ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

ANALYSIS OF SECURITY ISSUES OF MOBILE WIMAX 802.16E AND THEIR SOLUTIONS

Gaurav Soni

Assistant Professor, Department of Electronics and Communication Engineering,
Amritsar College of Engineering and Technology,Amritsar,India

Sandeep Kaushal

Associate Professor, Department of Electronics and Communication Engineering,
Amritsar college of Engineering and Technology, Amritsar , India

ABSTRACT

This paper examines threats to the security of the Mobile WiMax/ 802.16e broadband wireless access technology. Threats associated with the physical layer and MAC layer are reviewed in detail. Threats are listed and ranked according to the level of risk they represent. This review work can be used to prioritize future research directions in Mobile WiMax/802.16e security.

KEYWORDS : Mobile WiMax, 802.16e, FFT , OFDMA, Security issues.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

INTRODUCTION

The Mobile WiMAX (Worldwide Interoperability for Microwave Access.) standard of 802.16e is divergent from Fixed WiMAX. It attracted a significant number of Forum members towards an opportunity to substantively challenge existing 3G technology purveyors.

The 802.16e standard adds OFDMA 2K-FFT, 512-FFT and 128-FFT capability. Sub-channelization facilitates access at varying distance by providing operators the capability to dynamically reduce the number of channels while increasing the gain of signal to each channel in order to reach customers farther away. The reverse is also possible. For example, when a user gets closer to a cell site, the number of channels will increase and the modulation can also change to increase bandwidth. At longer ranges, modulations like QPSK (which offer robust links but lower bandwidth) can give way at shorter ranges to 64 QAM (which are more sensitive links, but offer much higher bandwidth). Each subscriber is linked to a number of sub channels that obviate multi-path interference. The upshot is that cells should be much less sensitive to overload and cell size shrinkage during the load than before.

WiMAX systems are based on the IEEE 802.16-2004 and IEEE 802.16e-2005 standards which define a physical (PHY) layer and the medium access control (MAC) layer for broadband wireless access systems operating at frequencies below 11 GHz. The first of these standards, published in 2004, addresses fixed services, and the second, published in 2005, is intended for mobile services. In this report, we focus on mobile WiMAX systems based on the IEEE 802.16e-2005 standard [1]. The IEEE 802.16e-2005 specifications actually define three different PHY layers: Single-carrier transmission, orthogonal frequency-division multiplexing (OFDM), and orthogonal frequency-division multiple access (OFDMA). The multiple access technique used in

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

the first two of these PHY specifications is pure TDMA, but the third mode uses both the time and frequency dimensions for resource allocation. From these 3 PHY technologies, OFDMA has been selected by the WiMAX Forum as the basic technology for portable and mobile services. Compared to TDMA-based systems, it is known that OFDMA leads to a significant cell range extension on the uplink (from mobile stations to base station). This is due to the fact that the transmit power of the mobile station is concentrated in a small portion of the channel bandwidth and the signal-to-noise ratio (SNR) at the receiver input is increased. Cell range extension is also achievable on the downlink (from base station to mobile stations) by allocating more power to carrier groups assigned to distant users.

The 802.16e version of WiMAX also incorporates support for multiple-input-multiple-output (MIMO) antenna technology as well as Beamforming and Advanced Antenna Systems (AAS), which are all "smart" antenna technologies that significantly improve gain of WiMAX. The 802.16e standard is being utilized primarily in licensed spectrum for pure mobile applications. Many firms have elected to develop the 802.16e standard exclusively for both fixed and mobile versions.

In the following section we introduce the protocol structure of Mobile WiMAX. We then disussed the security issues and the preferable solutions.

BASIC PROTOCOL STRUCTURE OF MOBILE WIMAX

A Mobile WiMax/802.16e wireless access network consists of base stations (BSs) and mobile stations (MSs). The BSs provide network attachment to the MSs. As a serving BS, an MS selects the one which offers the strongest signal. In this analysis, the subscriber plays the role

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

of the user while a BS and a collection of served MSs play the role of system. The protocol architecture of WiMax/802.16 is structured into two main layers: the medium access control (MAC) layer and physical layer, see Figure 1. The central element of the layered architecture is the Common Part sub layer. In this layer, MAC protocol data units (PDUs) are constructed, connections are established and bandwidth is managed. The Common Part exchanges MAC service data units (SDUs) with the Convergence layer. The Common Part is tightly integrated with the Security sub layer. The Security sub layer addresses authentication, establishment of keys and encryption. The Security sub layer exchanges MAC PDUs with the Physical layer. The Convergence layer adapts units of data (e.g. IP packets or ATM cells) of higher level protocols to the MAC SDU format, and vice versa. The Convergence layer also sorts the incoming MAC SDUs by the connections to which they belong. The Physical layer is a two-way mapping between MAC PDUs and Physical layer frames received and transmitted through coding and modulation of RF signals.

The high-level MAC/PHY protocol structure for mobile WiMAX as specified in IEEE 802.16-2005[5] is shown in Fig. 1. This structure is built on a simple OFDMA-based PHY and a MAC layer composed of two sub layers: the CS and MAC common part sub layer (MAC CPS).

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

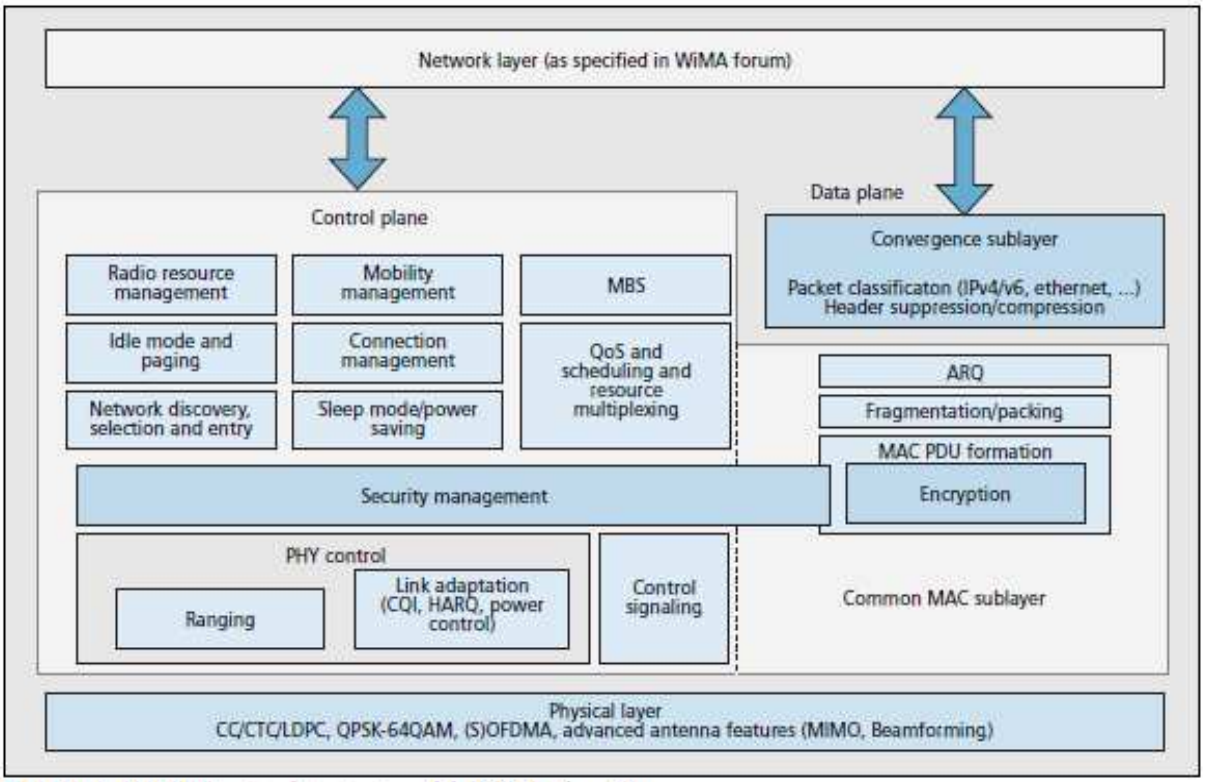

Figure 1: MAC/PHY protocol structure in mobile WiMAX[3]

The functional blocks in the CPS may be logically classified into upper MAC functions responsible for mobility control and resource management, and lower MAC functions that focus on control and support for the physical channels defined by the PHY. Although not formally separated in the standard, one may also classify functions into control plane and data plane functions. The upper MAC functional group includes protocol procedures related to radio resource control and mobility related functions such as:

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

- Network discovery, selection, and entry
- Paging and idle mode management
- Radio resource management
- Layer 2 mobility management and handover protocols
- QoS, scheduling, and connection management
- Multicast and broadcast services (MBS)

On the control plane, the lower MAC functional group includes features related to layer 2 Security and sleep mode management as well as link control and resource allocation and multiplexing functions. The PHY control block handles PHY signaling such as ranging, measurement/feedback (CQI), and hybrid automatic repeat request (HARQ) acknowledgment (ACK)/negative ACK (NACK). The control signaling block generates resource allocation messages. On the data plane, the ARQ block handles MAC ARQ function. For ARQ-enabled connections, the ARQ block logically splits MAC signaling data units (SDUs) into ARQ blocks and numbers each logical ARQ block. The fragmentation/ packing block performs fragmenting or packing MSDUs based on scheduling results from the scheduler block.

SECURITY ISSUES OF IEEE 802.16E

The previous IEEE 802.16d standard security architecture is based on PKMv1 (Privacy Key Management) protocol but it has many security issues. Most of these issues are resolved by the later version of PKMv2 protocol[4] in IEEE 802.16e standard which provides a flexible solution that supports device and user authentication between a mobile station (MS) and the home connectivity service network (CSN). Even though both of these standards brief the medium

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

access control (MAC) and physical (PHY) layer functionality, they mainly concentrate on point-to multipoint (PMP) networks. In the concern of security, mesh networks are more vulnerable than the PMP network, but the standards have failed to concentrate on the mesh mode.

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. We will here briefly discuss security vulnerabilities found in mobile WiMAX network. Vulnerabilities and threats associated with both layers in WiMAX (physical and MAC layers) are discussed along with possible solutions.

SECURITY FLAWS:-

This section explains the security flaws found in Mobile WiMAX.

a) PHY layer security issues: [5]: Scrambling and jamming are the two possible threats in PHY layer. For scrambling, the attackers will scramble the uplink slots of other MS's by their own data and make it unreadable for BS. Jamming at the physical layer is a kind of denial-of-service (DoS) attack that uses intentionally interfering radio communication by introducing the noise to disrupt the reception of messages in both uplink and downlink

b) MAC layer security issues in PMP Network:-The causes of MAC layer security issues are due to certain un-encrypted MAC management messages. The major security issues in PMP network are-

1. DoS/Reply attacks during MS Initial network entry

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

2. Latency during handover and unsecured pre authentication
3. Downgrade attack
4. Cryptographic algorithm computational efficiency
5. Bandwidth spoofing

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, PKMv2 authentication and registration process as depicted in Figure 2.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

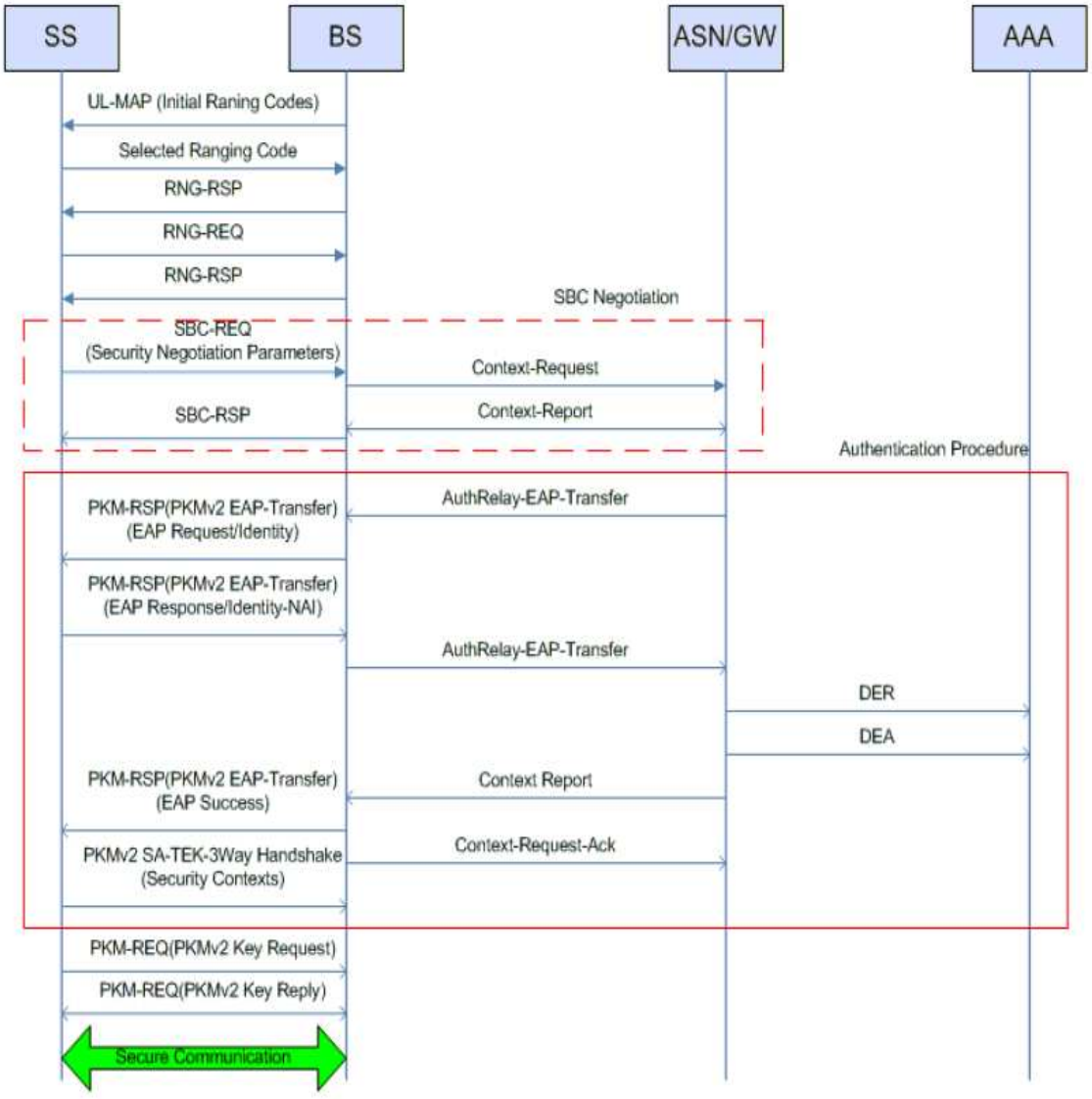

Figure 2: Initial Network Entry Procedure overview

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

a) 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, and 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 An attacker can also spoof or modify ranging messages to attack or interrupt regular network activities. This vulnerability can lead to a DoS attack. 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 To the above vulnerability: T. Shon and W. Choi [8] proposed a solution to this vulnerability by using Diffie-Hellman key agreement scheme as depicted in Figure 3.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

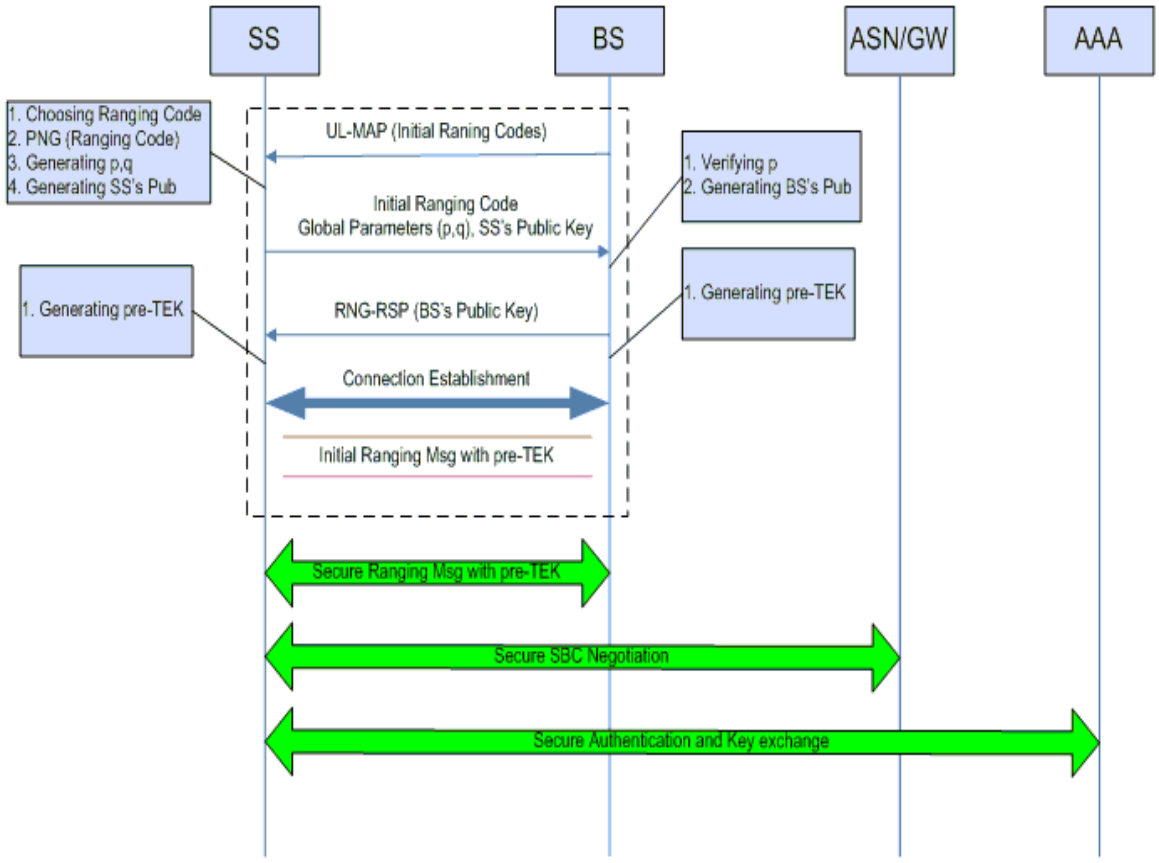

Figure 3: Proposed Network Initial Entry Approach

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 secret communication channels in the initial ranging procedure. After that, the SBC security parameters and PKM security contexts can be exchanged securely.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

2. Latency during handover and unsecured preauthentication: When handover occurs, the MS is preauthenticated and authorized by the target BS. The preauthentication and key exchange procedure increase the handover time, which affects the delay sensitive applications. In handover response message, BS informs the MS whether MS needs to do re-authentication with the target BS or not. If the MS is pre-authenticated by target BS before handover, then there is no need of device re-authentication but user authorization is still necessary. Two schemes are proposed to avoid the device re-authentication. The first scheme adopts the standard EAP but instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used using EMSK. Let MSKi and EMSKi be the master and extended master session keys in the ith authentication phase, then MS and AAA will generate the MSKi+1 and EMSKi+1 from the existing MSKi and EMSKi keys before handover takes place. So the device authentication and key (MSK, EMSK) exchange is avoided. The second method skips the standard EAP method and the device authentication is done by SA-TEK three-way handshake in PKMv2 process. Since this method avoids the standard procedures, it is not suitable for implementation. The handover latency can be reduced by simple preauthentication schemes. But pre-authentication schemes are inefficient and insecure. Another approach for reducing the handover latency is using PKI infrastructure for mutual authentication between target ASN and the MS before handover. Since the messages are encrypted using the public key, security is assured. Mobile IP (MIP) scheme is the new approach to solve the above issue. In this scheme, pre-negotiation with the target BS is in layer 3 MIP tunneling protocol.

Solution: For the above issue, MIP scheme is more efficient than the other methods, since the messages are more secured by tunneling protocol and it further reduces the latency during IP connectivity phase. If the MS doesn't have the MIP support, shared key-based EAP is efficient.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

3. Downgrade attack: The first message of the authorization process is an unsecured message from MS telling BS what security capabilities it has. An attacker could, therefore, send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked MS to agree on an insecure encryption algorithm.
Solution: A possible solution for downgrade attack is that the BS could ignore messages with security capabilities under a certain limit .

4. Cryptographic algorithm computational efficiency: The number of bits needed for encryption in RSA is more than Elliptic Curve Cryptography (ECC) for a required encryption, which increases the computation time.
Solution: ECC is the good substitute for RSA-based public key cryptography. ECC can achieve the same level of security as RSA with smaller key sizes. 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA. Another advantage of ECC is that it offers faster computational efficiency and well as memory, energy and bandwidth savings.

5. Bandwidth spoofing: In bandwidth spoofing, the attacker grabs the available bandwidth, by sending the un-necessary BW request message to BS.
Solution : To solve the bandwidth spoofing, the radio resource management in the BS should check the local policy function (LPF) and then allocates the bandwidth only if the MS has necessarily provisioned. This new recommendation is based on QoS model suggested by the WiMAX forum [2].

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

SOME OTHER FLAWS FOUND IN 802.16E ARE ANALYZED AS FOLLOWS:

Unauthenticated messages

Most of the management messages defined in IEEE 802.16e are integrity protected. This is done by a hash based message authentication code (HMAC) [6], or alternatively by a cipher based message authentication code (CMAC) [7]. However, some messages are not covered by any authentication mechanism. This introduces some vulnerability. Also, a couple of management messages are sent over the broadcast management connection. Authentication of broadcasted management messages is difficult since there is no common key to generate message digests. Furthermore, a common key would not completely protect the integrity of the message as mobile stations sharing the key can forge these messages and generate valid authentication digits.

MOB_TRF-IND

One of these broadcasted and unauthenticated management messages is the Traffic Indication message (MOB_TRF-IND). This message is used by the BS to indicate to a sleeping MS that there is traffic destined to it. Accordingly the MS is woken up from sleep mode. A unique Sleep ID is assigned to each MS in the base stations range. This sleep ID is a 10 bit value addressing 1023 different MSs. To accelerate message processing, the traffic indication message merges 32 Sleep IDs to one Sleep ID Group. Thus there exist 32 Sleep ID groups containing 32 Sleep IDs each. If the BS now receives traffic for a sleeping MS, the group ID for this MSs Sleep ID group is set to true. When receiving this message, every MS in the group will check if the traffic is addressed to it by verifying the traffic indication bitmap. This is a 32 bit value that is appended for each Sleep ID group and contains a bit for each individual MS in that group. If the corresponding bit in the traffic indication bitmap is set, the respective MS wakes up and can

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

receive the traffic. All other MSs can continue sleeping after verifying that the Sleep ID group indication bit of their group is set to false. An adversary could generate this message to frequently wake up MSs and stress their battery. If all bits in the Sleep ID group indication bitmap and all traffic indication bitmaps in this message are set to true, every reachable MSs in sleep mode is forced to wake up.

MOB_NBR-ADV

The Neighbor Advertisement message (MOB_NBR-ADV) is also not authenticated. The serving BS sends this message to announce the characteristics of neighbor BS to MSs seeking for handover possibilities. An adversary is able to keep back individual BSs by omitting information about their existence when he forges this message. This prevents MSs to handover to BSs which might have better characteristics as serving BS. He can also distribute wrong data about neighbor BSs or announce non existing BSs.

FPC

The broadcasted Fast Power Control message (FPC) is also not covered by any authentication mechanism. An FPC message is sent by the BS to one or multiple MS to adjust their transmitting power. By misusing this message it is possible to reduce the transmitting power of all reachable MSs to a minimum so that it is to low to be recognized by the BS. Thus, recursive power adjustments are necessary for the MS until the transmission power is strong enough to reach the BS again .Due to CSMA, the suddenly triggered cumulated power adjustment messages result in many uplink bandwidth requests. This causes collisions in uplink bandwidth request contention slots of the MSs and delays the time until each MS once again has the correct transmission power and can communicate with the BS. Another misuse of the message

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

is to set the transmitting power of all MSs to the maximum with the intention to stress their batteries.

MSC-REQ

An unauthenticated unicast message is the Multicast Assignment Request message (MSC-REQ). When sending this message the BS can remove a MS from a multicast polling group. A MS which receives such a remove message deletes itself from the polling group and subsequently sends a response back to the BS. This conversation is done using the primary management connection between BS and MS. A polling group is a group of MS which can get bandwidth from the BS via a polling mechanism. The BS therefore allocates an uplink transmission opportunity for each MS in the polling group. Then MSs can request uplink bandwidth using this transmission opportunity. As there is no authentication for this message an attacker can easily remove MSs from polling groups. If a MS is removed from a polling group, it has to use the mandatory contention based bandwidth allocation algorithm which results in a greater uplink delay.

DBPC-REQ

The Downlink Burst Profile Change Request message (DBPCREQ) is a further unicast message with no integrity protection. When the distance between BS and MS varies or the communication characteristics are changing due to another reason, the BS sends this message to change the MS burst profile to a more robust or a more effective one. The intention in misusing this message can be to temporarily break the communication between MS and BS by changing MSs burst profile so that it is not possible for the MS to demodulate the data received from the BS. Another flaw is the forgery of the Power Control Mode Change Response (PMC_RSP) message sent from the BS. With this message an adversary can directly change

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

the power control mode of the MS and also adjust its transmission power with the intention to disrupt the communication.

PMC-REQ

The broadcasted Fast Power Control message (FPC) is also not covered by any authentication mechanism. An FPC message is sent by the BS to one or multiple MS to adjust their transmitting power. By misusing this message it is possible to reduce the transmitting power of all reachable MSs to a minimum so that it is too low to be recognized by the BS. Thus, recursive power adjustments are necessary for the MS until the transmission power is strong enough to reach the BS again. Due to CSMA, the suddenly triggered cumulated power adjustment messages result in many uplink bandwidth requests. This causes collisions in uplink bandwidth request contention slots of the MSs and delays the time until each MS once again has the correct transmission power and can communicate with the BS. Another misuse of the message is to set the transmitting power of all MSs to the maximum with the intention to stress their batteries

MOB_ASC-REP

The Association Result Report (MOB_ASC-REP) is another un-authenticated message. When MS and BS are keeping association level 2, the BS does not directly have to answer a Ranging Request. Instead it is sending the Ranging Response over the backbone to the serving BS of the requesting MS. The serving BS collects all Ranging Responses of neighboring BSs and merges them to one association report message. This aggregated message is transmitted to the MS via the basic management connection. The ranging response message itself is integrity protected in most cases but the association report message is never. An adversary can change arbitrary response data in the message like time or power adjustments.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

RNG-REQ

For the Ranging Request (RNG-REQ) message the standard does not explicitly define when an authentication digest shall be appended. Here it should be stated that this message must always be covered by a digest when an Authentication Key (AK) is available. For initial network entry no authentication key is available but in most other cases an AK exists and the message can be protected. Besides there are other non authenticated messages but a forgery of their carried information can be considered as less dangerous for the operability of the protocol.

Unencrypted management communication

In Mobile WiMAX management messages are still sent in the clear. When a MS performs initial network entry, it negotiates communication parameters and settings with the BS. Here a lot of information is exchanged like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information and MS capabilities etc. Currently the complete management message exchange in the network entry process is unencrypted and the above mentioned information can be accessed just by listening on the channel. After initial network entry, the management communication over the basic and primary management connections remains unencrypted. As most of the management messages are sent on these connections, nearly all management information exchanged between MS and BS can be accessed by a listening adversary. The only messages which are encrypted are key transfer messages. An adversary collecting management information can create detailed profiles about MSs including capabilities of devices, security settings, associations with base stations and all other information described above. Using them data offered in power reports, registration, ranging and handover messages, a listening adversary is able to determine the movement and approximate position of the MS as well.

Shared keys in Multicast and Broadcast Service

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

The Multicast and Broadcast service offers the possibility to distribute data to multiple MS with one single message. This saves cost and bandwidth. Broadcasted messages in IEEE 802.16e are encrypted symmetrically with a shared key. Every member in the group has the key and thus can decrypt the traffic. Also message authentication is based on the same shared key. This algorithm contains the vulnerability that every group member, besides decrypting and verifying broadcast messages, can also encrypt and authenticate messages as if they originate from the 'real' BS. Another aspect which is much more problematic is the distribution of the traffic encryption keys (GTEKs) when the optional Multicast and Broadcast Re-keying Algorithm (MBRA) is used. To transfer a GTEK to all group members it is broadcasted but encrypted with the key encryption key (GKEK). Due to broadcasting, the GKEK must also be a shared key and every group member knows it. Thus an adversary group member can use it to generate valid encrypted and authenticated GTEK key update command messages and distribute an own GTEK. In a unicast connection this different keying material at the mobile station would be detected as the base station cannot decrypt data sent by the mobile station. This result in a TEK invalid message destined to the MS which subsequently refreshes its keying material. Since the MBS is only unidirectional, the BS cannot detect that MS has different GTEKs.

SOLUTIONS PROFFERED TO THE VULNERABILITIES

In this section, some solutions to improving and strengthening Mobile WiMAX (IEEE 802.16e) security as proposed by authors Taeshik Shon et.al [8], Chin-Tser Huang et.al [9]:-

Unauthenticated messages

Non-authenticated management messages sent on the primary or basic management connection can easily be authenticated using a HMAC or CMAC digit. It has to be decided if this authentication, which additionally needs up to 168 bits is acceptable. Most messages are very

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

short so that an appended digit would boost the message to a multiple of its original size. Due to this fact, a tradeoff between the security and the effectiveness of the protocol has to be found. One way for such a tradeoff is to authenticate all messages which can have serious effects if they are forged. In addition to the management messages which are already protected by an authentication digit .Other management messages can remain unauthenticated. To hold down the overall message size, the CMAC or the Short HMAC should be used, as it has much lower size as the full HMAC. HMAC is based on the SHA-1 algorithm so a MAC size of 128 bit is achieved. For the Short HMAC this value is truncated to 64 bit. With all other needed parameters (i.e., packet number, key sequence number and reserved fields) this results in a Short HMAC digest of 104 bit. CMAC uses AES128 which also results in a 128 bit value. For the finally used CMAC this value is truncated to 64 bit. With all additional information the complete CMAC digest is also 104 bit in total. Broadcasted messages have a problem when their authentication is not completely secure if a symmetric key is used, since this key must be shared by all group members. This offers the possibility that messages can be forged by every group member. However, a symmetric solution can be very fast and protects against message forgery from outside a group. It is possible to significantly increase the security without complete protection but with low requirements. Another possibility would be the use of asymmetric cryptography. Broadcasted messages in this case are authenticated by a signature created with the private key of the base station. For mobile stations this requires to verify this asymmetric signature with the known public key when they receive such broadcasted management messages. However, this solution has a big drawback, that is, it needs much time to be performed and the asymmetric keys must be managed. Additionally, authentication takes place very often and thus increases the requirements. This is iterated n times.

GTEK0 = random ()

GTEK1 = f (GTEK0)

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

GTEK2 = f (GTEK1)

GTEKn = f (GTEKn-1)

This hash chain allows for the verification of each GTEK by applying the same one way function to the previous one. To achieve this chained authentication, the last GTEK has to be distributed to each MS in a secure way as it is the only key in the chain which can not be authenticated by another one. One possibility is to distribute GTEKn in the GKEK update command message which is a unicast message and encrypted by a MS related key. If a MS receives a new GTEK via a broadcasted GTEK update command message it can verify its integrity by applying the one way hash function f to it. If the authentication is positive, the current GTEK can be overwritten and the received one is established.

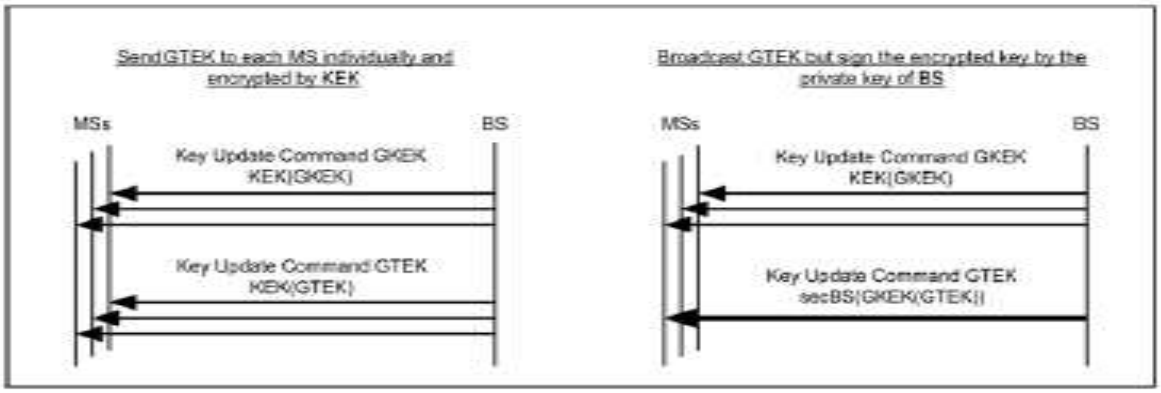

Figure 4: Possible solutions to transmit GTEK in a secure way [5]

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

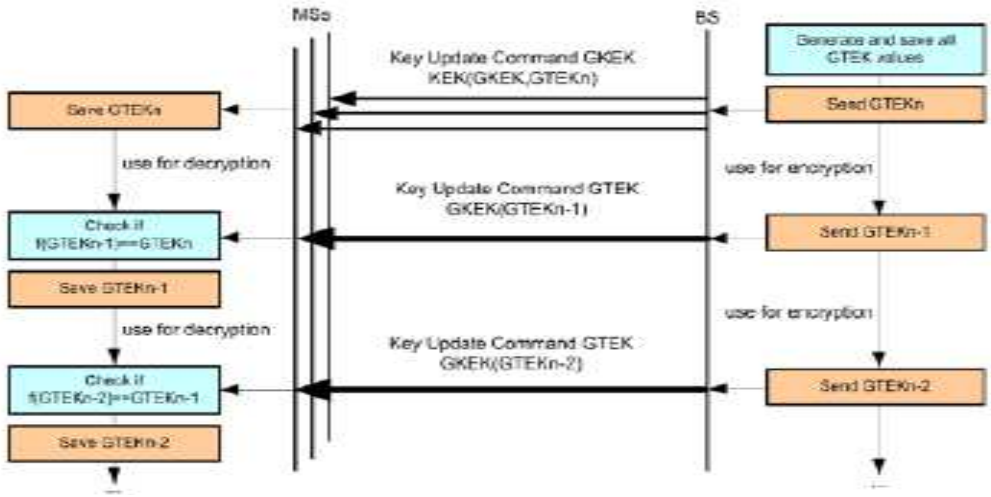

Figure 5: Avoiding key forgery by a GTEK hash chain [5]

If the authentication fails, the MS discards the message and requests a new GTEK via the unicast Request/Reply mechanism, the behavior of which is exhibited in Figure 5. To apply this algorithm, the key GKEK update command message has to be capable of transporting GKEK and GTEK keys together. The design of the key update command message already includes both keys so only a little modification is necessary here. Additionally the GTEK state machine at BS must generate the GTEK hash chain and store all the keys. The GTEK state machine at MS must add the functionality to authenticate GTEK keys by calculating the hash function and comparing it to the previous key. A drawback of this algorithm is that it has a reduced forward secrecy. This means a MS, joining the group, can decrypt all broadcasted data since the last hash chain generation. If forward secrecy is crucial, the hash chain has to be regenerated each time a MS enters the group.

CONCLUSION

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

An analysis of the threats to the security of the Mobile WiMax/ 802.16e broadband wireless access networks has been conducted. Critical threats are eavesdropping of management messages, BS or MS masquerading, management message modification and DoS attack. Major threats are jamming and data traffic modification (when AES is not applied). Countermeasures need to be devised for networks using the security options with critical or major risks. An intrusion detection system approach can be used to address some of the threats.

REFERENCES

[1] IEEE Stds. 802.16e-2005 and 802.16-2004/Cor 1-2005, “Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands” and Corrigendum 1, 2004.

[2] Carl Eklund, Nokia Research Center Roger B. Marks, National Institute of Standards and Technology Kenneth L. Stanwood and Stanley Wang, Ensemble Communications Inc. IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access June 2002

[3] Fan Wang, Amitava Ghosh, Chandy Sankaran, Philip J. Fleming, Frank Hsieh, and Stanley J. Benes, Networks Advanced Technologies, Motorola Inc. Mobile WiMAX Systems: Performance and Evolution, Nov, 2008, pp.-1-3

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

[5] Frank, A Ibikunle,Security Issues in Mobile WiMAX (IEEE 802.16e), 2009 IEEE Mobile WiMAX Symposium

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 3 NOVEMBER 2011

[6] Krawczyk H., Ballare M., Canetti R. “HMAC: Key- Hashing for Message Authentication”, RFC 2104, http://www.ietf.org/rfc/rfc2104.txt, IETF, 1997.

[7] Dworkin M.: Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, NIST special publication 800-38B, National Institute of Standards and Technology (NIST), MD, USA, 2005.

[8] Taeshik Shon, Wook Choi: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, First International Conference, NBiS 2007, LNCS, Vol. 4650, pp. 88-97, 2007.

[9] Chin-Tser Huang, J. Morris Chang, Responding to Security Issues in WiMAX Networks2008

[10] Michel Barbeau, WiMax/802.16 Threat Analysis, *Q2SWinet’05,* Montreal, Quebec, Canada, October 13, 2005,