International Journal of Internet, Broadcasting and Communication Vol.8 No.2 66-74 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.2.66

IJIBC 16-2-8

A Study of WiMAX Security threats and Their Solution

Seon-mi Woo[1] and Gisung Jeong [2*]

[1]*JINI Co., Ltd, B-102, Technobill, 109 banryong-toad, Deokjin gu, Jeonju si, Jeollabuk-do, Korea*
[*2]*Department of Fire Service Administration, WonKwang University, Republic of Korea*
E-mail: jgskor@wku.ac.kr

Abstract

In this study, we have discussed and illustrated the security issues of WiMAX technology including vulnerabilities, threats and some security solution. Both physical layer and data link layer have been considered. Jamming is a major threat in physical layer, and in data link layer we study an authentication problem and see the problem of some unencrypted messages leading to lack of confidentiality. Some of these vulnerabilities have been solved in the recent amendment of 802.16 and some still remain. Moreover WiMax is a new technology yet.

Keywords*: Security, WIMAX, Vulnerabilities, Data Encryption, Authorization*

1. Introduction

When it seemed necessary having a wireless broadband carrier network technology, IEEE designed and draw up a standard named WiMax (Worldwide Interoperability for Microwave Access) that started in 1999 and was approved in 2002 [2]. According to [1] security in wireless network is maintaining the Authentication, Confidentiality, Non repudiation and Integrity control. To save guard this security services protocols has been adapted. As it can be pointed out of the name, WiMax is a technology based on microwave signals with the goal of providing a high-speed connectivity over long distance and caching this reason. 802.16 operate in 2-to-66 GH frequency range. In figure 1 the protocol stack of 802-16 is illustrated. The bottom sublayer uses three different modulation schemes for transmission. The reason why we have three different modulationschemes refer to physical property of these millimeter waves in which signal strength decrease with distance from base station, and we have to use less bit per baud with increasing the distance. The main task of Convergence transmission Sublayer is to hide these different technologies from

Manuscript Received: Mar. 5, 2016 / Revised: Mar. 17, 2016 / Accepted: Apr. 2, 2016
Corresponding Author: jgskor@wku.ac.kr
Tel: +82-63-850-6398, Fax: +82-63-850-6907
Department of Fire Service Administration, WonKwang University, Republic of Korea

Data Link Layer. The Data Link Layer consists of three sublayers. The security sublayer deals with encryption, decryption and key management. In the Mac Common Part Sublayer the main protocols such as channel management are located. It is completely connection oriented. The last sublayer of Data Link layer is the Service Specific Convergence Layer whose main job is mapping the connection oriented data to packet protocols and preparing information to through Network Layer. Having said a little about WiMax architecture we can have a look at security problems and threats that 802.16 is dealing with. In this paper we categories the issues based on security classes in each separate layer of WiMax plus some extra threat issues.

2. Fundamental Wimax Concept

Wimax have five fundamental architecture components: **Base Station** (BS) is a node that logically connects wireless subscribers to the operator networks. Base Station is responsible for maintaining subscriber communication and access to the operator network. **Subscriber Station** (SS) also known as Stationary Station is a WiMax-capable radio system that connects to the Base Station. **Mobile Station** (MS) is a mobile WiMax-capable radio system; it is battery operated and employs power management**. Relay Station** (RS) is also SS that forwards connection to other RSs or SSs. It can either be in a mobile or fixed location. Finally, **Operator Network** (ON) engulfs the infrastructure network functions providing radio access and IP connectivity services to WiMax subscribers. WiMax devices use two wireless massage types for communication; **Data** messages transporting data across WiMax network and **Management** messages that transport data across WiMax network [15].

2.1 WiMax Services

WiMax provides Mobility service, Coverage service, Maintainability service and Roaming service etc. WiMax offers full cellular type mobile data transformation referred as Mobile WiMax or Non Line of Sight (NLOS). It also provides point to point data services known as Fixed WiMax also called Line of Sight (LOS). WiMax offers point to pint, point to multipoint, Multi hop and Mobile network topologies. Most valuable services provided by WiMax include Data and Network, CCTV surveillance, Home automation, Access control and Intercoms [6].

2.2 WiMax Standards and specifications

In 1999 IEEE standards has established the working group Broad Wireless Access (BWA) known as IEEE 802.16 for developing standard for world wide deployment of broadband Wireless Metropolitan Area Network [17]. In late 2001 first 802.16 standard was designed for PMP broadband wireless transmission. This standard is not convenient for lower frequency because of lack of support of non-line-of-sight (NLOS). Then in 2003, a new standard 802.16a was published for the support of this equipment. After revising many times, then it was ended in the last standard; 802.16-2004 corresponding to revision D. these standards are properly defined for Stationary and mobile use. This means end subscriber devices cannot move around between BS but may enter the network at deferring locations. In 2005, 802.16-2004 was amended to 802.16e and released to support mobility which makes possible for the MSs to handover between different BSs. The following table 1 shows IEEE 802.16 standards.

Table 1. WiMax Standards and Version size

Standard	802.16	802.16a/802.16REVd	802.16e
Spectrum	10 to 66 GHz	< 11 GHz	< 6 GHz
Channel Conditions	Line-of-Sight only	None-Line-of-Sight	Non-Line-of-Sight
Speed (bit rate)	32 to 134 Mbps	75 Mbps max, 20-MHz channelization	15 Mbps max, 5-MHz channelization
Modulation	QPSK 16QAM 64QAM	OFDM 256 subcarrier QPSK 16QAM 64QAM	same as 802.16a
Mobility	Fixed	Fixed	Pedestrian mobility, regional roaming
Channel Bandwidths	20, 25 and 28 MHz	Selectable between 1.25 and 20 MHz	same as 802.16a with sub-channels
Typical Cell Radius	1 – 3 miles	3-5 miles (up to 30 miles, depending on tower height, antenna gain and transmit power)	1-3 miles

3. WiMax Security Features

The secure communications provided by WiMax standards are achieved by three steps: Authentication, Dada Encryption and Key establishment. Figure 1 shows an overview of WiMax security framework. Secure connection between the SS/MS and the BS is provided by authentication procedures and key establishment, while secure data exchange is accomplished by data encryption [13].

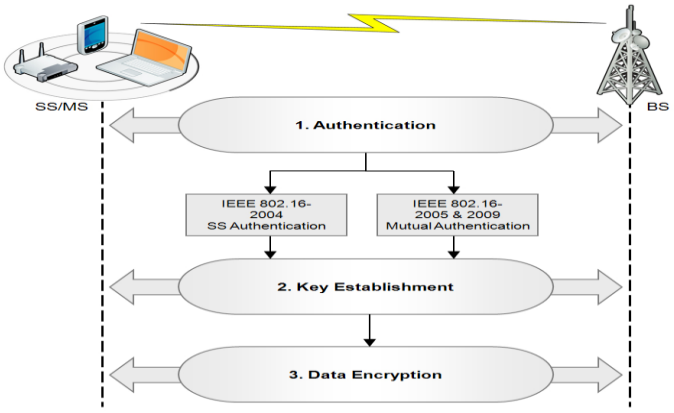

Figure 1. WiMax security Framework

Wimax provide protection to main entities MS/SS and BS with the help of the following security features.

3.1 Security Association (SA)

SA is used to facilitate secure communications between MS/SS and BS with a shared set of parameters. This defines secure parameter connection, be it encryption or algorithm. This shared set of parameters can be authentication SAs, data SAs or group SAs. Authentication and key management is facilitated by the Authorization SAs. Each SA has traffic encryption key (TEK) and also contains initialization vectors, its own identifier (SAID) and cryptographic suite which identify the selected secure algorithm [8].

3.2 Public Key Infrastructure

IEEE 802.16 uses the Privacy and Key management for secure key exchange, secure key transfer and secure key management between its entities (MS/SS and BS) [4]. The authentication of the MS/SS to the BS is also accomplished with the help of PKM protocol. X.509 digital certificate, Advanced Encryption Algorithm (EAS) and RSA (Rivest-Shamir-Adleman) are used by the PKM protocol [11]. Traditional standard of WiMax uses PKM version 1 (one way authentication method). This version of PKM is compromised by Man-In-The-Middle-Attack (MITMA). PKMv2 a two way authentication mechanism is used by newer versions of WiMax. Figure 2 show public key infrastructure in WiMax [20].

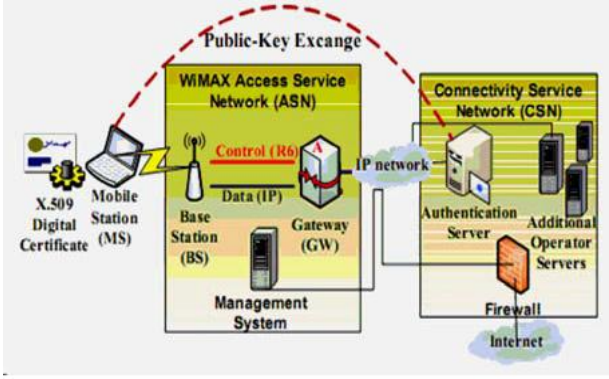

Figure 2. Public Key Infrastructure in WiMax (20)

3.3 Authentication and Authorization

Process of authenticating MS/SS and controlling their access to the network in WiMax is referred as authorizations. WiMax uses Privacy and Key Management (PKM) protocol for authentication and authorization to help distribute secure keys. To accomplish data and group encryption SAs, Public Key Management protocol uses authorization SAs to authenticate MSs and BSs. Enforcement function of PKM's authentication provides the system entities (MS and BS) with identical authentication keys. Then each of these keys derives the Massage Authentication Keys (MAK) and Key Encryption Keys (KEK), which in turn facilitates the secure exchange of TEKs. IEEE 802.16-2004 uses PKM version 1 (PKMv1) to derive AK. IEEE 802.16-2005 and IEEE 802.16-2009 use PKMv2 to derive AKs [15].

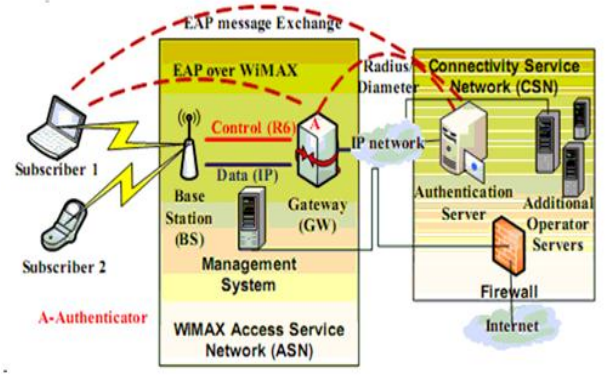

Figure 3. EAP based Authentication

3.4 Encryption Key Establishment

WiMax entities (MS and BS) share an active authorization key (AK) after authentication is accomplished. PKM then uses 160 bit message of TEKs, and 160 AK to derive 128 bit KEK. A three way handshake between entities is used by the secure TEK exchange [18].

3.5 Data Encryption

WiMax MAC layer encrypts only data messages not management messages. It checks the SA associated with the current connection and acquires the initialization vector. Then encrypt the MAC Protocol Data Unit (MPDU) plaintext payload by employing the generated MPDU and the authenticated TEKs. To indicate the payload in the MPDU is encrypted, it sets Encryption Control (EC) field of the MAC header to 1. Here, 2 bit encryption key sequence is used to indicate which TEK is used. Finally it updates the Cyclic Redundancy Check (CRC) field in accordance with changes in both the payload and MAC header [19].

4. WiMax Security Threats

WiMax security threats and vulnerabilities are mostly associated with its Physical and MAC layers. This exposes the network to a number of wireless attacks including modification, interception, replay and fabrication attacks [7]. Though lot of amendments has been carried on in WiMax to tackle problems inherited from older version, it still faces some.

4.1 Threats In Physical Layer

There are some physical attacks against WiMax that we mention two most important of them named jamming and scrambling.These attacks lead to going out of connectivity with base station. Interruption means prevention information from reaching the destination is attack on availability [14].

4.1.1 Jamming

Is when an attacker produce some disturb signal that makes the environment noisy so much that the subscriber station cannot understand the base station.

Solution: we can increase the power of signal or the bandwidth besides that there is some radio spectrum monitoring equipment by which we can simply detect and locate the source of signal.

4.1.2 Scrambling

It is something like jamming but more professional with time dividing in order to attack to some specific WiMax or part of frames in physical layer.

Solution: although it is more difficult to detect scrambling than jamming we there is still some equipment to detect scrambler.

4.1.3 Water torture attack

since the devices are using WiMax technology are usually portable and mobile device and very dependent on battery this kind of attack is considerable that in which the attacker forces the SS to send some unnecessary messages to BS in order to consume the electrical resource and computing resource of SS.

Solution: we can use some sophisticated mechanism to detect the bogus frame and prevent to send them.

4.2 Threats In Data Link Layer(Authentication)

The main technique is based on public key principle in which the A party who wants to send data to B party, encrypt data with his own private key and then B can decrypt the data with only public key of A, so the B party can realize that the information is sent by A. We can authenticate the data sender in this way.

4.2.1 Man in the middle attack: (Confidentiality)

In 802.16 we use X.509 certificate by which SSs (subscriber stations) will authenticate themselves to BS (base station). So no one else will be able to introduce himself as a legitimate SS while he is not. The problem is that it doesn't go the same from Base Station to Subscriber Station and this is where "Man in the Middle attack" can occur. The attacker can imitates legitimate BS and goes on pretending that is providing service for SS, whereas he is deceiving the SSs and have a plan to hack them. In this situation the Base Station is called the rogue BS [9].

Solution: there is an Extensible Authentication Protocol (**EAP**) which is already adopted in WiMax amendment (802.16e) and it uses an authentication method that identifies the BSs to SSs.

In order to provide information confidentiality we encrypt data that means converting the format of information into something that cannot be understood. There is a lots of encryption method and some really strong algorithm have been introduced recently which can be used in network communication.

4.2.2 Dos Attacks:

WiMAX uses AES (Advanced Encryption Standard) and it provides the strong support for confidentiality of data traffic.The problem arises from where some management messages in 802.16 are not involved in any authentication mechanism [3]. Although most of the control and management messages are encrypted, there are some messages which are not protected and so attacker can abuse them simply. Some of those messages are listed below and we will explain two of them for example:

1- MOB_TRF-IND
2- MOB_NBR-ADV
3- FPC
4- MSC-REQ
5- DBPC-REQ
6- PMC-REQ
7- MOB_ASC-REP
8- RNG-REQ

MSC-REQ

Multicast Assignment Request Message (MSC_REQ) is one of the management messages which is not encrypted. This message is used when BS wants to remove the MS from the multicast polling group. If a MS delete itself from a polling group, it won't be able to get bandwidth from the BS via a polling mechanism. And then MS has to use some other bandwidth allocation algorithm which leads to a great delay. An attacker can easily remove a MS from polling list because this message is not protected.

MOB_NBR-ADV

This message is sent by BS when he wants to handover the MS (mobile station) to a neighbour BS which probably have better quality for MS since now. This message also is not encrypted, so the attacker can keep back the MS from main BS as rouge neighbour base station or even can send message to MS that there is not any other BS available.

Solution: We can encrypt all this massage using Hash based Massage Authentication Code (HMAC), but the only problem exists is these messages are very short for this standard and we have to use appended digit [5].

4.3 Application layer:

It won't be useless if we mention briefly a vulnerability that can occur in the application layer if the user doesn't be careful enough about the security, as we know WiMax uses encryption method for communication in order to save the confidentiality of information. But there is some way that the person can disable these encryption method in the application layer and the solution is just be careful enough about the configuration and manipulating of application layer properties.

5. Some other Threats and their Solutions

This section shows other threats not addressed previously and their solutions.

5.1 Authorization Vulnerability

IEEE 802.16 standards use mutual authentication to protect from forgery attacks. WiMax cannot ensure message integrity. This causes authorization process vulnerability. Therefore, WiMax authorization message can be trapped, modified and retransmitted by properly placed radio receiver.

Solution: In [4] it is proposed that authorization vulnerability issue can be solved by some modifications to the authentication protocol and key management protocol. This is to add a timestamp to authentication message of the original protocol.

5.2 Key Space Vulnerability

According to [16] in 802.16e, 2 bit key sequence number is used to differentiate between successive generations of TEKs. 4 bit key sequence number is also used for AKs. Key size is insufficient to protect keying material from attacks.

Solution: for example increasing both sequence numbers up to 8 bit can easily solve this problem. But if large number of bits is added, it may affect the performance significantly.

5.3 Downgrade Attacks

WiMax authorization process starting message is unsecure, it moves from the SS telling the BS his security capability. Spoofed message can be sent to the BS with weaker security capabilities to force the BS and the SS to agree on an unsecure encryption algorithm [7]. WiMax has no strong solution for this attack.

Solution: Ignoring messages with lower security capability can be seen as a solution for this attack. In this situation SS with low security capability can suffer from Denial of Service attack.

5.4 Authorization Attack

Malicious radio receiver can make both legitimate SS/MS draw towards his network and to get permission to enter a legitimate BSs network. Recording the messages and replaying to the BS and SS/MS makes possible this attack. This can be described as "lack of defined clarification of intended receiver".

Solution: According to [12] this can be solved by using the RSA public and private keys for authorization.

6. Conclusion

How secure is the 802.16 is still a matter of time because WiMAX is a new technology and should be in practical environment to pass its examination. This technology is spreading faster and faster and without any doubt will be the aim of more and more hackers to attack. We have to be always ready to face some other vulnerability and threat will arise in this area of network and telecommunication technology.

References

[1] A. S. Tanenbaum, "Computer Networks," 4th Edition, Prentice Hall, Inc., New Jersey, 2006.
[2] http://en.wikipedia.org/wiki/WiMax
[3] Fuqiang Liu, Lei Lu, A WPKI-based Security Mechanism for IEEE 802.16e, IEEE Communications Society, Wuhan University, China 2006.
[4] Sen Xu Manton Matthews Chin-Tser Huang, Security Issues in Privacy and Key Management Protocols of *Ieee 802.16, Acm Se'06, March 10- 12, 2006, Melbourne, Florida, USA.*
[5] Krawczyk et. al., RFC 2104: HMAC: Keyed-Hashing for Message Authentication, February 1997, http://tools.ietf.org/html/rfc2104.
[6] Sen Xu, Chin-Tser Huang, Manton M. Matthews, Secure Multicast in WiMAX, *Journal Of Networks, Vol. 3, No. 2, February 2008.*
[7] Leonardo Maccari, Matteo Paoli, Romano Fantacci, Security analysis of IEEE 802.16, Communications, 2007. ICC '07. IEEE International Conference on 24-28 June 2007 PP.1160 – 1165.
[8] Tian Haibo, Pang Liaojun, Wang Yumin, Key Management Protocol of the IEEE 802.16e, Wu han University Journal of Natural Sciences Vol.12 No.1, 2007.
[9] Jie Huang, Chin-Tser Huang, Secure Mutual Authentication Protocols for Mobile
[10] Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations., *IEEE ICC, 2011. Vol.3, No.1, pp.1-12., 2011.*Wikipedia, RSA, http://en.wikipedia.org/wiki/RSA, accessed: 8:11:2011.
[11] Housley, et. al., RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, The Internet Society, April 2002,
[12] http://ieeexplore.ieee.org/iel5/10676/33683/016033

[13] Kejie Lu; Yi Qian; Hsiao-Hwa Chen, wireless broadband access: wimax and beyond - A Secure and Service-Oriented Network Control Framework for WiMAX Networks, IEEE Communications Magazine • May, Vol.1, No.1, pp.20-26, 2007
[14] http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/index.html

[15] Karen Scarfone, Cyrus Tibbs Matthew Sexton, Guide to Securing WiMAX Wireless Communications, *Recommendations of the National Institute of Standards and Technology, 2013.*
[16] Junaid Qayyum, Muhammad Lal, Faheem Khan, Muhammad Imad, Survey & Assessment of Wimax, Its Security Threats and Their Solutions, *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 11 No: 3, pp. 24-30, 2014.*
[17] http://en.wikipedia.org/wiki/802.16
[18] Rakesh Kumar Jha, Dr Upena D Dalal , A Journey on WiMAX and its Security Issues, *International Journal of Computer Science and Information Technologies, Vol. 1, No. 4, 256-263, 2010.*
[19] Nirwan Ansari; WiMAX Security: Privacy Key Management; *International Workshop on Network Security and Wireless Communications, Vol.1, No.1, pp.34-40,2007*
[20] A. A. Ayesha Altaf, Rabia Sirhindi, A novel approach against dos attacks in wimax authentication using visual cryptography,*The Second International Conference on Emerging Security Information, Systems and Technologies, securware, Vol.1, No.1, pp.56-64, 2008.*