International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 28, Issue 01) and (Publishing Month: March 2016)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Securing your Wimax Network

Jamal Omer Alhassan Mhmoud[1] and Dr. Hala ELdaw Idris[2]

[1]Faculty of Engineering, Computer Engineering, Al-Neelain University, Khartoum, Sudan
shongor999@yahoo.ca

[2]Faculty of Engineering, Al-Neelain University, Khartoum, Sudan

Publishing Date: March 30, 2016

Abstract

The paper discusses the operational (hardware & software) and services offer security requirements in an wimax system that are used in the transfer of secure digital data .The paper gives an overview on the security procedure like encryption, digital certificates ,key agreement, digital signatures and tunneling that are used to enforcement data protection during data transfer . Beside that the paper also discusses the security requirements in the system to prevent possible internal attacks by applying AAA (Authentication& Authorization& Accounting). The paper also gives a brief on the security enforced in a device itself by use proprietary security polices and security measure during the production of the device.

Keywords: *Wimax, Attacks and Threats, Security Issues.*

1. Introduction

WiMAX stands for Worldwide Interoperability for Microwave Access. It is the technology aimed to provide wireless data access over long distances. It is based on Institute of Electrical and Electronics Engineers (IEEE) 802.16 which was formed in June 2001 to promote conformance and interoperability of the standard. The WiMAX forum and IEEE 802.16 subcommittee are both involved in the development of open standards based broadband wireless networks. The Wimax equipment is getting increasingly connected more and more in network communications due good technical specification. The users of these devices are now able to execute almost all the network & internet applications that run in a Mobile or fixed on this communication system. These devices also handling secure data through public networks that needs protection from unauthorized access and thus the security requirements in Wimax Network have become urgent.

The secure data falls in different categories requiring different levels of security. According to whose interest the protection of the data is, the secure data can be classified as private data and restricted data. The secure data not only requires protection during data transfer but also while handling the data at the end user devices. Vulnerability at the end user device, like easy access to the secret keys that are used to encrypt or decrypt the data, can easily turn down the entire security measures. The protocol involved for the secure transmission of either of the aforementioned contents through a public network uses more or less the same techniques but the handling of the user restricted data at the user's end involves much more care as the content is protected from the user itself! Thus Wimax Network must implement procedure or protocol for secure data transfer and also should enforce security methods to defeat unauthorized access to control device. The IEEE 802.16 protocol architecture two main layers: the Medium Access Control (MAC) layer and the Physical (PHY) layer [Jain08]

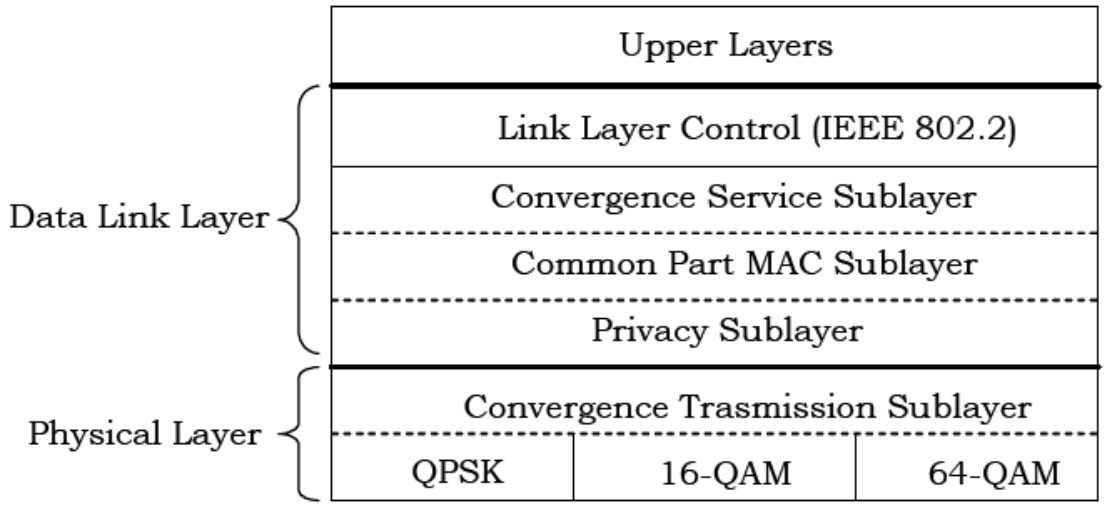

Figure 1: The IEEE 802.16 Protocol [IEEE, 2004]

The security needs for Wimax thus can be classified into two:

- Security requires for data transfer.
- Security requires to device.

2. Security require for data transfer

The data in a public network passes through a number of entrusted intermediate sites. Therefore the secure data must be scrambled in such a way that the data will be useless or not important for anyone who is having unauthorized access to the secure data. This can be achieved with the help of cryptographic methods such as Encryption, Key Agreement, Digital Signatures and Digital Certificates in wimax network to achieve data security the following section will explain this security problem in IEEE 802.16.

2.1 Data privacy & integrity

AX used AES algorithm for cipher. "designed by Rijmen-Daemen in Belgium has 128/192/256 bit keys, 128 bit data the algorism repeat the basic equations to convert the plain-text into cipher-text., processes data as block of 4 columns of 4 bytes, AES is recommended in IEEE 802.16. WiMAX has been designed accurately with complete security but it is still include vulnerable to various attacks.

2.2 digital certificates:

WiMAX supports allot off types of authentication which are impeded in the privacy sub-layer.(RSA) algorithm and X.509 digital certificates work together to achieve encryption mechanism to the MAC address of SSs to network (AK), SSs etch digital certificates with the BS, after the BS verification it used the PK to encrypt and transfer it to the SS. The network manager can choose one of them to achieve the mechanism.

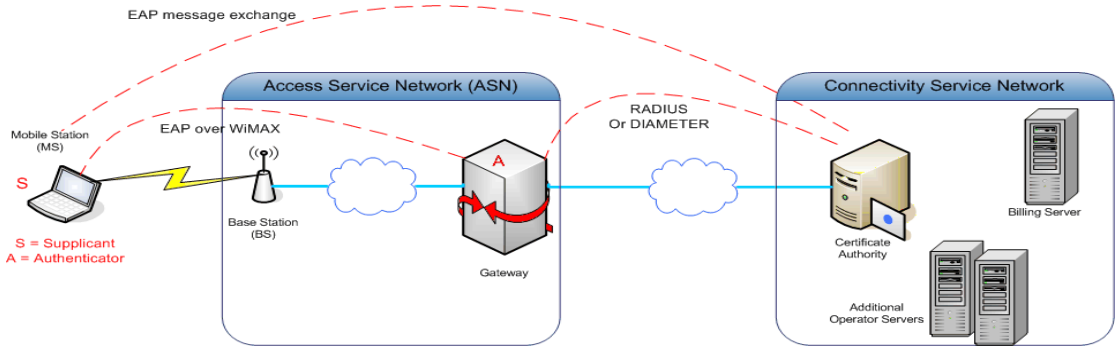

Figure 2: digital certificates verification [Bogdanoski08]

2.3 Public key Instructor

IEEE 802.16 uses the Privacy & public Protocol (PKM) for secure key management, keys exchanged between MSs, beside that the protocol verification SS to a BS. The PKM protocol uses digital certificates X.509 , RSA public-key algorithm and a strong encryption algorithm (AES). The late version of IEEE 802.16 uses PKMv1 (1-way authentication) but it's not secure for (MITM) attack. This problem was solved by PKMv2 to provide 2-way authentication techniques. The next figures explain an construes public key stricter [2]:

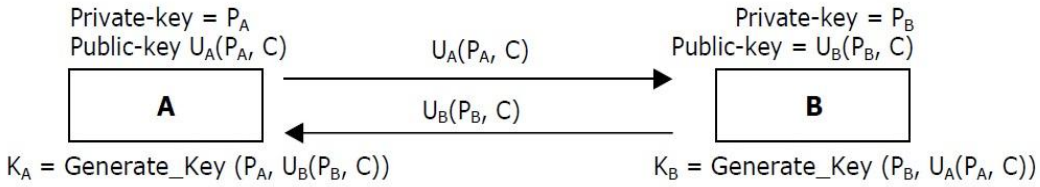

Figure 3: Public Key Exchange [2]

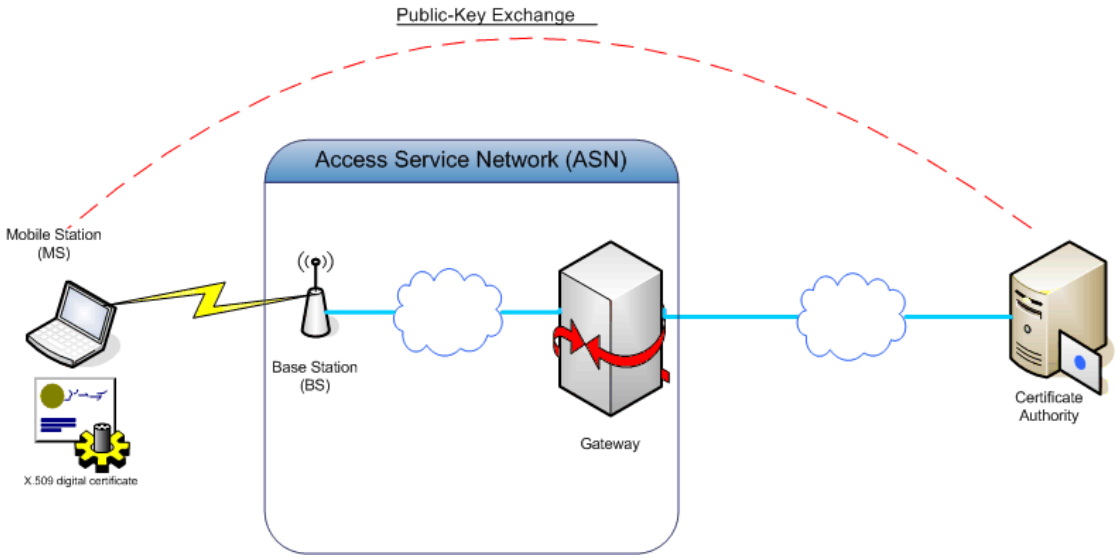

Figure 4: Public Key Exchange

2.4 Digital Signatures

A security association (SA) is a set of security opted parameters handiling between BS and one or more of SSs [Bogdanoski08]. Each SA has its own (SAID), (TEKs) and initialization modulus [Bogdanoski08].

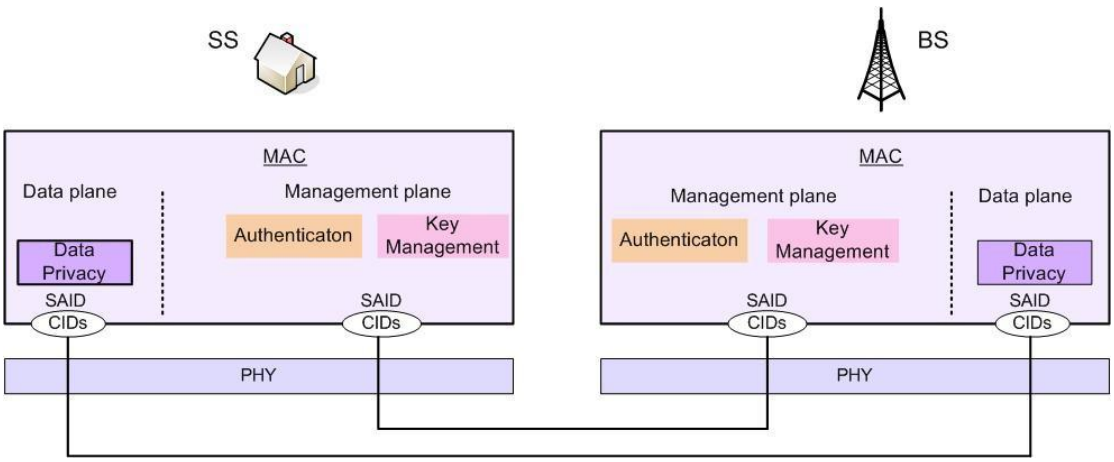

Figure 5: security Association [Aikaterini.2004]

2.5 Authorization SA (Authentication)

The authorization SA has a 60bitauthorization key (AK) and a 4bit quantity to identify the AK. To identify SS, it uses an X.509 certificate. The lifetime of AK 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)

Figure 6: Authorization pressing[Wongthavarawat, 2005]

3. Security requires to device

Whether it is the private-key of any public-key algorithm as discussed in data section or it is any previously negotiated shared secret between the devices, the security of data transferred depends in the secrecy of these keys. To enforce additional security, some cryptographic algorithms may also specify a set of constant values that should not be disclosed from the device. These secret keys and secret values stored in the device that requires protection from unauthorized exposure are referred as 'secret keys' in this document.

The secret keys are stored inside the device, some even for the lifetime of the device. Hardware and software security measures implemented in the device must defeat any attempts of unauthorized access to retrieve these secret keys. the security of all the copy-protected content handled by that device. One vulnerable device can thus results in helping an unauthorized device to access the copy protected content. The following section gives an example of prototype SoC to discuss the hardware and software support required to enforce the security within the device and thereby defeating the physical attack that compromises the security of the device [1]. The PKM protocol uses, RSA public key algorithm, X.509 digital certification, and strong encryption algorithm to carry out key exchanges between SS and BS (Xu et al, 2006). 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].

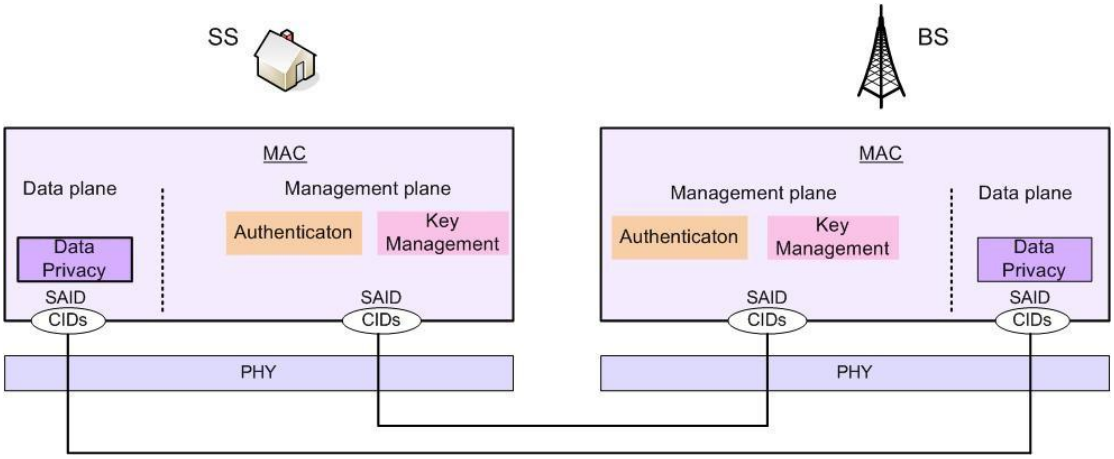

Figure 7: IEEE 802.16 Security Associations (SA), (Aikaterini, 2004)

3.1. System Time

The digital certificate of a device generally comes with validity period. The validity periods varies across different protocol implementation. Some protocols like SSL specify a fixed validity period of few years or decades whereas other protocols like DTCP specifies infinite validly for a certificate. The system time in an embedded device will generally have interfaces to user to set or modify the system time. For certificate verification process the device should maintain a system time that is different from the system time modified by the user so that the users are not able to modify the system time and make the device accept an expired certificate. Also Network Time Protocol :(one or more devices are design at edams the master clock keeper for all network system (known as an NTP master)) to applied security mechanisms.

3.2 Keys and certificate impeded during device manufacture

[Bogdanoski08] In many cases, the different hardware and software components in a communication device are supplied by different vendors. The hardware vendors provide the hardware component and the associated drivers for the device whereas the software vendor provides the software components. The device manufacturer or the deice vendor assembles these hardware and software components to make the product, which is marketed with an aim of attaining revenue. The secret key for each device has to be loaded in to the device during manufacture. It is usually is the interest of the device vendors to protect the secret keys of the devices and thus the device vendors may refrain from sharing the secret keys to different hardware and software vendors. But at least some part of the software has to use the shared secret and also as explained in previously, the communication equipment need hardware support to contain secret key. Two methods are explained here to handle the secret keys during production of the device.

1. The hardware vendor supplies hardware with write-protected Secure ROM, preprogrammed with unique random number for each device or for a set of devices. This random number can be used as a hardware master key to encrypt device secret keys.

2. The hardware vendor supplies hardware with programmable Secure ROM that can be programmed by the device manufacturer with device secret keys.

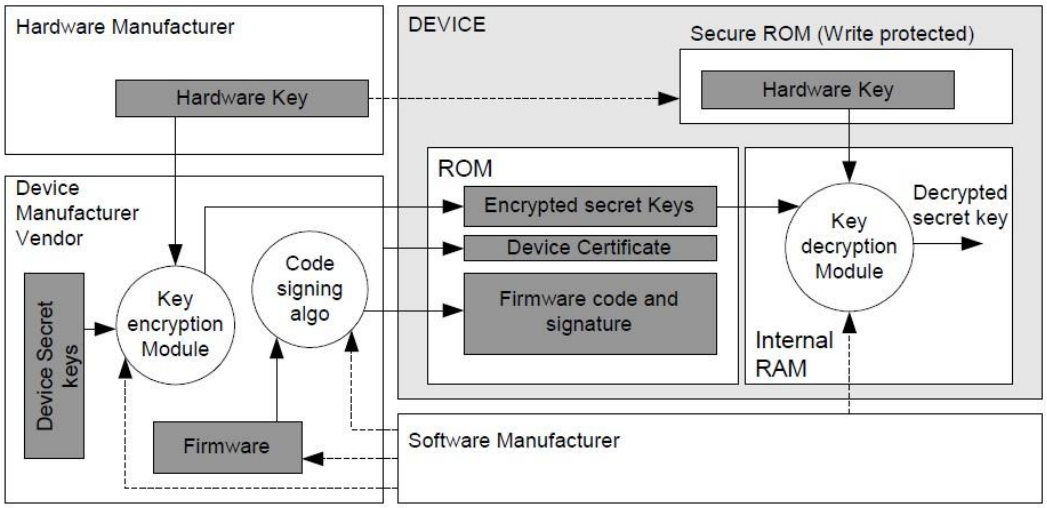

Figure 8: vendor supplies the hardware with pre-programmed Hardware Key[13]

4. Security Risks & Vulnerabilities

In wireless networks, privacy is a primary concern for secure transmission. Resistance to interception and eavesdropping are other common threats. Message authentication is for integrity of the message and sender authentication. Availability guarantees that the services are not prevented from access by DoS attack. Ant replay identifies and disrepute any message that is a repeat of a past message (Xu et al, 2006). According to Xu, Matthews and Huang (2006), there are some typical attacks on authentication protocols. One common attack is Message replay attack on authentication and authenticated key formation protocols. They added, "If the messages are exchanged in an authentication protocol that do not carry proper freshness identifiers, then an opponent can easily get himself authenticated by replaying messages copied from a legitimate authentication session". Man in the middle attack usually associated in a communication protocol where common when mutual authentication is missing. Other known attacks that are likely to occur include parallel session attack, reflection attacks, interleaving attacks, attacks due to type flaw, attacks due to name omission, and attacks due to misuse of cryptographic services. 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.

4.1. Threats to the PHY layer

As you see in fig [1], IEEE802.16 security function is implemented in the privacy sub-layer and the PHY layer does not contain security attributes. Therefore the PHY layer is unsecure and it is not immune from attacks [Barbeau05], wireless vulnerability and potential solutions presented following.

4.1.1. Jamming attack

M. Barbeau said "achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel" [Barbeau05]. They are tow type of Jamming can be either intentional or unintentional. It is easy to perform a jamming attack and easy to detect [Poisel03]

Solutions: According to Michel Barbeau [Barbeau05], you can prevent wireless network

against jamming by saving a good rate for signal to interference or by increasing the bandwidth of channel using spreading techniques such (FHSS) or (DSS). Furthermore, easy to detect jamming located by utilizing direction finding equipment.

4.1.2. Scrambling Attack

Also described in [Barbeau05], it's a type of jamming but only impact during short time on WiMAX frames or parts of it. 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].

4.1.3. Water torture attack:

D. Johnson and J. Walker [Johnson04] Saied "this is also a typical attack in , which an attacker sends a series of frames to drain out the receiver's battery. Additionally, attacker with a properly positioned Radio Frequency (RF) receiver can interrupt the messages sent through wireless, and therefore a security mechanism in the design is required of attack is considered even more destructive than a like (DoS) attack since the SS which is a usually mobile equipment is likely to have midget resources .

Solutions: Because the query rate from each client IP address is quite low and because there is no response amplification, it is difficult to determine simply from packet rates or bandwidth consumption which client IP-addresses are participating in the attack. And because the names change periodically, it can be time consuming to track and block queries to the domains being used in the attack. However, here are some specific steps you can take to minimize the impact of the attack:

- Check your timeout settings. Most resolvers allow you to specify the initial and subsequent timeout intervals. Make sure that these values are not too high (if they are, they will tie up resolver resources longer than necessary before a query fails).
- Increase the number of outstanding recursive queries if you have sufficient RAM on your server. This will give the resolver more resources to work with.
- Specify a non-zero TTL for the negative responses so that if a client requests the same non-responsive name more than once, the SERVFAIL answer is cached. By RFC, you should be able to specify up to a 5 minute TTL.

4.1.4. Other threats:

Beside a pave threats to the PHY layer wimax is also vulnerable to other attacks like fraud attacks in which an attacker with an adequate radio transmitter, wireless channel replay attacks and radio intercepted [Johnson04].

Solutions: WiMAX has fixed the security flaw of 802.16 by applying cooperative authentication to detect and fixed these kinds of these threats.

4.2. Threats to the MAC layers

Table 1 lists the values of eavesdropping, an undetected listener of the communication, for management messages and user traffic separately.

Table 1: MAC Layer Threats

THREAT	*ALGORITHM USED*	*PROBABILITY*	*IMPACT*	*RISK*
Jamming *Scrambling*		*3* *2*	*1* *1*	*3* *2*
Eavesdropping Management Message		*3:3*	*2:1*	*6:3*
Eavesdropping Traffic	*DES – CBC* *AES – CCM*			
BS or MS Masquerading	*Device List* *X.509 certificate-based* *EAP*	*3* *2:1* *2:2*	*3* *3:2* *3:2*	*9* *6:2* *6:4*
Management Message Modification	*NO MAC* *SHA –1 MAC* *AES MAC*	*3* *2* *1*	*3* *3* *3*	*9* *6* *3*
THREAT	***ALGORITHM USED***	***PROBABILITY***	***IMPACT***	***RISK***
Data Traffic Modification	*Without AES* *With AES*	*3* *1*	*1* *1*	*3* *1*
DOS on BS or MS	*EAP, SHA –1, AES, MAC*	*3:3*	*3:2*	*9:6*

The vulnerability of using (RNG-REQ, RNG-RSP) messages:

The RNG-REQ is initial negotiation message between SS and network access point trying to join a network also RNG-RSP message used to replacement uplink and downlink channel of the SS [Deininger07] [Naseer08].

Solution: Shon [07] proffer a solution to this vulnerability by using Diffie Hellman key agreement scheme as depicted in Figure 9.

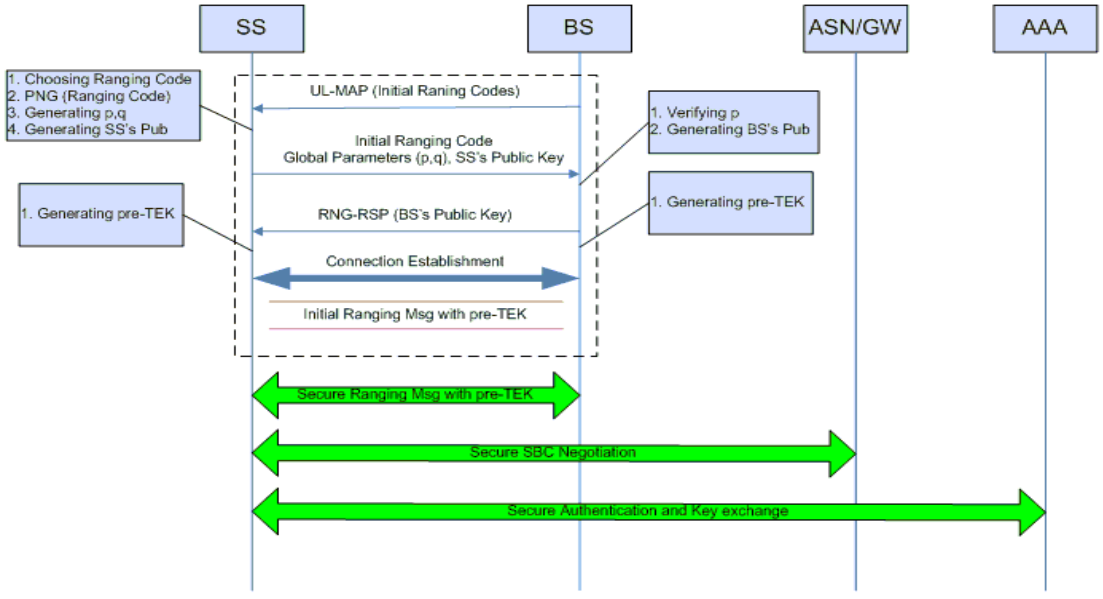

Figure 9: Proposed Network Initial Entry Approach

4.2.1. Threats to Access network Security

In [Shon07], T. displays vulnerability in wimae access network security. 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.

4.2.2. 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:

A masquerade attack is an attack that uses a counterfeit identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. The attack can be either inside or outside organization.

Identity Theft:

Identity theft is the illegal used someone identity for fraud network authentication. identity theft involves using personal information to access services in privacy area. However it's difficult to successfully perform this kind of attack in WiMAX but we can midget it by Appling powerhouse's authentication such as PKMv2 .

Attacks on basic PKM authentication protocol:

By adopting new version of PKM, WiMAX fixes many flaws in PKMv1 such as vulnerability to MITM due to the lack of mutual authentication [Xu06]. Attacker eavesdrop messages sent by SS and then perform a replay attack against the BS. 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.

Attacks on late Version PKM:

This late version does not protect the BS and it's not immune from a replay attack.

Attacks on PKMv2:

It provides a three-way authentication with a verification message from SS to BS. The potential attacks replay and an interleaving.

4.2.3. Other threats

Allot of serious attacks can exploit vulnerabilities in MAC layers .the two famous destructive attacks can be MITM and DoS attacks.

Man in the middle attack:

Although WiMAX immune against 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 late, it is known that 802.16 standard does not provide any security techniques for the SSBC negotiation parameters. [Han08] also proposed their solution to this kind of attack which they called "SINEP". Their method is based on Diffie-Hellman (DH) key exchange protocol.

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 . attacks may include 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.

5. Conclusion

In this paper, security solution, various vulnerabilities and possible attacks to WiMAX network system have been represent and justification. The attackers directed to both layers (PHY and Mac), jamming attack a major threat to the PHY layer. Eavesdropping, masquerading, modification and DoS present imported threat to MAC layer , allot off this vulnerabilities have been, reduce in recent version but some still current and we need additional solution Therefore Communication Company, internet service provider and consulted of IT should situates all security problem in consideration before implementation the Wimax technology.

6. List of Acronyms

AAA Authentication, Authorization, A counting
AK Authorization Key
AKA Authentication and Key Agreement
BS Base Station
FHSS frequency spread spectrum
DSS direct sequence spread spectrum
CPS Common Part Sub layer
DES Data Encryption Standard
DH Diffie-Hellman
DoS Denial of Service
EAP Extensive Authentication 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 fo Microwave Access
AES Advanced Encryption Standard
(RNG-REQ, RNG-RSP) Ranging Request-Response

References

[1] [Jain 08] http://www.cse.wustl.edu/jain/cse574-08
[2] Anoop MS, Elliptic Curve Cryptography - implementation guide, May 2007, Available at http://msitbox.blogspot.com/2008/03/elliptic-curve-cryptography.html
[3] [Bogdanoski08] 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
[4] Johnston, D., Walker, J. (2004). Overview of IEEE802.16 Security, retrieved on 1st May, 2006 from http://mia.ece.uic.edu/~papers/WWW/Bubbles/segment/WiMax_Security.pdf
[5] Eklund, C., Marks, R.B., Stanwood, K.L., & Wang, S.(2002) IEEE Standard 802.16: A Technical Overview of the Wireless MAN™ Air Interface for Broadband Wireless Access, retrieved on 1st May, 2006 from
[6] Aikaterini, A.V. (2004). SECURITY OF IEEE 802.16, retrieved on 1st May, 2006 from http://www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-332.pdf
[7] [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
[8] [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

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

[10] [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

[11] [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

[12] [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

[13] [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

[14] Xu, S., Matthews, M. & Huang, C. (2006). Security Issues in Privacy and Key Management Protocols of IEEE802.16, retrieved on 1st May, 2006 from http://www.cse.sc.edu/~huangct/acmse06cr.pdf