A survey of WiMAX security threats

Trung Nguyen, nguyent@seas.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download

Abstract:

As a promising broadband wireless technology, WiMAX has many salient advantages over such as: high data rates, quality of service, scalability, security, and mobility. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks in. This report is a survey of security vulnerabilities found in WiMAX network. Vulnerabilities and threats associated with both layers in WiMAX (physical and MAC layers) are discussed along with possible solutions.

Keywords:

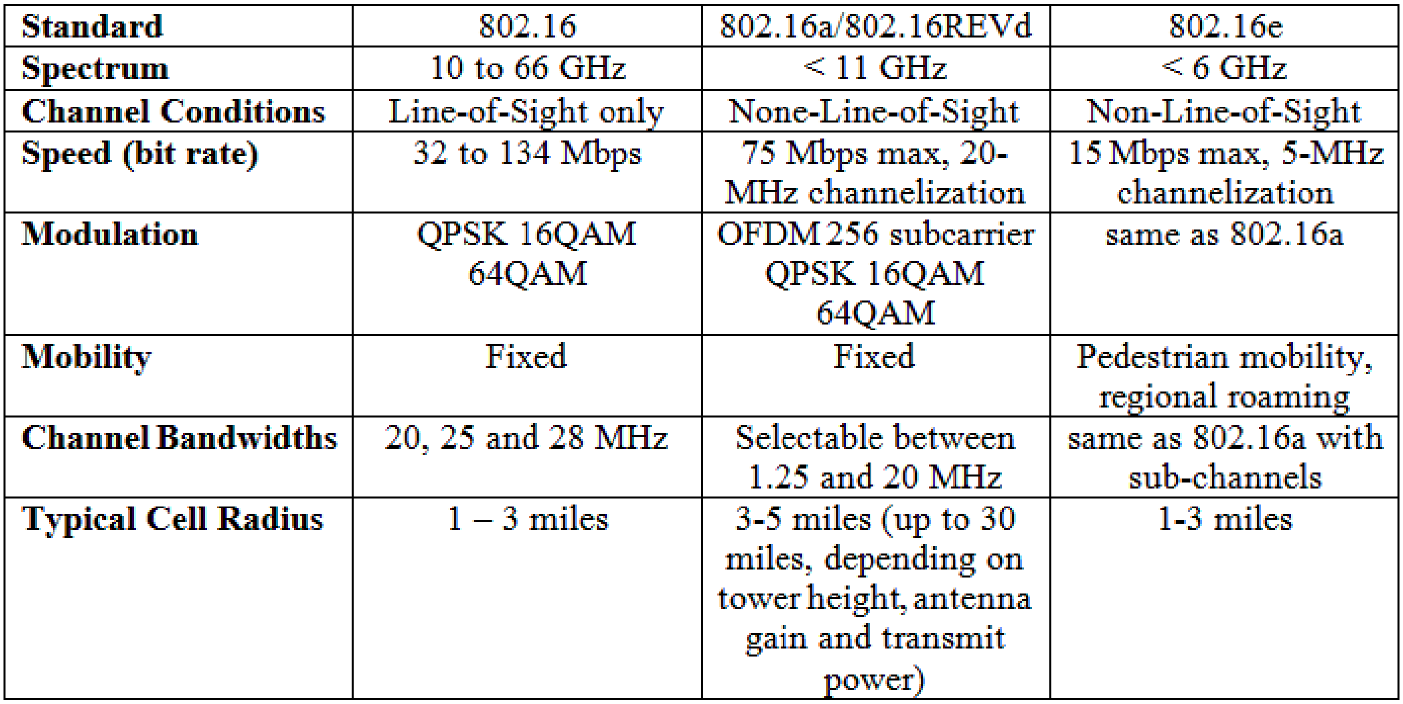
IEEE 802.16, WiMAX, wireless network, threat analysis, vulnerabilities analysis, security, network security, PKM, PKMv2, authentication, encryption, man-in-the-middle attacks, DoS attacks, WiMAX attacks.

Table of Contents

1. Introduction

Established by IEEE Standards Board in 1999, the IEEE 802.16 is a working group on Broad Wireless Access

(BWA) developing standards for the global deployment of broadband Wireless Metropolitan Area Networks [Wiki_802.16]. In December 2001, the first 802.16 standard which was designed to specialize point-to-multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement. Then, after being revised several times, the standard was ended in the final standard: 802.16-2004 which corresponds to revision D. These standards define the BWA for stationary and nomadic use which means that end devices cannot move between base stations (BS) but they can enter the network at different locations. In 2005, an amendment to 802.14-2004, the IEEE 802.16e was released to address the mobility which enable mobile stations (MB) to handover between BSs while communicating. This standard is often called “Mobile WiMAX7#8221;. The following table provides a summary of the IEEE 802.16 family of standards.



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

Table 1. Summary of the IEEE 802.16 family of standards.

Based on the IEEE 802.16 standard, the WiMAX (Worldwide Inter-operability for Microwave Access) is “a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access”[Wiki_WiMAX]. The WiMAX is supported by the WiMAX forum, which is a non-profit organization formed to promote the adoption of WiMAX compatible products and services [WiMAXABT]. WiMAX is a very promising technology with many key features over other wireless technologies [Jain08]. For instance, WiMAX network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc, and provides scalability and mobility with high data rates with NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMAX to achieve a maturity level and become a successful technology, more research on security threats and solution to these threats need to be conducted.

This report is organized as follows. In section 2, WiMAX protocol architecture and security solutions are presented to provide background and detailed information about WiMAX securities specifications in the security sub-layer. Then vulnerabilities in WiMAX security will be discussed in section 3. In this section, some possible threats or vulnerabilities are discussed along with some proposed solutions to them. Finally, section 4 concludes the report.

2. WiMAX: protocol architecture and security solutions

In order to understand WiMAX security issues, we first need to understand WiMAX architecture and how securities specifications are addressed in WiMAX. This section provides background and detailed information about WiMAX securities specifications in the security sub-layer.

2.1. IEEE 802.16 protocol architecture:

The IEEE 802.16 protocol architecture is structured into two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer, as described in the following table [Jain08]:

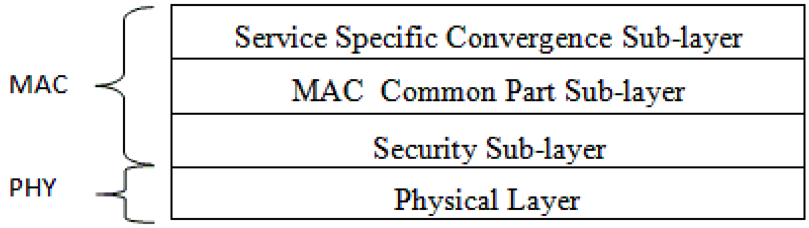

MAC
PHY
Service Specific Convergence Sub-layer
MAC Common Part Sub-layer
Security Sub-layer
Physical Layer

Figure 1. The IEEE 802.16 Protocol structure

MAC layer consists of three sub-layers. The first sub-layer is the Service Specific Convergence Sub-layer (CS), which maps higher level data services to MAC layer service flow and connections [Elleithy08]. The second sub-layer is Common Part Sub-layer (CPS), which is the core of the standard and is tightly integrated with the security sub-layer. This layer defines the rules and mechanisms for system access, bandwidth allocation and connection management. The MAC protocol data units are constructed in this sub-layer. The last sub-layer of MAC layer is the Security Sub-layer which lies between the MAC CPS and the PHY layer, addressing the authentication, key establishment and exchange, encryption and decryption of data exchanged between MAC and PHY layers.

The PHY layer provides a two-way mapping between MAC protocol data units and the PHY layer frames received and transmitted through coding and modulation of radio frequency signals.

2.2. WiMAX security solutions:

By adopting the best technologies available today, the WiMAX, based on the IEEE 802.16e standard, provides strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization. In WiMAX, most of security issues are addressed and handled in the MAC security sub-layer as described in the following figure:

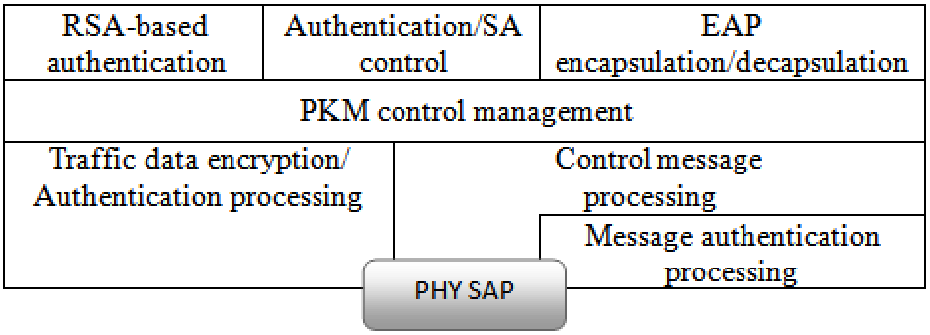

RSA-based authentication
Authentication/SA control
EAP encapsulation/decapsulation
PKM control management
Traffic data encryption/ Authentication processing
Control message processing
Message authentication processing
PHY SAP

Figure 2 . MAC Security sub-layer

Two main entities in WiMAX, including Base Station (BS) and Subscriber Station (SS), are protected by the following WiMAX security features:

Security association: A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share [Bogdanoski08]. Each SA has its own identifier (SAID) and also contains a cryptographic suite identifier (for selected algorithms), traffic encryption keys (TEKs) and initialization vectors.

Public key infrastructure: WiMAX uses the Privacy and Key Management Protocol (PKM) for secure key management, transfer and exchange between mobile stations. This protocol also authenticates an SS to a BS. The PKM protocol uses X.509 digital certificates, RSA (Rivest-Shamir-Adleman) public-key algorithm and a strong encryption algorithm (Advanced Encryption Standard – AES). The initial draft version of WiMAX uses PKMv1 which is a one-way authentication method and has a risk for Man-in-the-middle (MITM) attack. To deal with this issue, in the later version (802.16e), the PKMv2 was used to provide two-way authentication mechanism. The following figure provides an overview of public key infrastructure in WiMAX:

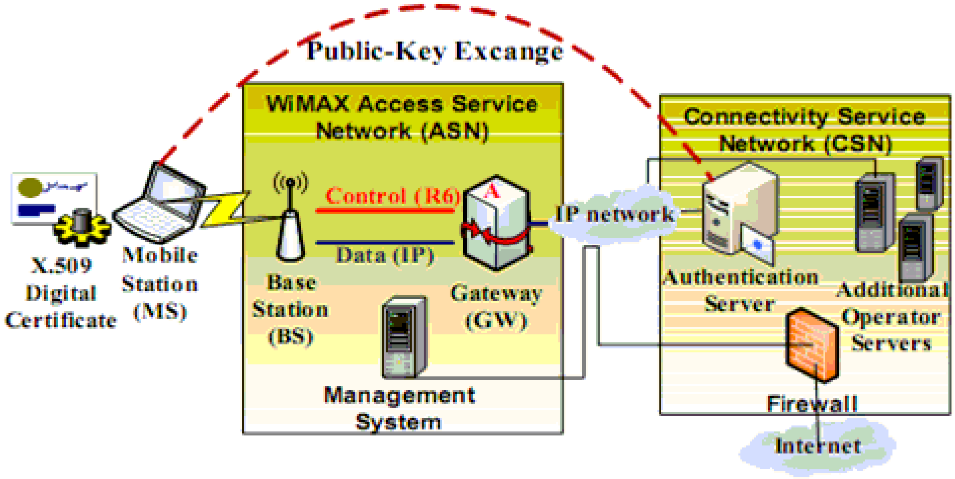


Figure 3 . Public Key Infrastructure in WiMAX [Bogdanoski08].

Device/User Authentication: Generally, WiMAX supports three types of authentication which are handled in the security sub-layer.

The first type is RSA-based authentication which applies X.509 certificates together with RSA encryption. The X.509 certificate is issued by the SS manufacturer and contains the SS's public key (PK) and its MAC address. When requesting an Authorization Key (AK), the SS sends its digital certificate to the BS, the BS validates the certificate, and then uses the verified PK to encrypt an AK and pass it to the SS.

The second type is EAP (Extensive Authentication Protocol) based authentication in which the SS is authenticated by an X.509 certificate or by a unique operator-issued credential such as a SIM, USIM or even by user-name/password. The network operator can choose one of three types of EAP: EAP-AKA (Authentication and Key Agreement), EAP-TLS (Transport Layer Security) and EAP-TTLS MS-CHAP v2 (Tunneled Transport Layer Security with Microsoft Challenge-Handshake Authentication Protocol version 2).

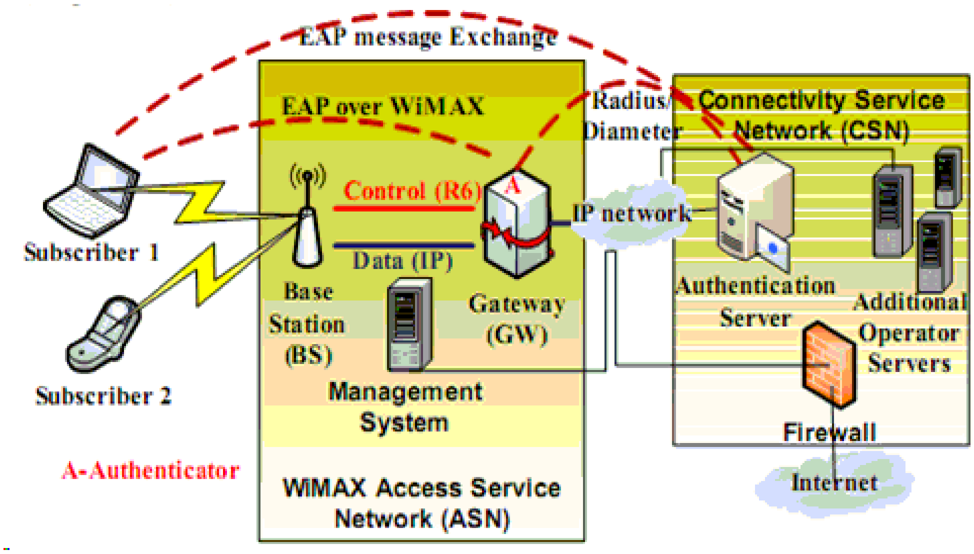


Figure 4. EAP-based authentication [Bogdanoski08].

The third type of authentication that the security sub-layer supports is the RSA-based authentication followed by EAP authentication.

Authorization: Following the authentication process is the authorization process in which SS requests for an AK and a SAID from BS by sending an Authorization Request message. This message contains SS�s X.509 certificate, encryption algorithms and cryptographic ID. The BS then interacts with an AAA (Authentication, Authorization and Accounting) server to validate the request from the SS, and sends back an Authorization Reply which includes the AK encrypted with the SS’s public key, a lifetime key and an SAIS.

Data privacy and integrity: WiMAX adopts the AES algorithm for encryption. “The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key”[Wiki_AES]. Since DES is no more secure enough, AES is recommended in WiMAX with many supported modes: CCM-Mode and ECB-Mode (in IEEE 802.16-2004), CBC-Mode, CTR-Mode, AES-Key-Wrap.

WiMAX has been designed carefully with security concerns but it is still vulnerable to various attacks. The following section will present these security issues in WiMAX.

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 [Narsreldin08]. 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 in 2.1, WiMAX security is implemented in the security sub-layer which is above the PHY layer. Therefore the PHY is unsecure [Barbeau05] and it is not protected from attacks targeting at the inherent vulnerability 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.

3.1.1. 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” [Barbeau05]. 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 [Poisel03] which teaches jamming techniques.

Solutions: According to Michel Barbeau[Barbeau05], 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.

3.1.2. Scrambling attack

Also described in [Barbeau05], 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 an 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” [Barbeau05].

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 [Barbeau05].

3.1.3. Water torture attack:

According to D. Johnson and J. Walker[Johnson04] , this is also a typical attack in which an attacker force a 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.

3.1.4. 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 [Johnson04] . 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: WiMAX has fixed the security flaw of 802.16 by providing mutual authentication to defend these kinds of attacks.

3.2. Threats to the MAC layers

There are a lot of defects or flaws in WiMAX security solutions at the MAC layer. The vulnerabilities with MAC management messages are presented first in section 3.2.1 and section 3.2.2. Then vulnerabilities in authentication mechanism and some specific attacks are discussed.

3.2. 1. 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 as depicted in Figure 5.

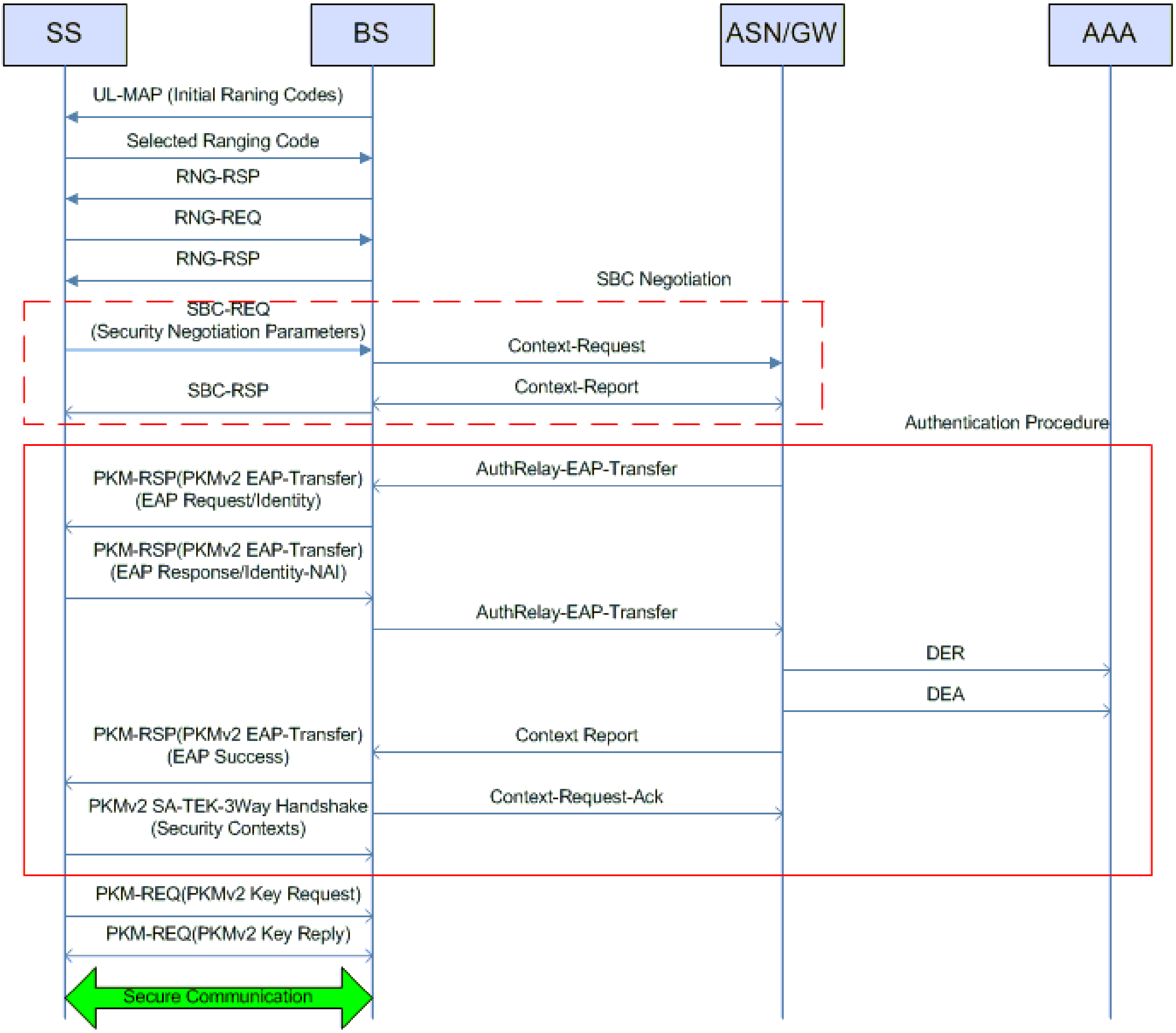


Figure 5. Initial Network Entry Procedure overview

The vulnerability of using Ranging Request-Response (RNG-REQ, RNG-RSP) 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 the least effective one, thus downgrading the service [Deininger07] [Naseer08]. An attacker can also spoof or modify ranging messages to attack or interrupt regular network activities. This vulnerability can lead to a DoS attack which will be presented in details in 3.2.4 section of this report.

Other initial network entry vulnerability: T. Shon and W. Choi presented a more general vulnerability of initial network entry in [Shon07]. 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 Figure 6.

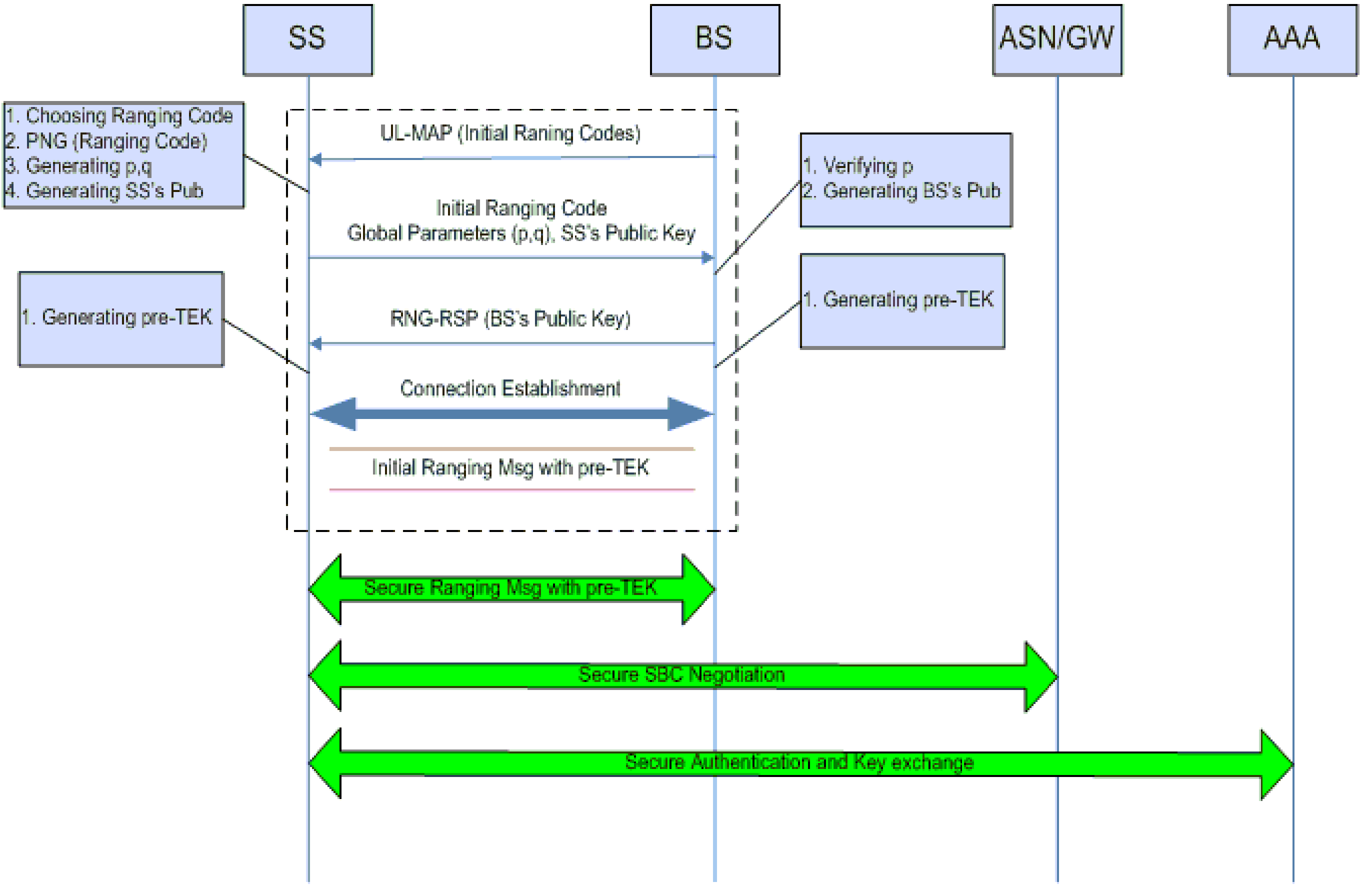


Figure 6. Proposed Network Initial Entry Approach

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.

3.2.2. Threats to Access network Security

In [Shon07], T. Shon and W. Choi also reviewed a 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 network functions 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 to subscribers. This AAA-architecture based model is illustrated in the following figure.

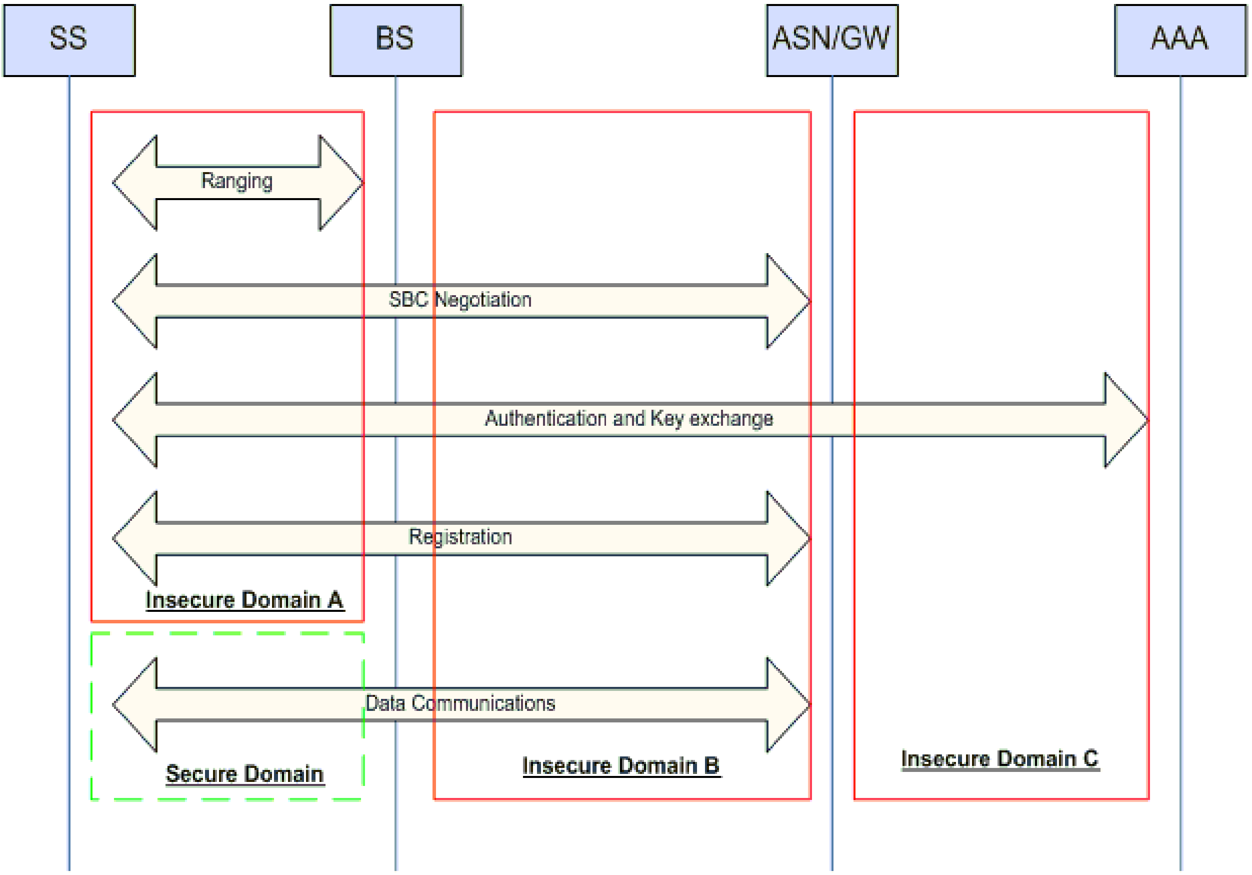


Figure 7. Access Network Security overview.

T. Shon and W. Choi divided the model into three insecure domains and one secure domain [Shon07]. 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. 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 the following figure:

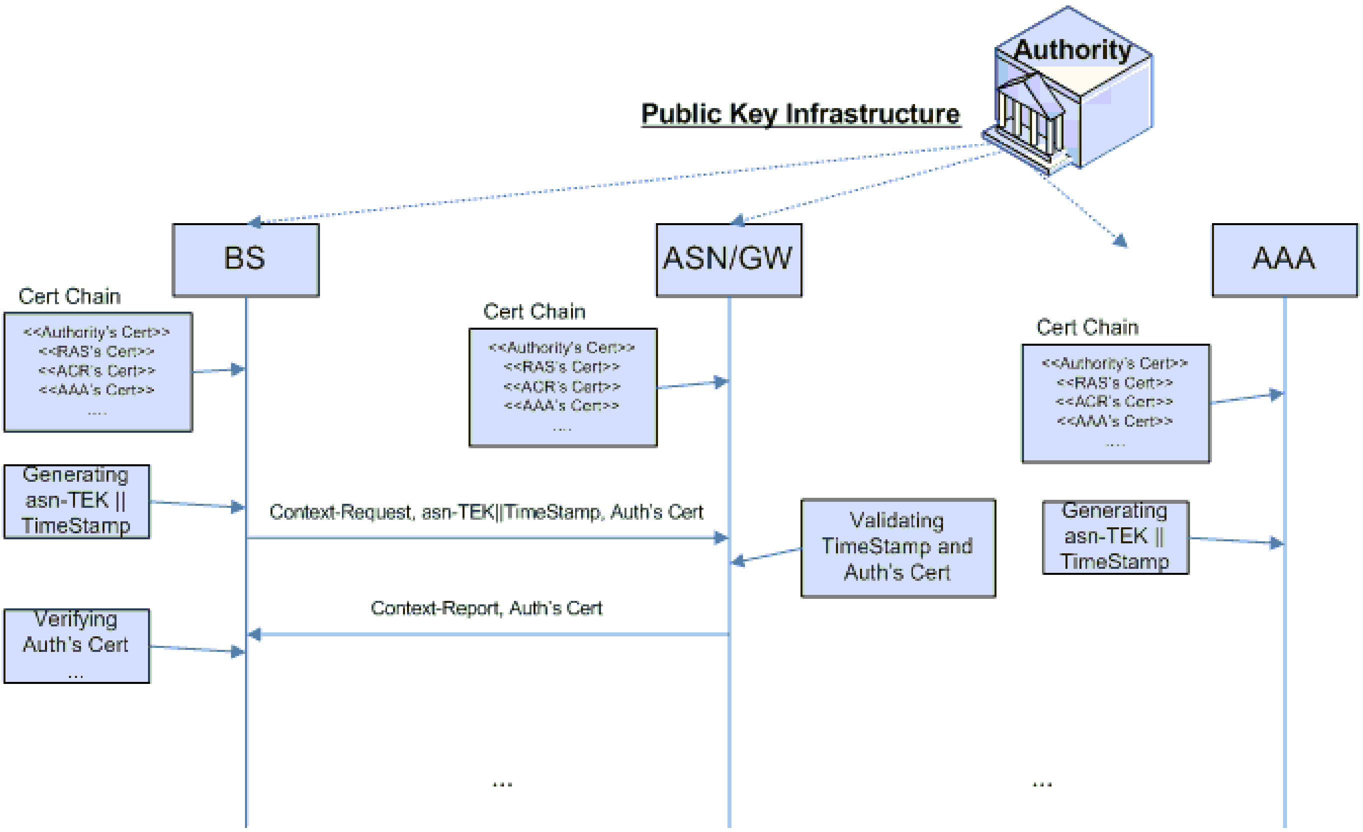


Figure 8. Proposed Access Network Approach.

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.

3.2. 3. Threats to authentication

Many serious threats also arises 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 [Barbeau05] 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.

- *Identity theft:*
  An attacker reprogram a device with the hardware address of another device. The address can be stolen by interfering the management messages.

- Rogue BS attack:
  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 in 802.16 and its later version-PKMv2:

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 [Xu06].

- *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 worse 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. Xu et. al. concluded that Basic PKM has many flaws such that it provides almost no guarantees to SS about the AK [Xu06]. 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.

3.2.4. Other threats

Some serious attacks can exploit vulnerabilities in many aspect 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 which is already presented in part 3.2.2 of this report. In 3.2.2, it is known that WiMAX standard does not provide any security mechanism for the SSBC negotiation parameters. Tao Han et. al. in [Han08] 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 [Shon07].

Denial of Service attack:

Comprehensive surveys [Naseer08] [Altaf08] [Elleithy08] [Park08]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 include the following:

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

An 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.

- *DoS attacks based on Mobile Neighbor Advertisement (MOB_NBR_ADV) message:*
  MOB_NBR_ADV message is sent from serving BS to publicize the characteristics of neightbor 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.

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

- *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.

- *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. This message is protected by HMAC but is still potential to be used to perform a DoS attacks.

In order to prevent DoS attacks, we first need to fix the vulnerabilities in the initial network entry. This work is discussed in section 3.2.1 of this report. Sheraz Naseer et. al also 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 [Naseer08].

4. Summary

In this report, 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. At MAC layer, critical threats include eavesdropping of management messages, masquerading, management message modification or DoS 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.

List of Acronyms

AAA	Authentication, Authorization, Accouting
AES	Advanced Encryption Standard

AK	Authorization Key
AKA	Authentication and Key Agreement
BS	Base Station
BWA	Broad Wireless Access
CBC	Cipher Block Chaining
CPS	Common Part Sublayer
DES	Data Encryption Standard
DH	Diffie-Hellman
DoS	Denial of Service
EAP	Extensive Authetication Protocol
HMAC	Hashed Message Authentication Code
KEK	Key Encryption Key
LOS	Line of Sight
MAC	Message Authentication Code
MITM	Man In The Middle
NLOS	Non-line of Sight
PHY	Physical
PKI	Public Key Infrastructure
PKM	Privacy and Key Management
PKMv1	Privacy and Key Management Version 1
PKMv2	Privacy and Key Management Version 2
RSA	Rivest-Shamir-Adleman
SA	Security Association
SS	Subscriber Station
TEK	Traffic Encryption Key
WiMAX	Worldwide Interoperability for Microwave Access

References

[Wiki_802.16] http://en.wikipedia.org/wiki/802.16

[Wiki_WiMAX] http://en.wikipedia.org/wiki/WiMAX

[WiMAXABT] http://www.wimaxforum.org/about

[Wiki_AES] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[Jain08] http://www.cse.wustl.edu/~jain/cse574-08/

[Johson04] David Johnson and Jesse Walker, "Overview of IEEE 802.16 Security", Intel Corp, IEEE Security and Privacy, 2004 http://portal.acm.org/citation.cfm?id=1009288

[Barbeau05] Michel Barbeau, �WiMax/802.16 Threat Analysis�, Proceedings of the 1st 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

[Narsredlin08] Mahmoud Narsreldin, Heba Aslan, 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

[Deininger07] Andreas Deininger, Shinsaku Kiyomoto, 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

[Elleithy08] Abdelrahman Elleithy, Alaa Abuzaghleh, Abdelshakour Abuzneid, �A new mechanism to solve IEEE 802.16 authentication vulnerabilities�, Computer Science and Engineering Department University of Bridgeport, Bridgeport, CT.
http://www.asee.org/activities/organizations/zones/proceedings/zone1/2008/Professional/ASEE12008_0022_paper.pdf

[Han08] 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

[Xu06] Sen Xu, Chin-Tser Huang, �Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions�, 3rd International Symposium on Wireless Communication Systems, ISWCS 2006.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4362284

[Shon07] Taeshik Shon, Wook Choi, �An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions�, Lecture notes in computer science, Springer, 2007.
http://www.springerlink.com/content/d03p14w7720x842l/

[Naseer08] Sheraz Naseer, 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

[Poisel03] R. Poisel, �Modern Communications Jamming Principles and Techinques�, Artech House Publishers, 2003.
Click here to order from Amazon.com

[Altaf08] Ayesha Altaf, Rabia Sirhindi, Attiq Ahmed, �A Novel Approach against DoS Attacks in WiMAX 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

[Park08] 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

[Bogdanoski08] Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski, �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

Last Modified: April 20, 2009.
This and other papers on latest advances in network security are available on line at http://www.cse.wustl.edu/~jain/cse571-09/index.html
SHARE Back to Raj Jain's Home Page