shared key is established and MS continues to communicate with BS; otherwise, MS ceases the communication.

Suppose a MS's ISSI number is: 0346AE2D and it consists the cryptographic function:

$$f(x)= x^3 + x-5$$

Now, the initial communication will be as follows:

Step1: MS says that: "I am a legitimate subscriber".

Step2: Suppose, BS sends a random number R_{BS} = 3 to MS as challenge to MS.

Step3: MS calculate the value of f(x) =25, and send the value as well as the ISSI number.

Step4: BS also calculates the value of f(x) for the given ISSI number and finds that it is a legitimate MS.

Step5: Suppose, MS also sends a random number R_{MS} =5 to BS as a challenge to BS.

Step6: BS calculates the value of f(x) =125, send to MS.

Step7: MS verify the value and continue to communicate with BS if the value of the cryptographic function matches with MS's calculated value. Otherwise MS ceases the communication.

Afterward, both MS and BS exchange their public key and generate a common key by DH algorithm for exchanging management information and other messages which verify the message authenticity and enhance system reliability that gives no information to attackers.

4.2 Performance Analysis:

After employing the proposed system, it is sure that the system runs as a secured system without any probability of attacks on the management communications. Even this system eliminates the possibility of man-in-the-middle attacks in initial network entry procedure and makes authentication process more easy and reliable. Moreover, the proposed encryption process required less execution time than the existing process which does not introduce any traffic overhead in the network. The comparative analysis of the performance between proposed system and the existing system is described in the following table 5.1.

Existing System	Proposed System
01. After negotiation with the network MS sets up a security association (SA). This SA manages the keys for all encryption processes. So the initial negotiation process remains unencrypted.	01. In proposed system, keys are not managed only by the SA; rather keys also have been generated by Diffie-Hallman algorithm [8] before negotiation and this key generation provides the opportunity to encrypt the messages required for negotiation.
02. If the management information remains unencrypted it makes possible to get user's ranging information, channel information, vendor information and registration information etc. which threats user secrecy and interrupt the communication.	02. The proposed system allows the network to establish a shared key and this is used to encrypt all management messages. So it is not possible for an attacker to listen the user's ranging information, channel information, user's vendor information, etc. and communication continues without any interruption.

TABLE I. COMPARATIVE ANALYSIS BETWEEN PROPOSED SYSTEM AND EXISTING SYSTEM

Authentication process of the proposed system is too much simple and required only four steps to send and receive the random numbers and corresponding function values. But in the existing systems, authentication process is very much complex and not sufficient to eliminate man-in-the –middle attacks because the authentication process is performed only by the BSs not by MSs. Proposed system required four steps for authentication process:

1. BS sends a random number to MS
2. MS calculates and sends the function value for the corresponding random number and ISSI number to BS
3. Again BS receives a random number from MS and calculates the function value for the given ISSI number.
4. MS received function value from BS for the given random number.

Existing system's authentication process required steps are:

1. MS sends Authentication-Inf-Mess (manufacturer X.509 certificate) to BS
2. MS sends Authentication-Req-Mess (X.509 cert, Capability, Basic CID, SAID) to BS.
3. BS sends Authentication-Rep-Mess (AK-Seq, Life time, SA-Descriptor) by encrypting MS's public key.
4. MS calculates KEK and message authentication keys HMAC_ Keys (HMAC_Key_U, HMAC_Key_D) and sends response by using these keys.

C
H
A

Here, we found that the BSs have to calculate Authorization Key (AK), life lime, and to generate security association descriptor and also have to perform encryption by using MS's public key. Again MSs have to calculate key encryption key (KEK), Authorization keys (HMAC_Key_U, HMAC_Key_D). So this complex but one-way authentication required total three keys calculation and one key generation and RSA encryption and one SA-Descriptor generation processes. So we found that the proposed authentication process is very simple and required only two operations (calculate two functions value) where existing system is very much complex and required five operations (three key generations, one descriptor generation and one encryption process). The operation time depends on vendor's capability. The following figure 5: shows the comparative analysis of the number of operations have to process for N subscribers and we found that the proposed systems require 2.5 times less operations and perform authentications for both BSs and MSs

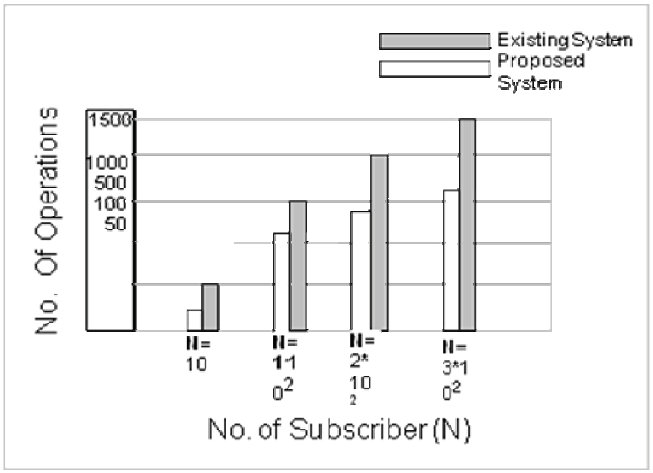

Figure 5. Comparative analysis of Authentication Process (Operations vs. Subscribers)

	Authentication Process	Man-in-the-middle Problem	Management Communication
Existing System	Very complex	Possible to arise	Remains unencrypted
Proposed System	Simple	Eliminated	Encrypted

TABLE II. OUTCOME AFTER IMPROVEMENT

5.0 CONCLUSION

In this paper, an overview of security scheme in IEEE802.16 based mobile WiMAX is presented. We investigate various vulnerabilities in mobile WiMAX network and we propose DH key exchange protocol to enhance the security level during the initial network entry procedure to reduce unauthenticated messages and to encrypt the initial management communication. We modify DH protocol to fit mobile WiMAX to eliminate man-in-the-middle attack by using cryptographic sealing function. Verily it could eliminate the possibilities of the man-in-the-middle attacks as well as resist DoS attacks toward mobile WiMAX.

REFERENCES

1. Johnston D., Walker J.: Overview of IEEE 802.16 Security, IEEE Computer Society, 2004.

2. Xu, S., Matthews, M. & Huang, C. (2006). Security Issues in Privacy and Key Management Protocols of IEEE802.16, retrieved on 1st May, 2006.

3. Eklund, C., Marks,R.B., Stanwood, K.L., & Wang, S.(2002) IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access, retrieved on 1st May, 2006.

4. 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.

Yuksel E.: Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling, Technical University Denmark, DTU, 2007.

5. Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka: Security Vulnerabilities and Solutions in Mobile WiMAX, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007.

6. Krawczyk H., Ballare M., Canetti R.: HMAC: Key-Hashing for Message Authentication, RFC 2104.

7. Whitfield Diffie and Martin E. Hellman: New Directions in Cryptography, Invented Paper.

8. Charles P. Pfleeger, “Security in Computing” VOL No. 2

9. Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu: Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, IEEE Xplore.