Military Technical College

Kobry El-Kobbah,

Cairo, Egypt

8th International Conference on Electrical Engineering

ICEENG 2012

WiMAX 802.16 Networks: Threats, attacks, and Solutions

Ahmed Mohamed El-Amin
Military Technical Research center
ahmed_elamin_omran@yahoo.ca

Alaa El -Din Rohiem
Military Technical College

Essam Abd-Elwanees
Military Technical College
mohwanees@yahoo.com

Abstract:

Worldwide Interoperability for Microwave Access (WiMAX) is going to be an emerging wireless technology for the future. With the increasing popularity of Broadband internet, wireless networking market is thriving. Wireless network is not fully secure due to rapid release of new technologies, market competition and lack of physical infrastructure. In the IEEE 802.11 technology, security was added later. In IEEE 802.16, security has been considered as the main issue during the design of the protocol. However, security mechanism of the IEEE 802.16 (WiMAX) still remains a question. WiMAX is relatively a new technology; not deployed widely to justify the evidence of threats, risk and vulnerability in real situations. This paper will address the security aspects of the IEEE 802.16 Standard and point out the security vulnerabilities, threats and risks associated with this standard and their countermeasures.

1. Introduction

WiMax is a wireless based technology standard that provides high throughputbroadband connections over long distances. Security is one of the majorconsiderations in broadband wireless access especially when wireless devices are added to it. Wimax/802.16 is also not free from vulnerability, threats, risks or other attacks to provide secured and robust services like as other standards 802.11 and so on. With the high and effective security confirmation, this technology would be more reliable and trustworthy. This paper works on all possible attacks of Wimax standard and provided their solutions which separately came on light so far.

The IEEE 802.16 standard is still “on paper” and some methods are under development. Time and scope are the constraints for this paper. Therefore, research has been done based on published materials, literature & journal study, and IEEE publications and mostly from website; however references has been provided wherever necessary. To understand the security aspects of IEEE 802.16 technology, it is required to provide an overview of this

standard as a relevant work. In this paper, only MAC and Physical layer of the standard has been discussed shortly. "WiMAX" and "IEEE 802.16 standard" will be used as synonyms.

2. IEEE 802.16 Protocol Layer

Physical Layer:

WiMAX uses OFDM technology. Orthogonal frequency division multiplexing (OFDM) allows assigning subcarriers to different users. It is resilient to multipath that helps to overcome multiple signals hitting the receiver[1,13].
In IEEE 802.162004 standard, the OFDM signal is divided into 256 carriers and IEEE 802.16e will use Scalable OFDMA. The IEEE 802.16 standard supports wide range of frequencies and the physical layer contains several forms of modulation and multiplexing (Boom, 2004). The modulation methods in the downlink (DL) and uplink (UL) are binary phase shift keying (BPSK), quaternary PSK (QPSK), 16quadrature amplitude modulation (QAM), and 64QAM [13].

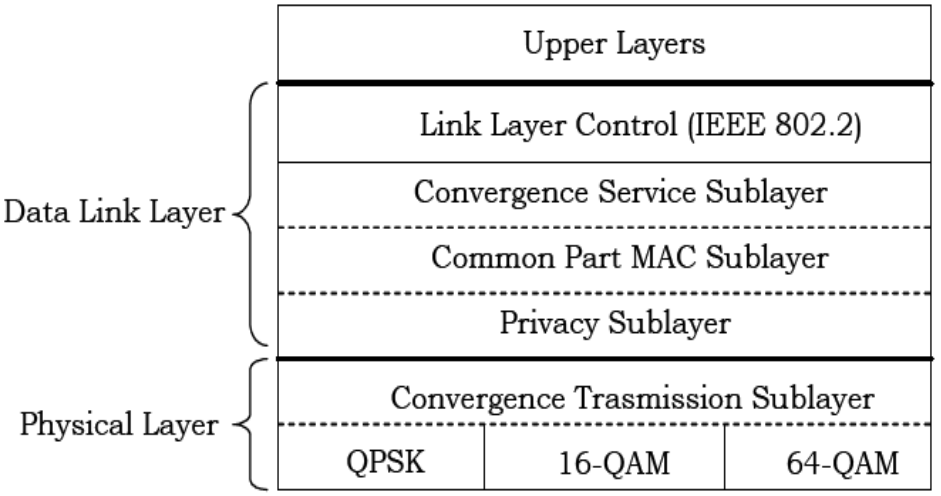

Figure 1: IEEE 802.16 Protocol Layer (IEEE, 2004)

IEEE 802.16 MAC:

The 802.16 MAC is connection oriented. The MAC Layer of IEEE 802.16 was designed for point to multipoint (PMP) broadband wireless access applications (IEEE, 2004). IEEE 802.16 standard is made up of a protocol stack with properly defined interfaces. There is a Base Station (BS) as the Access Points in 802.11 and several Subscribers Stations (SS). BS is basically wired, and it broadcasts to the Subsciber Stations (SS). In contrast to 802.11 CSMA/CA method, 802.16 uses Uplink and Downlink maps to confirm collision free access. SS uses Time Division Multiple Access (TDMA) to share the uplink, while BS uses TDM (Time Division Multiplexing). All these functions are done through ULMAP and DLMAP messages (Aikaterini, 2004) [2,3].
MAC layer consists of three sub layers. ***Service Specific Convergence Sublayer*** (MAC CS), ***the MAC Common Part Sublayer*** (MAC CPS) and the ***privacy sublayer*** [2,18]. The MAC CS sublayer is to converse with higher layers and transforms upper-level data services to

MAC layer flows and associations. MAC CS has two types of sub-layers: one is ATM convergence sublayer for ATM networks & services and the other one is Packet Convergence sublayer for packet data services for example, Ethernet, PPP, IP and VLAN [4,5,27]. The basic function of CS Layer is that it receives data from higher layers, classifies data as ATM cell or packet and forwards frames to CPS layer [5,27].

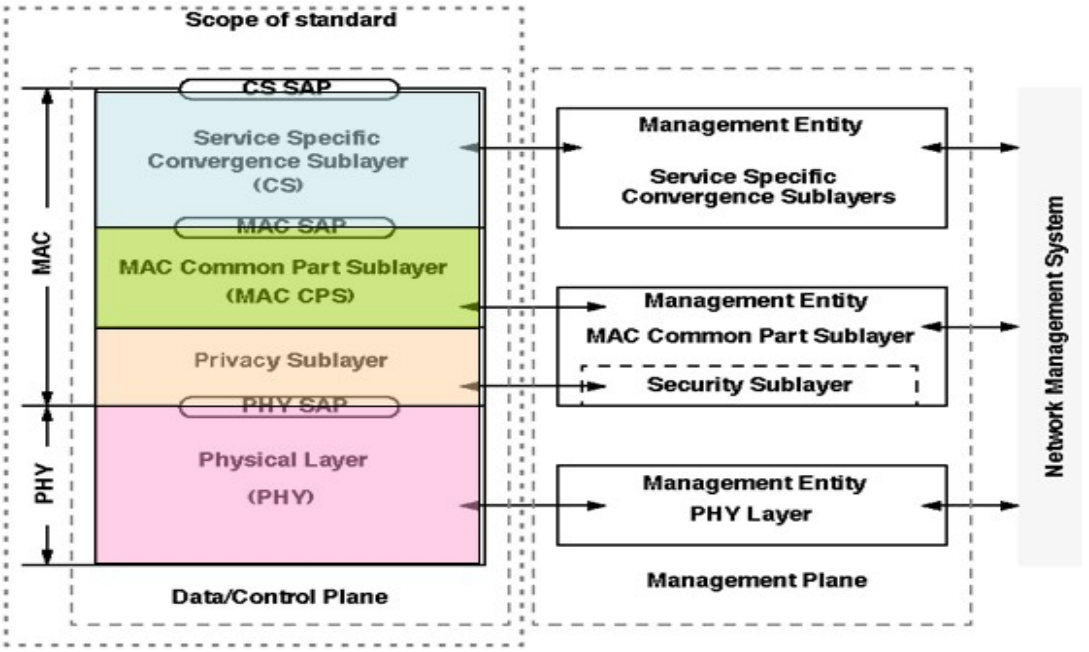

Figure 2: IEEE 802.16 MAC and Physical Layer [27]

Format of MAC Messages:

MAC Protocol Data Units (MPDUs) contains exchange messages of BS MAC and SS MAC. It has three parts: a fixed length MAC header, which contains frame control information; a variablelength Payload (frame body) and a frame check sequence (FCS), which holds IEEE 32bit CRC (Liu, 2005). Again, MAC header types are: MAC Service Data Unit (MSPU), where payloads are MAC SDUs/segments, i.e., data from the upper layer (CS PDUs). Second one is, Generic MAC header (GMH) where the payloads are MAC Management messages or IP packets encapsulated in MAC CS PDUs. Both are transmitted on management connections [4, 23,27]. The third one is Bandwidth Request Header (BRH) which is sent out without payload. Except the Bandwidth Request PDUs, MAC PDUs may hold either MAC management messages or convergence Sublayer data MSDU. For both GMH and MSDU, Header Type (HT bit) is always set to 0 (zero) while Bandwidth Request Header is set to 1 (one). The MAC header contains a flag, which indicates whether the payload of the PDU is encrypted or not[23,27].

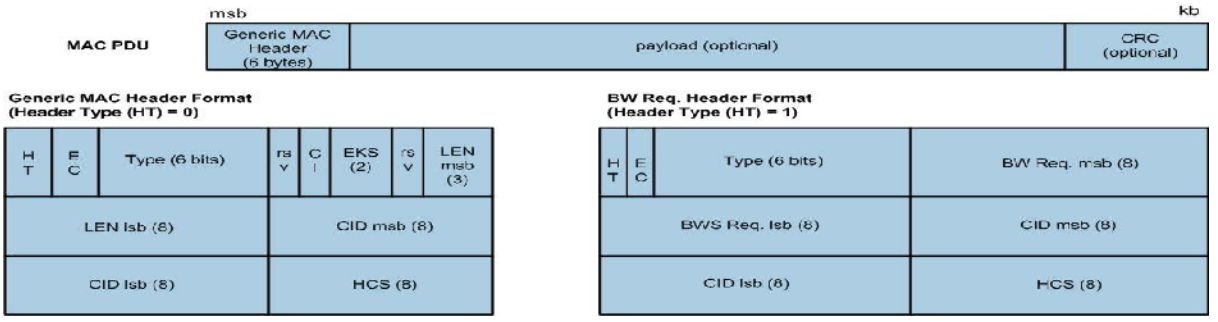

Figure 3: MAC PDU Field description [27]

According to IEEE Standard 802.16 (2001), MAC header and all MAC management messages are not encrypted. This decision was made to "facilitate registration, ranging and normal operation of the MAC sublayer" as it allows generation of false management messages. Consequently, this leads to vulnerabilities, otherwise if encrypted, spoofing was difficult during BS and SS had exchanged encryption keys (Boom, 2004). In case of vulnerabilities in management messages, authentication will be exposed to eavesdropping, man in the middle attacks, active attacks and replay attacks. In the latest IEEE 802.16e standard, the payload of MAC PDUs is encrypted with DES in the CBC mode or AES in the CCM mode (IEEE, 2006). The amended 802.16e introduces an integrity protection mechanism for data traffic. The EKS (Encryption Key Sequence) field is used to make sure that the BS and SS are synchronized in their use of Traffic Encryption Keys (TEK) and Initialization Vectors (IV). When a SS joins a BS network, it follows a multistep process. And when the SS detects an active connection it transmits its presence to BS through a Range Request (RNGREQ) message. The SS and BS continue their conversation via RNGREQ and RNGRSP messages using newly assigned basic CID by BS. BS replies with REGRSP message describing the supported capabilities. SS acknowledges the REGRSP with REGACK message [6, 23, and 27].

Privacy Sublayer:

Two main protocols work in this 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 BS to SS. It also enables BS to impose conditional access to network services. The PKM protocol uses, RSA publickey algorithm, X.509 digital certificates, and strong encryption algorithm to carry out key exchanges between SS and BS [7,27]. This Privacy protocol is based on the PKM protocol of the DOCSIS BPI+ specification; it has been enhanced to accommodate stronger cryptographic methods such as AES to fit into the IEEE 802.16 MAC. (Eklund et al, 2002). The entire security of IEEE 802.16 is in the privacy sublayer. The function of this sublayer is to provide access control and confidentiality of the data link. Security Associations (SA) is identified by SAID, which contains, Cryptographic suite (i.e., encryption algorithm) and Security Info (i.e., key, IV). The basic and primary management connections do not have SAs. The secondary management connection can have an optional SA. Transport connections always have SAs [6, 27].

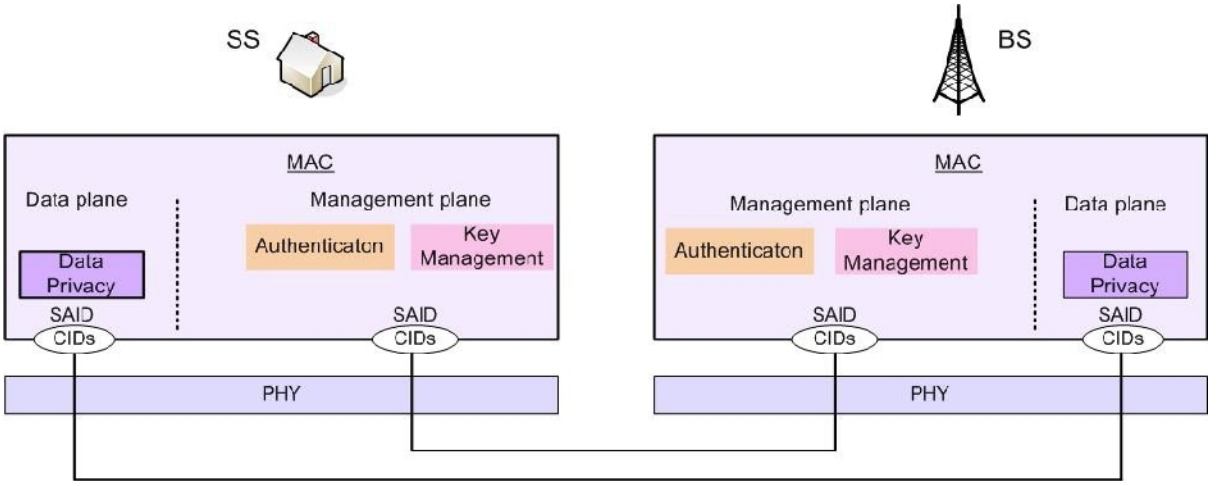

Figure 4: IEEE 802.16 Security Associations (SA), [27]

Data SA (Security Associations):

Data SA has a 16bit SA identifier, a Cipher (DES in CBC mode) to protect the data during transmission over the channel and two Traffic encryption keys (TEKs) to encrypt data: one is the current operational key and the other is TEK. When the current key expires, TEK a 2bit key identifiers is used. A 64bit initialization vector (IV) is used for each TEK. The lifetime of TEK is between 30 minutes to 7 days. There are three types of data SA: Primary SA is used during link initialization, static SAs are configured on the BS and dynamic SAs are used for transport connections when needed. The primary SA is shared between an MS and its BS. Static SAs and dynamic SAs can be shared among several MSs (Mobile stations) during multicast. During the connection process, SA first starts a data SA using a connection request function. A SS generally has two or three SAs, one is the secondary management connection and one is for both uplink and downlink connections; it may use separate SAs for uplink and downlink channels (Johnston & Walker 2004)[9]. BS ensure that each SS has access only to SA it's authorized.

Authorization SA (Authentication):

The authorization SA has a 60bit authorization key (AK) and a 4bit quantity to identify the AK. To identify SS, it uses an X.509 certificate. The lifetime of AK ranges from 1 to 70 days, default is 7 days. Key encryption key (KEK) has a 112bit 3DES key for distributing TEKs (Temporal encryption key) and a list of authorized data SAs. It uses a downlink & uplink HMAC (Hash function based message authentication code) key providing data authenticity of key distribution messages from the BS to SS and SS to BS respectively. An authorization SA state is shared between a particular BS & SS. Base stations use authorization SAs to configure data SAs on the SS (Johnston & Walker 2004)[8,10,27].

Figure 5: IEEE 802.16 Authentications, [27]

SS authentication uses X.509 certificate (Privacy Key Management (PKM) authorization protocol and encryption) negotiate security capabilities between BS and SS, which establish security association (SAID) through Authentication Key (AK) exchange. AK serves as authorization token, which is encrypted using public key (RSA) cryptography. Authentication is done when both SS and BS possess AK (Wongthavarawat, 2005) [27].

Data Key Exchange:

Data encryption requires data key called Transport Encryption key (TEK), which uses AK from authentication process to derive Key Encryption Key (KEK) and Message Authentication Key (HMAC key). TEK is generated by BS randomly. TEK is encrypted with 3DES (use 112 bits KEK), RSA (use SS's public key) and AES (use 128 bits KEK). Key Exchange message is authenticated by HMACSHA1, which provides Message Integrity and AK confirmation (Wongthavarawat, 2005) [9, 27].

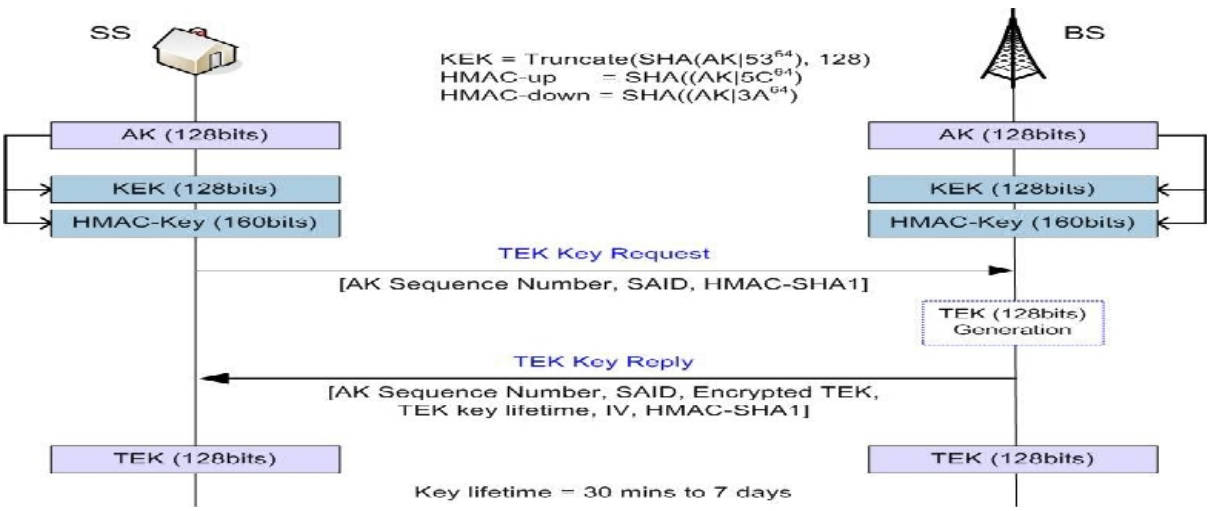

Figure 6: IEEE 802.16 IEEE 802.16 Data Key Exchange, (Wongthavarawat, 2005)

3. WiMAX security vulnerabilities and countermeasures

WiMAX has security vulnerabilities in both PHY and MAC layers, exposing to various classes of wireless attack including interception, fabrication, modification, and replay attacks [10, 16]. Some vulnerabilities of WiMAX originate from flaws of IEEE 802.16 on which WiMAX is based. A lot of problems and flaws have been fixed in the enhanced version but WiMAX still has some exposes. In this section some possible threats or vulnerabilities will be reviewed and some solutions will be discussed.

3.1 Threats to the PHY layer

As described before, WiMAX security is implemented in the security sub-layer which is above the PHY layer. Therefore the PHY is unsecure [12, 15]and it is not protected from attacks targeting at the inherentvulnerability of wireless links such as jamming, scrambling or water torture attack. WiMAX supports mobility, thus it is more vulnerable to these attacks because the attackers do not need to reside in a fixed place and the monitoring solutions presented below will be more difficult [11].

Jamming attack:

Jamming is described by M. Barbeau as an attack achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel [15]. Jamming can be either intentional or unintentional. It is not difficult to perform a jamming attack because necessary information and equipments are easy to acquire and there is even a book by Poisel[23]which teaches jamming techniques.
Solutions: According to Michel Barbeau[15], we can prevent jamming attack by increasing the power of signals or by increasing the bandwidth of signals using spreading techniques such as frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS). Furthermore, since it is easy to detect jamming by using radio spectrum monitoring equipment and the sources of jamming are easy to be located by using radio direction finding tools, we can also ask help from law enforcement to stop the jammers.

Scrambling attack:

Also described in [15], scrambling is a kind of jamming but only provoked for short intervals of time and targeted to specific WiMAX frames or parts of frames at the PHY layer. Attackers can selectively scramble control or management information in order to affect the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more difficult to perform a scrambling attack than to perform a jamming attack due to “the need, by the attacker, to interpret control information and to send noise during specific intervals.
Solutions: Since scrambling is intermittent, it is more difficult to detect scrambling than jamming. Fortunately, we can use anomalies monitoring beyond performance norm (or criteria) to detect scrambling and scramblers.

Water torture attack:

According to D. Johnson and J. Walker[14], this is also a typical attack in which an attacker forcesthe SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources.
Solutions: To prevent this kind of attack, a sophisticated mechanism is necessary to discard bogus frames, thus avoiding running out of battery or computational resources.
Table 1 summarized the WiMAX 802.16 Physical layer threats and their solutions.

Other threats:

In addition to threats from jamming, scrambling and water torture attacks, 802.16 is also vulnerable to other attacks such as forgery attacks in which an attacker with an adequate radio transmitter can write to a wireless channel [14]. In mesh mode, 802.16 is also vulnerable to replay attacks in which an attacker resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process.
Solutions: providing mutual authentication to defend these kinds of attacks.

Threats / Layer	Attacks	Solutions
Physical Layer	Jamming Attack	Increasing the power or using (FHSS) or (DSS)
	Scrambling Attack	Monitoring to detect scrambling and scrambles
	Water torture Attack	Using a sophisticated mechanism to discard bogus frames, thus avoiding running out of battery or computational resources
	Replay Attack	Mutual Authentication

Table1 WiMAX 802.16 Physical layer threats and solutions

3.2 Threats to the MAC layers

Threats to Mac Management message in Initial network entry:

The initial network entry procedure is very important since it is the first gate to establish a connection to Mobile WiMAX by performing several steps including: initial Ranging process, SS Basic Capability (SSBC) negotiation, PKM authentication and registration process [14].

The vulnerability of using Ranging Request-Response messages:

This message is used in the initial ranging process. The RNG-REQ message is sent by a SS trying to join a network to propose a request for transmission timing, power, frequency, and burst profile information. Then, the BS responds by sending a RNG-RSP message to fine-tune the setting of transmission link. After that, the RNG-RSP can be used to change the uplink and downlink channel of the SS. There are several threats related to these messages. For instance, an attacker can intercept the RNG-REQ to change the most preferred burst profile of SS to theleast effective one, thus downgrading the service [17, 22]. An attacker can also spoof or modify ranging messages to attack or interrupt regular network activities. This vulnerability can lead to a DoS attack.

Other initial network entry vulnerability: T. Shon and W. Choi presented a more general vulnerability of initial network entry in [21].During the initial network entry process, many important physical parameters, performance factors, and security contexts between SS and BS, specifically the SBS negotiation parameters and PKM security contexts. Although the security schemes offered WiMAX include a message authentication scheme using HMAC/CMAC codes and traffic encryption scheme using AES based on PKMv2, these schemes are applied only to normal data traffic after initial network entry process. Subsequently, the parameters exchanged during this process are not securely protected, bringing a possible exposure to malicious users to attack.

Solution: T. Shon and W. Choi also proposed a solution to this vulnerability by using Diffie-Hellman key agreement scheme as depicted in [23].

In this approach, the Diffie-Hellman key agreement scheme will be used for SS and BS to generate a shared common key called “pre-TEK” separately and establish a secret communication channels in the initial ranging procedure. After that, the SBC security parameters and PKM security contexts can be exchanged securely.

3.3 Threats to Access network Security

In [21], T. Shon and W. Choi also reviewed vulnerability in access network security in WiMAX. In order to accommodate the requirements of WiMAX End-to-End Network Systems Architecture for mobile WiMAX network, the WiMAX forum defined network Reference Model (NRM) which consists of the following entities: Subscriber Station (SS), Access Service Network (ASN), and Connectivity Service Network(CSN). ASN consists of at least one BS and one ASN Gateway (ASN/GW) forming a complete set of networkfunctions necessary to provide radio access to mobile subscribers. CSN consists of AAA Proxy/Server, Policy,Billing, and Roaming Entities forming a set of network functions to provide IP connectivity services tosubscribers. This AAA-architecture based model is illustrated in [21,24].

T. Shon and W. Choi divided the model into three insecure domains and one secure domain [21]. The only secure domain covered by encryption and authentication schemes in 802.16 standard is the data communications between SS and BS. The initial network entry which is examined in the 3b section belongs to domain A [21]. Domain B and C are considered insecure because the Network Working Group in WiMAX forum just assumes that domain B is in a trusted network without proposing any protection and just suggests a possibility of applying an IPSec tunnel between ASN and AAA in domain C.

Solutions: T. Shon and W. Choi proposed a countermeasure for this problem by using a simple and efficient key exchange method based on PKI. Their method is described in [21].In this approach, all network devices have their certificate and a certificate chain for verification. The PKI structure is used as a method to obtain correspondent’s public keys

and verify the certificates, thus enabling entities to create a shared secret key for establishing a secure connection.

3.4 Threats to authentication

Many serious threats also arise from the WiMAX's authentication scheme in which masquerading and attacks on the authentication protocol of PKM are the most considerable.

Masquerading threat:

Masquerade attack is a type of attack in which one system assumes the identity of another. WiMAX supports unilateral device level authentication [15]which is a RSA/X.509 certificate based authentication. The certificate can be programmed in a device by the manufacturer. Therefore sniffing and spoofing can make a masquerade attack possible. Specifically, there are two techniques to perform this attack: identity theft and rogue BS attack.For the Identity theft, an attacker reprograms a device with the hardware address of another device. The address can be stolenby interfering the management messages where in Rogue BS attack, the SS can be compromised by a forged BS which imitates a legitimate BS. The rogue BS makes the SSs believing that they are connected to the legitimate BS, thus it can intercept SSs' whole information. In IEEE 802.16 using PKMv1, the lack of mutual authentication prevents confirming the authentication of BS and makes Man-In-The-Middle (MITM) attack through rogue BS possible by sniffing Auth-related message from SS. However, it is difficult to successfully perform this kind of attack in WiMAX which supports mutual authentication by using PKMv2.

Attacks on the authentication protocols of basic PKM versions:

By adopting new version of PKM, WiMAX fixes many flaws in PKMv1 such as vulnerability to MITM due to the lack of mutual authentication. However, the newly proposed PKMv2 has been found to be also vulnerable to new attacks [20].

Attacks on basic PKM authentication protocol:
Attacker can intercept and save the messages sent by a legal SS and then perform a replay attack against the BS. The SS also might face with this kind of attack. In the worst case, since mutual authentication is not supported in basic PKM, BS is not authenticated. Therefore malicious BS can perform a MITM attack by making its own Auth-Reply message and gain the control of the communication of victim SS.
S. Xuet. al. concluded that Basic PKM has many flaws such that it provides almost no guarantees to SS about the AK [20]. These problems have been fixed in the Intel Nonce version of PKM.

Attacks on Intel Nonce Version PKM:
In this version, nonce is a possible alternative to timestamp in authentication protocol. This approach does not protect a BS from a replay attack.

Attacks on PKMv2:
This version provides a three-way authentication with a confirmation message from SS to BS. There are two possible attacks as follows. First, a replay attack can be performed if there is no signature by SS. Second, even with the signature form SS; an interleaving attack is still possible.

3.5 Other threats

Some serious attacks can exploit vulnerabilities in many aspects of the MAC layers. Two of the most destructive attacks can be MITM and DoS attacks.

Man in the middle attack:

Although WiMAX can prevent MITM attack through rogue BS by using PKMv2, it is still vulnerable to MITM attack. This possibility is due to the vulnerabilities in initial network entry procedure. Tao Han et. al. in [19]shows that through intercepting and capturing message in the SSBC negotiation procedure, an attacker can imitate a legitimate SS and send tamped SSBC response message to the BS while interrupting the communication between them. The spoof message would inform the BS that the SS only supports low security capabilities or has no security capability. If the BS still accepts, then the communication between the SS and the BS will not have a strong protection. Under these circumstances, the attacker is able to wiretap and tamper all the information transmitted. Tao Han et. al. also proposed their solution to this kind of attack which they called "SINEP". Their method is based on Diffie-Hellman (DH) key exchange protocol. This approach is very similar to that by T. Shon and W. Choi in [21].

Denial of Service attack:

Comprehensive surveys [22, 24, 18, 25]show that there are many vulnerabilities exposing IEEE 802.16e networks to DoS attacks such as unprotected network entry, unencrypted management communication, unprotected management frame, weak key sharing mechanism in multicast and broadcast operations, and Reset-Command message). Some of noticeable DoS attacks may be based on; Ranging Request/Response messages, Mobile Neighbor Advertisement message, Fast Power Control message, Authorization-invalid (Auth-invalid) message, and Reset Command message.

In DoS attacks based on Ranging Request/Response (RNG-REG/RNG-RSP) messages, the attacker can forge a RNG-RSP message to minimize the power level of SS to make SS 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 SS, effectively draining the SS's battery.

InDoS attacks based on Mobile Neighbor Advertisement (MOB-NBR-ADV) message, the message is sent from serving BS to publicize the characteristics of neighbor base stations to SSs searching for possible handovers. This message is not authenticated. Thus it can be forged by an attacker in order to prevent the SSs from efficient handovers downgrading the performance or even denying the legitimate service.

In DoS attacks based on Fast Power Control (FPC) message, the message is sent from BS to ask a SS to adjust its transmission power. This is also one of the management messages which are not protected. An attacker can intercept and use FPC message to prevent a SS from correctly adjusting transmission power and communicating with the BS. He can also use this message to perform a water torture DoS attack to drain the SS's battery.

In DoS attacks based on Authorization-invalid (Auth-invalid) message, the Auth-invalid is sent from a BS to a SS when AK shared between BS and SS expires or BS is unable to

verify the HMAC/CMAC properly. This message is not protected by HMAC and it has PKM identifier equal to zero. Thus, it can be used as DoS tool to invalidate legitimate SS.

In DoS attacks based on Reset Command (RES-CMD) message, this message is sent to request a SS to reinitialize its MAC state machine, allowing a BS to reset a non-responsive or malfunction SS, also this message is protected by HMAC but is still potential to be used to perform a DoS attacks and in order to prevent DoS attacks, we first need to fix the vulnerabilities in the initial network entry. This work is discussed before thatSherazNaseeretalso suggest that the authentication mechanism should be extended to as many management frame as possible. They also suggest using digital signatures as an authentication method [22]. Table 2 summarized theThreats for the MAC layer.

Threats / Layer	Attacks		Solutions
Mac layers	MAC Management message in intial network entry	(RNG-REQ, RNG-RSP) Message threats	Diffie-Hellman Key agreement Scheme. [21]
		Acces Network Security Threats	Simple and efficient key exchange method based on PKI [21]
	Authentication Threats	Identity threat	Mutual Authentication
		Rouge BS Attack	
	Attacks on basic authentication protocol PKMv1	Replay attack and Man in the middle attack	Updating this version to PKMv2
	Attacks in Intel Nonce PKM	Replay attack	Using PKMv2
	Attacks on PKM v2	Replay attack if there is no signature by SS and MIMA	Mutual Authentication
	Man in the middle attack (MIMA)	Mutual Authentication	
	Denial of Service attacks	DOS attacks based on Rangig Request/Response messages	Digital signature (On Paper)
		DoS attacks based on Mobile Neighbor Advertisement (MOB_NBR_ADV) message	
		DoS attacks based on Fast Power Control (FPC) message	
		DoS attacks based on	

		Authorization-invalid (Auth-invalid) message	
		DoS attacks based on Reset Command (RES-CMD) message	

Table2 WiMAX 802.16 MAC layer threats and solutions

4. Conclusion

In this paper, IEEE 802.16 protocol layers, security solution, various vulnerabilities and possible attacks to WiMAX network have been discussed and illustrated. The threats apply to both layers of WiMAX. At PHY layers, jamming can be considered a major threat. Somecritical threats are included such as eavesdropping of management messages, masquerading, management message modification andDoS attacks. Some of these issues have been fixed with the adoption of recent amendments and security solutions in IEEE 802.16 but some still exist and need to be considered carefully. However, through this review, we can see that WiMAX does offer much more strong security solutions in comparison with other wireless technologies such as Bluetooth or Wireless Fidelity (WiFi). WiMAX is still under development and need more research on its securities vulnerabilities. In the near future, when WiMAX achieves a maturity level, it would have a great opportunity to be a successful wireless communication technology.

5. References

[1] A.K.M. NazmusSakib, Mir Md. Saki Kowsar, "Shared Key Vulnerability in IEEE 802.16e: Analysis & Solution",Proceeding of 13th International Conference on computer and information Technology (ICCIT 2010) 23-25 December 2010,Dhaka,Bangladesh.

[2] PerumalrajaRengaraju, Chung-Horng Lung, Yi Qu, "Analysis on Mobile WiMAX Security", (TIC-CTH IEEE 2009)Department of Systems and Computer EngineeringCarleton University, Ottawa, Ontario, Canada.

[3] LI1, Zhiyi FANG1, Peng XU1, Wei XIAO1 and Wei WANG "Experimental Research on a New Authentication Protocol for Wireless Communication Network Based on WiMAXRuixue", College of Computer Science and Technology, Jilin University Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education Changchun 130012, Chinalee_ruixue@yahoo.com.cn, fangzy@jlu.edu.cn School of Computer, Northeast Normal University Changchun 130000, China IEEE 2008.

[4] "Design of Distributed Security Architecture for MultihopWiMAX", Networks.2010 Eighth Annual International Conference on Privacy, Security and Trust.

[5] Huixia Jin1 Li TuGelan Yang Yatao Yang, "An Improved Mutual Authentication Scheme in Multi-Hop WiMax Network" 2008 International Conference on Computer and Electrical EngineeringDepartment of Physics and Telecom Engineering, Hunan City University, Yiyang, China 413008) Department of Computer Science, Hunan City University, Yiyang, China 413008) 3(Beijing Electronic Science & Technology Institute, Beijing, China 100070) E-mail: jinhuixia1980@163.com.

[6] Wei-min1, ZHONG Jing-li1, LI Jian-Jun, "Research on the Authentication Scheme of WiMAX 2008 IEEELANG", Department of Information Warfare,PLA Institute of Communication Command, Wuhan, ChinaE-mail: wemlang@sina.comQI Xiang-yu2 2. Armored Force Engineering Institute, Beijing, ChinaE-mail: wmlang76@tom.com

[7] Leonardo Maccari, Matteo Paoli, Romano Fantacci, "Security analysis of IEEE 802.16", ICC 2007 ProceedingDepartment of Electronics and Telecommunications - University of Florence Telecommunication Network Lab Florence, Italy, Email: {maccari, paoli, fantacci}@lart.det.unifi.it.

[8] Frank, AIbikunle"Security Issues in Mobile WiMAX (IEEE 802.16e)2009", IEEE Mobile WiMAX Symposium*Covenant University, Electrical and Information Engineering Department, Ota*.faibikunle2@yahoo.co.uk.

[9] David Johnson and Jesse Walker, "Overview of IEEE 802.16 Security", Intel Corp, IEEE Security and Privacy, 2004http://portal.acm.org/citation.cfm?id=1009288

[10] Michel Barbeau, "WiMax/802.16 Threat Analysis", Proceedings of the first ACM international workshop on Quality of service & security in wireless and mobile networks, Quebec, Canada 2005.http://portal.acm.org/citation.cfm?id=1089761.1089764.

[11] Mahmoud Narsreldin, HebaAslan, Magdy El-Hennawy, Adel El-Hennawy, "WiMAX security", 22nd International Conference on Advanced Information Networking and Applications, 2008.http://portal.acm.org/citation.cfm?id=1395554.

[12] Andreas Deininger, ShinsakuKiyomoto, Jun Kurihara, Toshiaki Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007. http://paper.ijcsns.org/07_book/200711/20071102.pdf.

[13] AbdelrahmanElleithy, AlaaAbuzaghleh, AbdelshakourAbuzneid, "A new mechanism to solve IEEE 802.16 authentication vulnerabilities", Computer Science and Engineering Department UniversityofBridgeport, CT.http://www.asee.org/activities/organizations/zones/proceedings/zone1/2008/Professional/ASEE12008_0022_paper.pdf.

[14] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu, "Analysis of Mobile WiMAX Security", Vulnerabilities and Solutions, Mobile Ad Hoc and Sensor Systems, 2008.MASS 2008.http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4660134.

[15] SenXu, Chin-Tser Huang, "Attacks on PKM Protocols of IEEE 802.16 and Its LaterVersions", 3rd International Symposium on Wireless Communication Systems, ISWCS 2006.http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4362284.

[16] TaeshikShon, Wook Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Lecture notes in computer science, Springer, 2007.http://www.springerlink.com/content/d03p14w7720x842l.

[17] SherazNaseer, Dr. Muhammad Younus, Attiq Ahmed, "Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks", A Survey, Proceedings of the 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4617395.

[18] R. Poisel, "Modern Communications Jamming Principles and Techinques", Artech House Publishers, 2003.

[19] Ayesha Altaf, RabiaSirhindi, Attiq Ahmed, "A Novel Approach against DoS Attacks inWiMAX Authentication using Visual Cryptography", The Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE, Cap Esterel,France 2008.http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4622589.

[20] D.W. Park, "A Study of Packet Analysis regarding a DoS Attack in WiBro Environments", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.http://paper.ijcsns.org/07_book/200812/20081257.pdf.

[21] MitkoBogdanoski, PeroLatkoski, AleksandarRisteski, BorislavPopovski, "IEEE 802.16 Security Issues", A Survey, Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, Skopje, Macedonia. http://2008.telfor.rs/files/radovi/02_32.pdf.

[23]Management Frame Attacks in WiMAX Networks: Analysis and PreventionIEEE 2010 1Krishna Bakthavathsalu, 2Srinivas SampalliFaculty of Computer ScienceDalhousie UniversityHalifax, NS, CanadaE-mail: {1krishna, 2srini}@cs.dal.ca Qiang Ye Dept. of Computer Science and Information TechnologyUniversity of Prince Edward IslandCharlottetown, PE, CanadaE-mail: qye@upei.ca

[24] J. Mar, J.P. Huang, "Traffic Performance Analysis of the Integrated Dual Band Cellular Radio Networks," IEE Proc.-Comm., Vol.147, No.3, pp.180--186, June 2000.

[25] RachnaDhamija and J. D. Tygar. The Battle AgainstPhishing: Dynamic Security Skins. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), pages 77--88, July 2005.

[26] RachnaDhamija, J. D. Tygar, and Marti Hearst. Whyphishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 581--590, 2006.

[27] WiMAX HANDBOOK Building 802.16 Wireless Network. FRANK OHRTMAN "McGraw-Hill Communication".