Security analysis of the WiMAX technology in Wireless Mesh networks

Md. Rezaul Karim Siddiqui & Sayed Mohammad Atiquur Rahman

This thesis is presented as part of Degree of Master of Science in Electrical Engineering with emphasis of Telecommunication

Blekinge Institute of Technology (BTH), Karlskrona, Sweden
November 2009

Blekinge Institute of Technology
School of Computing
Department of Telecommunication
Supervisor: Dr. Lennart Isaksson
Examiner: Anders Nelsson
Acknowledgement

The thesis is carried out in the Department of Masters of Electrical Engineering with emphasis of Telecommunication, Blekinge Institute of Technology (BTH), Karlskrona, Sweden. Our research is consists of exploring security faults and their solutions in WiMAX mesh network. Current violence in wireless communication has emphasizes us to think about the security issues. We tried to explore different security holes, threats and vulnerabilities and possible solutions. Our friends had given us a helping hand to do this paper. Of course, we would like to take the opportunity to express thanks to the people who guided and supported us during our thesis work.

We wish to express exceptionally grateful to our Supervisor Dr. Lennart Isaksson for showing great interest in our work and for the guidance to make a quality thesis. We thank our parents for skillfully guiding us into a academia. We will enjoy thanking Mr. Gunnar Råhlén who was responsible to handle our thesis proposal and obviously we have to express our thanks to our examiner Mr. Anders Nelsson who took a very deep concern regarding the thesis and always communicated with our supervisor.

MD.Rezaul Karim Siddiqui  &  Sayed Mohammad Atiquur Rahman

Karlskrona, November 2009
Abstract

The IEEE 802.16 (WiMAX) is the promising technique to overcome some disadvantages on the Security concern of the widespread IEEE 802.11 standard. For providing high speed wide area broadband wireless access, WiMAX is an emerging wireless technology for creating multi-hop Mesh network. Based on the wired backbone wireless Mesh networks serve to get over present dependencies of wireless system. Wireless operates on Physical layer and MAC layer in the air interface to provide fixed and Mobile Broadband Wireless Access (BWA) in broad range of frequencies. Due to the lack of Physical infrastructure of wireless networks are inherently less secure. In order to protect data exchange between the MAC layer and PHY layer WiMAX specifies a security sub-layer at the bottom of the MAC layer. The security sub-layer provides privacy with SS and BS from service hijacking. For providing authentication, data traffic privacy services and key management a PKM protocol defined by the WiMAX MAC as a sub-layer where the PKM protocol is the main protocol work in the security sub-layer. WiMAX is only a “Paper based” newly established technology based on Wi-Fi system then it is tough to find out its security holes in all the way. Keeping all the fact in mind the objectives of the thesis are to analyze the WiMAX security architecture security keys (AK, KEK and HMAC) are used for authorization, authentication and key management and TEK is for secure data transmission, possible security vulnerabilities, threats and risks are classified according to different layer with 802.16 std Mesh network. In addition, vulnerabilities comparison between IEEE 802.11 and 802.16 std has been pointed out in details, as well as security improvements and possible solutions has been proposed to protect WiMAX attacks.

Keywords: IEEE 802.16, WiMAX, Mesh mode, mesh network, Vulnerability, security threats
# Table of Contents

Chapter 1: Introduction .......................................................................................................................... 1  
1.1 WiMAX Technology Background: ................................................................................................. 1  
1.2 Related Works: ............................................................................................................................... 2  
1.3 Thesis Organization: ....................................................................................................................... 2  

Chapter 2: IEEE 802.16 Evolution and Architecture ........................................................................... 3  
2.1 Evolution of IEEE family of standard ............................................................................................. 3  
2.1.1 IEEE 802.16-2001 ....................................................................................................................... 3  
2.1.2 IEEE Std 802.16c-2002 .............................................................................................................. 3  
2.1.3 IEEE 8020.16a-2003 .................................................................................................................. 3  
2.1.4 IEEE 802.16-2004 ..................................................................................................................... 4  
2.1.5 IEEE 802.16e-2005 .................................................................................................................... 5  
2.2 WiMax Operation Modes: .............................................................................................................. 5  

Chapter 3: IEEE 802.16 Security Architecture: .................................................................................. 9  
3.1 Protocol Layers within IEEE 802.16 .............................................................................................. 9  
3.1.1 The Medium Access Control (MAC) Layer .............................................................................. 10  
3.1.2 Physical Layer .......................................................................................................................... 14  
3.2 Cryptography: ............................................................................................................................... 15  
3.2.1 TEK Encryption ......................................................................................................................... 15  
3.2.2 Data Encryption Method .......................................................................................................... 17  

Chapter 4: Privacy Key Management (PKM) for Mesh Mode protocol: .............................................. 18  
4.1 Authorization scheme used in PKMv1 and PKMv2 protocol ........................................................ 18  
4.2 Authentication Protocol in 802.16: ............................................................................................... 20  
4.3 Security Roaming of Key Association during handover: .............................................................. 21  
4.4 Authorization and AK Exchange: ................................................................................................. 22  
4.5 Traffic Encryption Key (TEK) Exchange: ...................................................................................... 25  
4.6 Secure Keys for WiMax Communication: ...................................................................................... 28  
4.6.1 Authentication Keys (AKs): ...................................................................................................... 28  
4.6.2 Key Encryption Keys (KEKs): ................................................................................................... 28  
4.6.3 Traffic Encryption Keys (TEKs): ............................................................................................... 28  
4.6.4 Hashed Message Authentication Code (HMAC): ................................................................... 29
Chapter Five: WiMAX Security Analysis

5.1 Vulnerabilities comparison between IEEE 802.11 and IEEE 802.16

5.1.1 Identity vulnerabilities:

5.1.2 Potential vulnerabilities to meet in 802.16 standards:

5.1.3 Attacks on 802.16:

5.2 Security Threats specially meets of IEEE 802.16 in Mesh Mode

5.2.1 Topological Attack

5.2.2 Threats to link Establishment

5.2.3 Threats to TEKs

5.2.4 Traffic Threats

Chapter Six: Conclusion and Possible Enhancements:

6.1 Protection against the WiMAX attacks:

6.1.1 Mutual Authentication:

6.1.2 Spreading technique for jamming:

6.1.3 Data Protection Error:

6.1.4 Authorization Node Spoofing:

6.2 Security Improvements:

6.2.1 Certificate Chain:

6.2.2 RSA based authentication:

6.2.3 Cryptographic issues:

6.2.4: Random number & Signature system:

6.3 Future work
Lists of Tables:

Table 1: Comparison of IEEE standard ................................................................. 4
Table 2: Message attributes in the AK management [15] ........................................ 25
Table 3: Message attributes in the TEK management [15] ........................................ 28

Lists of Figures:

Figure 1: PMP mode .................................................................................................. 5
Figure 2: Mesh mode ................................................................................................. 6
Figure 3: IEEE 802.16a standards point to multipoint mode (a) and mesh mode (b) [12] 7
Figure 4: WiMAX Standard protocol Structure ........................................................ 9
Figure 5: MAC PDU Field description [9] .................................................................. 11
Figure 6: Node Initialisation Overview ..................................................................... 12
Figure 7: IEEE 802.16 Security Associations [11] .................................................... 14
Figure 8: Protocol Layering in IEEE 802.16 ............................................................ 14
Figure 9: TDEA work structure ............................................................................... 15
Figure 10: TEK Encryption with RSA ....................................................................... 16
Figure 11: AES TEK encryption (128 bit) ................................................................. 17
Figure 12: Authorization scheme used in PKMv1 protocol ....................................... 18
Figure 13: Authorization scheme used in PKMv2 protocol ....................................... 19
Figure 14: Authentication Protocol in 802.16 ........................................................... 22
Figure 15: Modified Authentication Protocol ........................................................... 21
Figure 16: Authentication Protocol with nonce in [14] ............................................ 21
Figure 17: Security Roaming of Key Association ..................................................... 22
Figure 18: AK management [15] ............................................................................. 23
Figure 19: TEK management [16] .......................................................................... 26
Figure 20: HMAC Creation ....................................................................................... 29
Figure 21: Graphical representation of deauthentication attack, attackers need generate one packet for each six exchange. [24] .............................. 31
Figure 22: Using RES-CMD failure De-authentication attack [22] ............................ 32
Figure 23: Representations of virtual carrier sense attack. [24] ................................. 35
Figure 24: Security model [25] ............................................................................... 36
Figure 25: Use of AUX port to circumvent [24] ....................................................... 37
Figure 26: Inject message on TDD frame. [22] .......................................................... 38
Figure 27: Attack process RSP-RNG [22] ................................................................. 40
Figure 28: Focused on invalid message at authorization state machine. [22] .............. 41
Figure 29: Wormhole attack. As an attacker tunnel message through hidden channel, node A believe node B as neighbour. [30] ................................................. 42
Figure 30: Sinkhole Attack ....................................................................................... 43
Figure 31: Node authorization procedure .................................................................. 44
Figure 32: Disclose OSS with Reply Attack .............................................................. 45
Figure 33: Link Establishment process ..................................................................... 45
Chapter 1: Introduction

1.1 WiMAX Technology Background:

In order to avoid the limitations of traditional wired networks, there have been many efforts to develop wireless technologies. Wireless technology has been developed from 19th century and lots of development done on this prospect. Wireless networks are based on the IEEE 802.11 standard. IEEE 802.11 standard were first created in the 2.4 GHz band using protocols defined by the IEEE 802.11b standard. Two other well-known standards in IEEE 802.11 standard family are IEEE 802.11a and IEEE 802.11g. Though they provide high speed WLAN standard, the coverage area is limited. The IEEE 802.11 standard, commercially known as WiFi, requires a large number of WiFi access points and to connect with the other nodes it needs wired connection. Due to this reason Institute of Electrical and Electronics Engineers (IEEE) innovating a new standard to provide a large wireless networks. IEEE 802.16 is a standard providing broadband access alternative of cable connection. WiMAX is the trade name IEEE 802.16 standard. With the support of Mesh networking, WiMax systems can be easily configured as a wireless metropolitan area networks (WMAN). It has further enhanced the ability of WMANs with mobility support. Researchers have started to revisit the protocol design for existing wireless network likely IEEE802.11, adhoc and IEEE 802.16. This all actively working on new application for WMANs. In 2004, 802.16 provide extended support for NLOS in 2 – 11 GHz spectrum with Mesh network connections.

Mesh mode enables each node in a network to connect with others directly. Traffic can occur not only between the base stations but also among subscriber stations. So, Mesh network provides alternative routing paths. If an intermediate node is down or there is an obstacle, the message can be routed through another node and it is necessary to analyze the security of IEEE 802.16 in Mesh networks. [1]

With the deployment of wireless communication in recent years, security issues in wireless networks also become a growing concern. Privacy or confidentiality is fundamental for secure communication, which provides resistance to interception and eavesdropping. Message authentication provides integrity of the message and sender authentication, corresponding to the security attacks of message modification and impersonation. Message replay attack is one of the most common attacks on authentication and authenticated key establishment protocols. If the messages exchanged in an authentication protocol do not carry appropriate freshness identifiers, then an adversary can easily get himself authenticated by replaying messages copied from a legitimate authentication session. Man-in-the-middle attack is another classic attack and is generally applicable in a communication protocol where mutual authentication is absent. Other familiar attacks include parallel session attack, reflection attack, interleaving attack, attack due to type flaw, attack due to name omission, and attack due to misuse of cryptographic services. [2]. In order to prevent forgery or replay attack mutual authentication is always required for any wireless medium. [3]
This paper presents an analysis of the security threats to WiMax security that reflects to most recent work of the IEEE and WiMax Forum and performed based on the following questions -

- What are the Vulnerabilities and Security threats of the WiMAX Technology in Mesh networks?
- What are the security threats at the Physical Layer then at the MAC layer?
- What are the possible solutions can be achieved from WiMAX Mesh networks?
- How can the solution improve the security?

1.2 Related Works:

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. As with many newer technologies (and some mature ones), the security features available may not be as comprehensive or robust as necessary. The earlier version of Wireless network was not strength on security issue. Vulnerabilities

Bluetooth's challenge-response is simplistic. It suffers various types of lacking such as authentication, auditing, and non repudiation. [4] A one-way challenge for authentication is susceptible to man-in-the-middle attacks.

WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security. To rectify the security issues with WEP, the Wi-Fi Alliances a new cryptographic protocol named Wi-Fi Protected Access (WPA). Leak of WEP keys leads to eavesdropping, message modification, and masquerading. Session hijacking may occur during handover process. [4]

IEEE 802.16 standard is new and still needs to be examined before deploying. Additionally, Mesh networks are gaining more interest and IEEE 802.16 is seen as one of promising techniques to build up mesh networks, we believe that it is necessary to analyze the security of IEEE 802.16 in mesh networks.

1.3 Thesis Organization:

The first chapter is an introduction of the thesis work. The rest of the chapters are organized as follows:

Chapter Two: A brief description of the WiMAX technology, the versions of the IEEE 802.16 standard and the Characteristics of Mesh Network are described in this chapter.

Chapter Three: This chapter is an overview of the Security architecture of the IEEE 802.16 standard in Mesh network to identify vulnerabilities.

Chapter Four: A security comparison between IEEE 802.11 and IEEE 802.16 and explanation of the vulnerabilities analysis is conducted in this chapter.
Chapter Five: An improved scheme focused on Privacy key management proposal is proposed to strengthen the security.

Chapter Six: In this chapter possible solution are proposed to improve security for the IEEE 802.16 in Mesh networks.

Chapter 2: IEEE 802.16 Evolution and Architecture

This chapter represents the evolution of the IEEE 802.16 standard and PMP and Mesh mode operations. At the end of this chapter provides the whole operation between the BSs and SSs when the network is deployed on both operational modes.

2.1 Evolution of IEEE family of standard

The IEEE 802.16 standard contains the specification of Physical (PHY) and Medium Access Control (MAC) layer. The first version of the standard IEEE802.16-2001 was approved on December 2001 and it has gone through many amendments to accommodate new features and functionalities and published in April 2002. The current version of the standard IEEE 802.16-2004 [6], approved on September 2004, modified all the previous versions of the standards. To understand the development of the standard, the evolution of the standard is presented below.

2.1.1 IEEE 802.16-2001

The IEEE 802.16-2001 is the first version of the IEEE Std 802.16 standard. It was approved in December 2001 and published in April 2002. The IEEE Std 802.16-2001 [5] defines the MAC and PHY for fixed, broadband wireless in a Point to Point (PTP) or Point to Multipoint (PMP) connection. In term of duplexing technique this standard supports both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD). QPSK, 16QAM and 64 QAM modulation schemes are used here. It uses single carrier modulation from 10 Ghz to 66 Ghz and for the duplexing of uplink and downlink channel. To reduce multipath distortion, the standard can work only in LOS environments because of its high frequencies.

2.1.2 IEEE Std 802.16c-2002

The IEEE 802.16c-2002 is the amendment to the IEEE Std 802.16-2001. The amendment specifies the detailed system profiles for operating in 10-66 GHz band. It standardizes more details in the wireless technology and also corrected some errors and inconsistencies of the first version.

2.1.3 IEEE 8020.16a-2003

The IEEE Std 802.16a-2003 is the second amendment for the IEEE Std 802.16-2001. It supports operating at the 2-11 GHz frequencies. The standard improves PMP MAC and defines new PHY specifications. Due to inclusion of below 11 GHz range, Non Line of
Sight (NLOS) operation becomes possible. Due to NLOS operation multipath propagation becomes an issue. To deal with multipath propagation and interference mitigation features like advanced power management technique and adaptive antenna arrays were included in the specification [7]. In addition to the single carrier modulation, QPSK, 16QAM, 64 QAM, Orthogonal Frequency Division Multiplexing (OFDM) is an option in this standard. Also in the range 2-11 GHz Orthogonal Frequency Division Multiple Access (OFDMA) is added.

### 2.1.4 IEEE 802.16-2004

The IEEE Std 802.16-2004 was created combined with IEEE 802.16-2001, 802.16a-2003 and 802.16c-2002. At first, it was published as a revision of the standard named 802.16REVd, but the changes were so genuine that the standard was reissued named 802.16-2004. In this version, the whole family of the standard is ratified and approved. This standard is designed for both licensed and license-exempt frequencies. It provides the ability to support NLOS environment. The MAC supports both PMP and Mesh modes.

<table>
<thead>
<tr>
<th>Spectrum</th>
<th>802.16-2001</th>
<th>802.16c-2002</th>
<th>802.16a-2003</th>
<th>802.16-2004 802.16 Rev D</th>
<th>802.16e-2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Popagation/channel</td>
<td>LOS</td>
<td>LOS</td>
<td>NLOS</td>
<td>NLOS</td>
<td>NLOS</td>
</tr>
<tr>
<td>Conditions</td>
<td>10-66 GHz</td>
<td>10-66 GHz</td>
<td>2-11 GHz</td>
<td>2-11 GHz</td>
<td>2-6 GHz</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>32-134 Mbps (28Mhz channelization)</td>
<td>Up to 75 Mbps (20Mhz channelization)</td>
<td>Up to 75 Mbps (20Mhz channelization)</td>
<td>Up to 15 Mbps (5Mhz channelization)</td>
<td></td>
</tr>
<tr>
<td>Modulation</td>
<td>QPSK, 16QAM and 64 QAM</td>
<td>QPSK 16QAM</td>
<td>OFDM 256 subcarriers QPSK, 16QAM, 64 QAM</td>
<td>OFDM 256 sub-carriers QPSK, 16QAM, 64 QAM</td>
<td>Scalable OFDMA</td>
</tr>
<tr>
<td>Mobility</td>
<td>Fixed</td>
<td>Fixed</td>
<td>Fixed</td>
<td>Fixed/ Nomadic</td>
<td>Portable/mobile</td>
</tr>
<tr>
<td>Typical Cell</td>
<td>1-3 miles</td>
<td>1-3 miles</td>
<td>4 to 6 miles</td>
<td>4 to 6 miles</td>
<td>1-3 miles</td>
</tr>
<tr>
<td>Radius</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Comparison of IEEE standard
### 2.1.5 IEEE 802.16e-2005

The IEEE Std 802.16e-2005 is an amendment of the IEEE Std 802.16-2004 in December 2005. This includes the PHY and MAC layer enhancement to enable combined fixed and mobile operation in licensed band. In addition, the standard for mobile subscribers moving at vehicular speeds. It provides handover function between BSs. Although fixed SSs can operate with the IEEE Std 802.16e-2005 BSs, mobile functionalities are added into the amendment.

### 2.2 WiMax Operation Modes:

**PMP Mode:**

FDD scheme and TDD scheme is used in this operational mode. The signal traffic occurred only between the BS and SS. The signal direction from BS to SS is called downlink and the opposite like direction called uplink. In the FDD scheme, both the uplink and downlink signal transmission occurred simultaneously and in the TDD scheme, transmission time divided into uplink and downlink periods.

![Figure 1: PMP mode](image1.png)

The downlink is usually broadcast the signal. The SSs which have connections to an antenna sector with a given frequency channel receive the same signal transmission. The uplink bandwidth to the BS is shared by the SSs. The IEEE Std 802.16 defines the bandwidth allocation and request mechanisms depending on the class of service utilized. [6]
Mesh Mode:

The IEEE Std 802.16a-2003 introduced to allow the WiMAX nodes to establish mesh networks. [6] Defines “Mesh” as “network architecture, wherein systems are capable of forwarding traffic from and to multiple other systems”. If every node in a network directly connects to every other node, it is called a “fully meshed network”. Otherwise, it is a “partial meshed network”. In partial Mesh Network, every node is not connected to each other. On the other hand, in full mesh network, every nodes are connected each other so that if a node is disconnected anyway or unable to forward signal to another node then it can chose alternative node.

PMP and Mesh Operation

In case of mesh network measure unit is node where each node is directly or by neighbouring connected to each other. It can expand one neighbour to extend neighbour depends on distance one more hope away
Figure 3: IEEE 802.16a standards point to multipoint mode (a) and mesh mode (b) [12]

According to fig where we see a single upward node which is called BS and others nodes called SSs. It starts automatically initialization and entry procedure when a node became a member of a mesh.

In case of transmission missing the node follows different steps is followed to recover it. We make a short description this procedure as follows:

- By using MSH-NCFG the node search active network. This step is performed by Physical layer.
- The node tries to obtain operator and neighbour list.
- Select a sponsor node from neighbour and it request to make a temporary relation during initialization time. When this relation established candidate sponsor node be act as a sponsor node.
- Completing previous stage both new and other node sending an acknowledgement which ensures supporting basic capabilities. e.g. physical parameter and bandwidth.
- To ensure authorization, authorization node exchange AK with new node.
- When new node allows entering network then it assign node ID and through this way it complete registration.
- Through DHCP (Dynamic host configuration protocol) new node can able to get IP address.
• Through time server new node synchronized time & date and acknowledgement (req-res) is over sponsor channel.

• Download configuration file which contain operational parameter.

• Setup provisioned parameter where quality of service provisioned packet by packet and it obtained by new node.

• Finally new node makes connections to another node while it becomes neighbour.
Chapter 3: IEEE 802.16 Security Architecture:

The protocol layers of the standard provide an idea of interaction between different protocol stack. Finally, this chapter ends up with a brief discussion of the IEEE 802.16 based network architecture, deployment topology and applications.

3.1 Protocol Layers within IEEE 802.16

The IEEE 802.16 std includes of a protocol stack with various types of interfaces. In IEEE 802.16 std, MAC layer is designed for PMP broadband wireless access application [6]. The MAC layer consists of three sublayers.

- Service specific Convergence Sublayer (MAC CS).
- MAC Common Part Sublayer (CPS).
- Privacy Sublayer.

![WiMAX Standard protocol Structure](image)

Service Specific Convergence Sublayer transform data between higher level layers and CS layer and MAC CS provides two types of sub-layers, ATM convergence sublayer which is for ATM networks services and packet convergence sublayer for packet data services which support Ethernet, PPP, IP (IPv4 and IPv6) and VLAN (Virtual Local Area Network). [8].

MAC CPS is the core part of MAC layer. It defines rules and mechanisms for System access bandwidth allocation, connection control and Automatic Repeat Request
(ARQ). It also provides duplexing, centralization and channel access. CS and CAP are communicated by MAC SAP (Service Access Point). [8]

The privacy Sublayer is the sublayer between MAC CPS and PHY layer. It provides encryption and decryption of data that is entering and leaving the PHY layer. It also used for 56 bit DES encryption for traffic and 3 DES for Key Exchanges. [8]

The PHY layer make the standard adaptable to different frequency ranges including multiple specifications. The flexibility of the PHY layer that enables the system designers to tailor their system according to the requirements. Including some optional features the PHY layer specifies some mandatory features for implementing with the system.

3.1.1 The Medium Access Control (MAC) Layer

MAC layer Overview

The WiMAX MAC protocol is connection oriented and designed for Point-to-Multipoint (PMP) broadband wireless access applications. [6] The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the physical layer. Base Station (BS) is usually wired, and it broadcasts to the Subscribers Station’s (SS’s) where BS can be seen as the Access Points (AP’s) in IEEE 802.11 std, although the two standards are completely different in the way that they use the airwaves. MAC is built to support this point to multipoint (P2M) technology.

Very high data bits are needed for both UL (SS to the BS) and DL (from the BS to the SS). The medium access algorithm and bandwidth allocation algorithm accommodate multiple terminals per channel and terminals may be shared by multiple end users. The MAC design includes a convergence sublayer that can interface with a variety of higher-layer protocols, such as Asynchronous Transfer Mode (ATM), Time Division Multiplexing (TDM) Voice, Ethernet, IP, and any unknown future protocol. [6] The users require the services according to their nature and include legacy time-division multiplex (TDM) voice and data, IP connectivity, and packetized VoIP. The WiMAX MAC must accommodate both continuous and burst traffic in order to support various services.

MAC messages format

MAC Protocol Data Units (PDUs) message exchange between BS MAC and SS MAC. The message consists of three parts: A fixed length MAC header, a variable-length Payload (frame body) and a Frame Check Sequence (FCS). The MAC header contains frame control information, FCS holds IEEE 32-bit Cyclic Redundancy Checking (CRC). [9]
MAC header types are: MAC Service Data Unit (MSPU), where payloads are MAC SDUs/segments, i.e., data from the upper layer (CS PDUs). Second one is, Generic MAX header (GMH) where the payloads are MAC Management messages or IP packets encapsulated in MAC CS PDUs. Both are transmitted on management connections. [9] The third one is Bandwidth Request Header (BRH) which is sent out without payload. [9]

Except the Bandwidth Request PDUs (that have no payload) MAC PDUs may hold either MAC management messages or convergence sublayer data- MAC Service Data Unit (MSDU). Header type (HT bit) is always set to 0 (Zero) for both GMH and MSDU when Bandwidth Request Header is set to 1 (One). The MAC header contains a flag, which the payload of the PDU is encrypted or not. [10]

<table>
<thead>
<tr>
<th>MAC PDU</th>
<th>Msb</th>
<th>Payload</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMH (6 bytes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BW Req. Header Format (Header Type (HT) =1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H T E C Type (6 bits) rs v C I EKS (2) rs v LEN Msb(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEN lsb (8) CID msb (8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CID lsb (8) HCS (8)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: MAC PDU Field description [9]

MAC header and all MAC management messages are not encrypted. This decision was made to “facilitate registration, ranging and normal operation of the MAC sublayer”. But, as a result this leads to vulnerabilities. On the other hand, if it was encrypted, spoofing was difficult to occur during BS and SS had exchanged encryption keys.
Establishing connection in Mesh Mode

During the entrance or in case of signal lost of a node in a Mesh network the node will follow the initialization and network entry procedures. The node initialization overview of the procedures is shown in Figure 3. The shaded process (Node Authorization) in Figure 3 implies that the process is related to the security sublayer.

![Node Initialization Overview Diagram]

Figure 6: Node Initialisation Overview

1. **Scan for active network**: In Mesh network, every node broadcast MSH-NCFG message to enter in a network on a regular basis. The messages contain PHY layer information for the new node to acquire coarse synchronization. In addition, MSH-NCFG message provides a list of available BSs and a list (Node ID) of neighboring nodes of the sender. The new node selects a sponsor node to join the network.

2. **Obtain network parameters**: The new node obtain network parameters, i.e. operator identifier, and builds a physical neighbor list.

3. **Open Sponsor Channel**: When a new node wants to join in to a network then the new node selects one of its neighbors as the candidate Sponsor Node. It requests the candidate Sponsor Node to establish Sponsor Channel which is a temporary schedule for message delivery during initialization. Finally, the candidate Sponsor Node becomes the Sponsor Node when the request is accepted by the candidate Sponsor Node and the new node receives the acknowledgement message.
4. **Negotiate basic capabilities:** The new node starts sending its basic capabilities after establishing a logical link. The other node sends a reply with the basic capabilities. The Physical Parameters Support and Bandwidth Allocation Support are the parameters in the basic capabilities.

5. **Node authorization:** A candidate node needs authorization to access the Mesh network. This can be achieved through a handshake between the candidate node and an Authorization node. The sponsor node tunnels the message from the candidate node to the Authorization node. The Authorization center verifies the information of the candidate information with the request. If it fails then Authorization center sent Auth Reject. On the other hand, if the candidate is authentic.

6. **Perform registration:** If the new node is accepted for the registration to enter the network from the Registration Node via the tunnel provided by the Sponsor Node then the new node is assigned a Node ID.

7. **Establish IP connectivity:** By using Dynamic Host Configuration Protocol (DHCP) over the Sponsor Channel the new node obtains IP address.

8. **Establish time of day:** The request and response messages of the new node are transmitted over the Sponsor Channel and it also synchronizes the current date and time from the time server.

9. **Transfer operational parameters:** The new node download a configuration file from the Trivial File Transfer Protocol (TFTP) server. The configuration file contains required operational parameters.

10. **Setup provisioned traffic parameters:** The new node obtains the QoS parameters during transferring operational parameters in the previous process.

11. **Establishing link to neighbors:** The new node can become its neighbors to connect with the other nodes.

**Privacy sublayer**

The whole security of IEEE 802.16 std depends on Privacy Sublayer which provides access control and confidentiality of the data link. Encapsulation protocol and Privacy Key Management Protocol (PKM) are the main protocol work in this security sublayer where The Encapsulation protocol encrypt packet data and PKM provides secure distribution of keying data from BS to SS. Security Associations (SA) is identified by SAID which contains cryptographic suite such as encryption algorithm and security info like key, IV. Both the basic and primary management connections do not have SAs while the secondary management connection can have an optional SA. Transport connections always have SAs.
3.1.2 Physical Layer

The PHY layer is only used in the line-of-sight (LOS) operation. However, it was originally designed for 10-66 GHz range. Later, 2-11 GHz physical layer is driven by the need for non-line-of-sight (NLOS) operation. Various techniques were applied in order to get maximum throughput within a long distance, such as Orthogonal Frequency Division Multiplexing (OFDM), Time Division Duplex (TDD), Frequency Division Duplex (FDD), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM).

In short, OFDM delivers a wireless signal much farther with less interference than competing technologies. In the IEEE 802.16, modulation technique in the downlink and uplink are QPSK, 16-QAM, BPSK and 16-QAM. In IEEE 802.16-2004 std, the OFDM signal is divided into 256 carriers and IEEE 802.16e will use scalable OFDMA.
In TDD, both uplink and downlink transmission share same frequency but are separated on time. TDD splits the bandwidth into time slots which shared by uplink, and downlink but do not transmit simultaneously. On the other hand, FDD separates the uplink and downlink into two individual channels which support simultaneous operation. In FDD, within difference frequencies uplink and downlink communication take place at the same time.

### 3.2 Cryptography:

#### 3.2.1 TEK Encryption

There are four types of technology use for encrypting. We make a short brief each of them.

- **TDEA (Triple Data Encryption Standard):** KEK is divided two parts where each part containing 64 by left and right side. Its algorithm identifier is 0x01.

![TDEA work structure](image)

Figure 9: TDEA work structure
TDES operation can be done 64 bit KEK encryption Decryption and Encryption way. In codebook mode each key contain (ECB) 56 bit. [FIPS PUB 46-3, 1999, NIST special publication 800-38A, 2001, Schneier, 1996].

- **RSA:** By Using RSA TEK is encrypting where use node’s public key and for Decryption use node’s private key. RSA use block cipher and its most widely implemented. Its algorithm identifier is 0x02.

![Diagram](image_url)

**Figure 10: TEK Encryption with RSA**

- **AES (Advance Encryption Standard):** Use 128 bit TEK with 128 bit AES in ECB. Its algorithm identifier is 0x03.
We just show the snapshot of how this algorithm work, elaboration we escape beyond the paper.

### 3.2.2 Data Encryption Method

**Data Encryption in CBC:** DES algorithm is defined on [FIPS PUB 46-3, 1999 FIPS PUB 74, 1981, FIPS PUB 81, 1980]. Residual block processing is used when MAC PDU last block is less than 64 bit.

**AES using CCM:** AES use two method for encryption CTR (Counter mode) and CBC (Message authentication CBC-MAC) [NIST special publication 800-38C, 2004, FIPS PUB 197]. This algorithm facilitates Authentication and encryption.

**AES using CBC and CTR:** Residual block process is used CBC algorithm when block size less than 128 bit while CTR use 8 bit roll over counter. [NIST special publication 800-38A, 2001, FIPS PUB 197, 2001, RFC 3686, 2004]
Chapter 4: Privacy Key Management (PKM) for Mesh Mode protocol:

Both PMP and Mesh modes supports in 802.16-2004 std. but PKM1 version supports only Mesh. So, Limitations of PKMv1 and PKMv2 protocol, Authorization, TEK, AK exchange and internal security keys for WiMax communication are described in this chapter.

4.1 Authorization scheme used in PKMv1 and PKMv2 protocol

PKM protocol is for providing the secure distribution of keying data from BS to SS as well as enabling BS to enforce conditional access to network services. The PKM protocol supports the authorization of the SS, periodic authorization, reception/renewal of key materials. At a client/server model the PKM protocol uses X.509 digital certificates, RSA public-key algorithm, and strong encryption algorithm to perform key exchanges between SS and BS.

The IEEE 802.16e standard has two versions of PKM, the PKMv1 and PKMv2. As the PKMv1 had some limitations it was modified and transformed to PKMv2. PKMv1 did not provide mobility due to certain limitations. The authorization protocol used in PKM is basically 3 way handshake protocol between the SS and BS. The authentication in PKMv1 is just from the SS but not from the BS. It means that only SS will authenticate itself to BS. Message1 is sent from the SS to BS consisting the X.509 certificate. Together with the capabilities and Basic Connection Identity (BCID) Message 2 is sent again from the SS which contains the certificate for itself. After that finally BS reply to SS containing the AK encrypted with SS’s public key along with sequence number, life time of AK and Security Association Identity List (SAIDL).

![Figure 12: Authorization scheme used in PKMv1 protocol](image-url)
In PKMv2, the major security problems were solved. To prevent attacks this version makes secure enough in authorization procedure. After initial authorization, PKMv2 also checks for reauthorization periodically.

![Initiating the authorization protocol](image)

**Figure 13**: Authorization scheme used in PKMv2 protocol

X.509 certificates are used for RSA based authentication. In case of PKMv1 only one way X.509 certificate used but in case of PKMv2 three-way authentication is used. In IEEE 802.16e-2005, Mutual authentication problem has been solved.

At first SS sends its MCer\(_{SS}\) (manufacturer’s certificate) and then sends its own Cer\(_{SS}\) which is X.509 certificate along with a nonce; a 64 bit random number generated by the SS, BC-Identity and cryptographic Capb (capabilities). BC-Identity is assigned to SS when it enters in a network and requests for ranging.

BS responds by sending some information and a nonce when the authorization request message from SS is arrived. Additionally, For mutual authentication BS attaches its certificate (CerBS) in response to SS. BS also includes its signatures for validity in response message to SS. A 256 bit key (Pre-Au-K) with the SS’s identifier (SSID) is encrypted by the BS with the public key of SS. A 4 bit sequence number (Seq_No) for the authorization key (and its life time with the SAID’s List (SAIDL) are sent by the BS. After validating the message from BS, the SS sends the acknowledgement message with nonce created by BS and MAC address (MAC\(_{SS}\)) of the subscriber station. Authorization
Key (AK) transmitted by BS to SS in previous message is used to encrypt the NonceBS (BS generated random number) and MACSS.

The IEEE Std 802.16-2004 supports operations both in PMP and Mesh modes. Later, the IEEE Std 802.16e modifies the existing PKM protocol and renames it to PKMv1. The amendment also defines PKMv2 supporting mobile subscribers in PMP mode because the PKMv2 protocol does not support operations in Mesh mode. So, only PKMv1 is described in this part.

4.2 Authentication Protocol in 802.16:

By sending Authentication information message an SS begins authorization. The SS sends an Authorization Request Message (Auth-REQ) to the BS. By the investigation process the BS checks the SSs validation. In this period the BS inquires the encryption algorithms and protocols shared with the SS, generates an AK and share protocols between the SS. Afterwards the BS generates an AK and send it to the SS.

![Figure 14: Authentication Protocol in 802.16](image)

In this figure Cert (SS. Manufacturer) is the SS manufactures X.509 certificate and Cert (SS) is manufactures X.509 certificate. Capabilities are the SS supported data encryption algorithms and authentication. BCID is the Basic CID of SS. KUss (AK) is the Authentication key encrypted by SS public key. Seq No. is a 4-bit sequence number for AK. Lifetime gives the number of seconds before AK expires (32 bits) and SAIDList contains the identities and properties of the single primary SA and zero or more static SAs. Message 2 is sent in plaintext to promote authentication. But, in this case BS will face replay attack from malicious SS. The malicious SS is unable to get the AK from message 3 because the attacker does not have the corresponding private key. For tiring the BS the attacker can replay message 3 several times. In addition the attacker also enforces BS to contradict the SS who is the owner of Cert (SS).

For these replay attacks [13] mentioned to add timestamps in message 2, together with a signature of SS which provides the message authentication and non-repudiation. To encrypt the critical information the signature uses SS private key. Correspondingly, Message 3 also imperils SS in replay attacks. Here, SS faces the fraudulence from the malicious BS who interrupts its Auth-REQ message. The BS generates AK itself to control of the communication of the victim SS. The timestamp received from Message 2 is also replied in message 3 to ensure SS that the Message 3 responds to its request.
Timestamp from BS assures its liveness and freshness. BS signature is added at the end of the Message 3 which provides the authentication and non-repudiation of the message.

| Message 1: SS -> BS: Cert (SS. Manufacturer) |
| Message 2: SS -> BS: T_S | Cert (SS) | Capabilities | SAID | SIG_{SS} (2) |
| Message 3: BS -> SS: T_S | T_B | KU_{SS} (AK) | Lifetime | SeqNo |
| SAIDList | Cert (BS) | SIG_{BS} (3) |

Figure 15: Modified Authentication Protocol

Observing the Figure 2, we see that $T_S$ and $T_B$ are timestamps generated by SS and BS respectively. Signature of SS named $SIG_{SS}$ (2) and Signature of BS named $SIG_{BS}$ (3) are added at the end of the Message 2 and Message respectively.

From [14] we found that the Nonc and timestamp are two major methods for the verification of message. To maintain time synchronization of timestamp communicating parties are needed and this is the main draw-back of timestamp.

| Message 1: SS -> BS : Cert (SS. Manufacturer) |
| Message 2: SS -> BS : NS | Cert (SS) | Capabilities | SAID |
| Message 3: BS -> SS : NS | NB | KU_{SS} (pre-AK) | Lifetime | SeqNo |
| SAIDList | Cert (BS) | SIG_{BS} (3) |

Figure 16: Authentication Protocol with nonce in [14]

As an alternative of timestamp Nonce can be added with the message in the authentication protocol. However, the exchange of nonces only ensures SS that Message 3 is a reply corresponding to its request. But, the BS still faces the reply attack because BS cannot tell whether Message 2 is recent message or an old message.

**4.3 Security Roaming of Key Association during handover:**

As we mentioned before that since the PKMv2 is still under development, thus [13] proposed a security roaming of keying materials for handover scheme based on the basic PKM protocol.

In this section we will discuss on the security roaming of keying materials. It is necessary keep the keying materials encrypted and sent from serving BS to target BS. Due to the frequent communication between BS, it is desirable to distribute a Shared Secret Key (SK) to each pair of the BS. Here, we will consider TBS and SBS already have SK.
RAK (Roaming Authentication Key) derived from the AK shared by SBS and MSS. As we see the Figure 4, Message 2 contains N1 is nonce, which provides freshness in ACK. The TBS replies with ACK, SBS will notify MSS about the roaming acceptance information. MSS starts initial ranging with the TBS and this is occurred when the handoff exchange with SBS is finished. Without sending the X.509 certificate MSS achieves re-authentication. In the Message 5, new-AK is the current AK shared by MSS and TBS. Message 5 can be intercepted by SBS whenever it has RAK, hence decrypt the following messages exchanged between MSS and TBS. But, it is a bit better than simply using the RAK. A possible enhancement letting TBS and MSS derive the new-AK. Both MSS and TBS contribute to the new-AK.

### 4.4 Authorization and AK Exchange:

A node sends an Authentication Information message containing the node manufacturer’s certificate to the Authorization Node. Each certificate contains the node’s public key and MAC address. The manufacturer’s certificate is issued by the Certificate Authority (CA) or the manufacturer itself. The Auth Info message is used contain the manufacturer’s certificate to the Authentication Node. Without waiting for any reply from the Authorization Node, the node sends an Authorization Request message to the Authorization Node to ask for an AK and the SAIDs which the node is authorized to access. The message contains a set of supported cryptographic algorithms and the node’s certificate.

The Authorization Node verifies the node’s certificate in the Auth Request message and determines the cryptographic algorithms shared with the node and activates an AK for the node. The AK is encrypted with the node’s public key and the Authorization Node sends the AK in an Authorization Reply message to the node.

The node requests new AK from the Authorization Node in a seasonal manner. The timer is called the Authorization Grace timer. At the Authorization Grace time before the expiration of the current authorization, the node sends a new Auth Request message to the Authorization Node.
By sending a Key Request message, the node starts TEKs just after the Authorization process. The message is authenticated from the AK by a key derived. If the Key Request message from the nodes indicates the newer of the two AKs, it indicates that the node has
received the newer AK and the Authorization Node starts using the newer AK to encrypt the TEKs.

If the Authorization Node rejects the node’s request then it sends an error code. The error code containing Authorization Reject message indicates the reason of the rejection of the request of the specific node. If it is a permanent authorization failure, any further traffic from the node will be ignored. On the other hand, If the error code does not indicate permanent condition, the node will wait for a period of time and send a new Auth Request message.

The Authorization Node continuously informs Auth reply to the node message. The node obtains continuous a new AK before the expiration of the AK, otherwise the node is considered unauthorized and the Authorization Node sends the node an Authorization Invalid message. If the Authorization Node unable to verify the HMAC-Digest in a Key Request message, it replies an Auth Invalid message. After receiving the Auth Invalid message, the node waits for a period of time and an Auth Request message for reauthorization.

The message attributes of the messages in the AK management are shown below:

<table>
<thead>
<tr>
<th>Message</th>
<th>Attribute</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Info</td>
<td>CA-Certificate</td>
<td>Certificate of manufacturer CA that issued the node’s certificate</td>
</tr>
<tr>
<td>Auth Request</td>
<td>SS-Certificate</td>
<td>The node’s X.509 user certificate</td>
</tr>
<tr>
<td></td>
<td>Security-Capabilities</td>
<td>Describes requesting node’s security capabilities</td>
</tr>
<tr>
<td></td>
<td>SAID</td>
<td>SS’s primary SAID equal to the Basic CID</td>
</tr>
<tr>
<td>Auth Reply</td>
<td>AUTH-Key</td>
<td>AK encrypted with the target client SS’s public key</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Key-Lifetime</td>
<td>AK’s active lifetime</td>
</tr>
<tr>
<td></td>
<td>Key-Sequence-Number</td>
<td>4-bit AK sequence number</td>
</tr>
<tr>
<td></td>
<td>(one or more) SA Descriptor(s)</td>
<td>Each compound SA-Descriptor attribute specifies an SA ID and additional properties of the SA</td>
</tr>
<tr>
<td></td>
<td>PKM Configuration settings (optional)</td>
<td>PKM timer values</td>
</tr>
<tr>
<td></td>
<td>Operator Shared Secret</td>
<td>Key known to all</td>
</tr>
<tr>
<td></td>
<td>Key-Sequence-Number</td>
<td>Sequence number of the Operator Shared Secret</td>
</tr>
<tr>
<td></td>
<td>Key-Lifetime</td>
<td>Lifetime of the Operator Shared Secret</td>
</tr>
<tr>
<td>Auth Reject</td>
<td>Error-Code</td>
<td>Error code identifying reason for rejection of authorization request</td>
</tr>
<tr>
<td></td>
<td>Display-String (optional)</td>
<td>Display String providing reason for rejection of authorization request</td>
</tr>
<tr>
<td>Auth Invalid</td>
<td>Error-Code</td>
<td>Error code identifying reason for Authorization Invalid</td>
</tr>
<tr>
<td></td>
<td>Display-String (optional)</td>
<td>Display String describing failure Condition</td>
</tr>
</tbody>
</table>

Table 2: Message attributes in the AK management [15]

### 4.5 Traffic Encryption Key (TEK) Exchange:

During TEK exchange a node starts sending a *Key Request* message to the neighbor to request TEKs. The Key Request message is authenticated with keyed message digest termed the HMAC-Digest. The message digest is created with HMAC_KEY_S derived from the Operator Shared Secret. The neighbor verifies the HMAC-Digest in the Key Request using its key HMAC_KEY_S. If the HMAC-Digest is valid, the neighbor sends a *Key Reply* message containing two current active TEKs and key parameters to the node. The TEKs are encrypted using a Key Encryption Key (KEK) using the key encryption algorithm.
Figure 19: TEK management [16]
The node periodically refreshes TEKs supports from the neighbor. The timer is set by a configurable TEK Grace Time is set for the timer. At the TEK Grace Time before the expiration of the newer TEK, the node sends a Key Request message to the neighbor. After sending the Key Request message, the node waits for the Key Reply until timeout. If it does not receive any reply, it resends a Key Request message to the neighbor.

<table>
<thead>
<tr>
<th>Message</th>
<th>Attribute</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Request</td>
<td>SS-Certificate</td>
<td>X.509 certificate of the node</td>
</tr>
<tr>
<td></td>
<td>SAID</td>
<td>Security association identifier</td>
</tr>
<tr>
<td></td>
<td>HMAC-Digest</td>
<td>HMAC using HMAC_KEY_S</td>
</tr>
<tr>
<td>Key Reply</td>
<td>Key-Sequence-Number</td>
<td>AK sequence number</td>
</tr>
<tr>
<td></td>
<td>SAID</td>
<td>Security Association identifier</td>
</tr>
<tr>
<td></td>
<td>TEK-Parameter</td>
<td>“Older” generation of key parameters relevant to SAID</td>
</tr>
<tr>
<td></td>
<td>TEK-Parameter</td>
<td>“Newer” generation of key parameters relevant to SAID</td>
</tr>
<tr>
<td></td>
<td>HMAC-Digest</td>
<td>Keyed SHA message digest</td>
</tr>
<tr>
<td>Key Reject</td>
<td>Key-Sequence-Number</td>
<td>AK sequence number</td>
</tr>
<tr>
<td></td>
<td>SAID</td>
<td>Security Association identifier</td>
</tr>
<tr>
<td></td>
<td>Error-Code</td>
<td>Error code identifying reason for rejection of Key Request</td>
</tr>
<tr>
<td></td>
<td>Display-String (optional)</td>
<td>Display string containing reason for Key Reject</td>
</tr>
<tr>
<td></td>
<td>HMAC-Digest</td>
<td>Keyed SHA message digest</td>
</tr>
<tr>
<td>TEK Invalid</td>
<td>Key-Sequence-Number</td>
<td>AK sequence number</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>SAID</td>
<td>Security Association identifier</td>
<td></td>
</tr>
<tr>
<td>Error-Code</td>
<td>Error code identifying reason for TEK Invalid message</td>
<td></td>
</tr>
<tr>
<td>Display-String(optional)</td>
<td>Display string containing vendor-defined information</td>
<td></td>
</tr>
<tr>
<td>HMAC-Digest</td>
<td>Keyed SHA message digest</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Message attributes in the TEK management [15]

### 4.6 Secure Keys for WiMax Communication:

#### 4.6.1 Authentication Keys (AKs):

AKs are shared between the Authorization node and the node and the AK is derived from KEK, a HMAC_KEY_D and a HMAC_KEY_U. The KEK, HMAC_KEY_D, HMAC_KEY_U are derived from an AK. The AK is a 20 byte key and AK is activated by the Authorization node and encrypts and AK. Because of the algorithm the AK turns a 128-byte quantity occurs just after the encryption. The AKs lifetime is defined by the Authorization node in an Auth Reply message. Each AK is active until its expiration specified in the key lifetime attribute. In an Auth Reply message the AKs lifetime is defined by the Authorization node. An AK lifetime is also included to indicate when the AK expires. The default lifetime is 7 days but it can range from 1 to 7 days. [18]

#### 4.6.2 Key Encryption Keys (KEKs):

KEK is 128 bits long and it is directly derived from the AK. KEK is not used for encrypting traffic data. KEK is just used to encryption key where TEK generates as a random number generating in the BS using the TEK encrypting algorithm. The KEK is constructed from AK as follows: KEK= Truncate-128(SHA1 (((AK | 0^{44}) \oplus 5^{34}))), where Truncate-128(·) means to discard all but the first 128bits of the argument, a| b denotes the concatenation of strings a and b, \( \oplus \) denotes exclusive OR, \( a^n \) denotes the octet a repeated n times, and SHA1 is defined by the secure hash standard. [17]

#### 4.6.3 Traffic Encryption Keys (TEKs):

TEKs are used to encrypt data transmission between the BS and SS. TEKs is generated by BS randomly. TEK encrypted with- i) Triple-DES (Use 128 bits KEK), ii) RSA (Use SSs public key), iii) AES (Use 128 bits KEK).
The data SA defines two TEKs, one for current operations and a second to be used when the current one expires. The default value for this parameter is half a day and assumes a minimum value of 30 minutes and value of seven days. The TEK lifetime is also included to indicate when the TEK expires. The TEKs are identified by 2-bit key sequence numbers enabling 4 different keys (TEK0-TEK3).

### 4.6.4 Hashed Message Authentication Code (HMAC):

HMAC is used by the receiver to verify the sender. This process become possible for the sender where the sender creates an HMAC of the message it wishes to send using a key known by the sender and receiver. [4] Basically, HMACs are used to provide message authentication.

![HMAC Creation Diagram](image)

The figure demonstrated the HMAC creation process. The hash key is exclusive-ored (XORed) with an ipad which is the byte 0X36 repeated 20 times to match the size of hash key. This 160 bit value is appended to the beginning of the message which is then hashed. The IEEE 802.16 standard defines the use of SHA-1 to compute the hash. Afterward the hash again XORed with an opad which is the OX5C byte repeated 20 times to match the size of hash key. The 160-bit value is appended to the beginning of the output of the previous hash. After combining the two hashed values HMAC is produced.
Chapter Five: WiMAX Security Analysis

This chapter include comparison between IEE802.11 and IEEE 802.16 and explanation of the vulnerabilities.

IEEE 802.11 introduced as a first expanded network in wireless arena. More efficient channel coding and free spectrum and cheapest hardware interface made popular 802.11 based network. For this circumstance, it is a matter of interesting issue to exploit its vulnerabilities. However, widespread deployment of 802.11 make concentrate to potential attack. Not only that, Security flaws explored by professionals and general user. Denial of service, cryptographic weakness plays an important role behind the vulnerabilities.

In this chapter we will discuss and analysis of 802.11 vulnerabilities, their reflection of exploit, finally there will be comparison whether these vulnerabilities exist 802.16 standard.

If we considered previous publication based 802.11 vulnerabilities where they focused two main criteria namely identity and media access control vulnerabilities. Now when we discuss about 802.16 vulnerabilities we will consider as well following this two categories.

5.1 Vulnerabilities comparison between IEEE 802.11 and IEEE 802.16

5.1.1 Identity vulnerabilities:

The vulnerabilities arise due to impact trust of 802.11 network and source address. As we know MAC layer contain 12 byte address where each frame contain sender and receiver address. If we focus class one frame where include management and control message but surprisingly 802.11 didn’t include and identity mechanism which ensure correctness and verification of authentication data. As a result, attackers take this advantage and spoof other nodes, request Mac service on favour of him. This may leads version distinct vulnerabilities.

De-authentication Attack

When 802.11 clients selected an access point which authenticate itself first, to the access point before continue further communication. Authentication framework allows access point and client, to explicitly deauthenticate each other. Through this message is not authenticate by using any key material. As a result this message is spoofed by attackers for false appearance of AP or client or direct to other party. Until authentication became re-establish, AP and Client will stop authentication and discard. All next packet duration of to make a function reestablishment and how quickly the client take action to re authenticate also any high level time slot. That may depend on necessity of
communication. Client may keep transmitting or receiving data specifically to persistent the repeating of attack.

It makes great facility when attacker choose deny access for individual user in simply use deny service on whole channel. To accrue these goal attackers should need efficiently monitoring channel. Moreover when a new authentication compiled smoothly a deauthentication message should send this place. In order to escaping protect to neighbour AP, attacker make through scan of all channel as if client cannot switched or overlap another.

**Dissociation**

Association protocols which use authentication contain similar vulnerability. When authentication take place on a client by using multiple AP then the 802.11 standard allow association message as if agreed client and AP which means forward packets on the wired network on behalf of client.

![Graphical representation of deauthentication attack](image)

Figure 21: Graphical representation of deauthentication attack, attackers need generate one packet for each six exchange. [24]

Association frame also an unauthenticated on authentication. Moreover, similar to deauthentication 802.11 facilitate disassociation message. In deauthentication attack, exploiting vulnerability work same. Nevertheless, dissociation attack is more efficient then dissociation. It can prove according to this sense where deauthentication put more pressure to victim node as if associated state return then dissociation. [24]
Power Saving

It is also identity based vulnerability. In order to preserve energy, sleep state may occurred when client unable to transmit or receive. When enter sleep state client ensure it to the access point as if this period can buffer bounded traffic for node. [24]

When the client awakened count AP for pending traffic then the buffered data is delivered by Access Point. On the contrast, discard its buffer content. Polling message is spoof behalf of client. When it is in sleep mode then it ignores client packet. These types of occurrence are done by the AP.

In the same way, it is possible to make false measuring on client node which refers no packet on AP, though it is not true. Buffered packet presents itself as a traffic indicator map (TIM). It is also known as periodically broadcast packet. When TIM is spoofed, an attacker can convince client as if, it shown absent of pending data which occurred client to rivet back sleep mode. Power conserve technique depend on the Access Point and clients time period depend where client concern itself time of awake.

802.16 standard:

Same as 802.11 use 802.16 also MAC message for de-authentication. Initially (RES-CMD) Rest command message to send SS by BS as it can reset later itself. BS used this malfunctioning to SS.

![Flowchart](image)

Figure 22: Using RES-CMD failure De-authentication attack [22]
When RES-CMD is received by SS. MAC is became reinitialize and take step to repeat it. Moreover, DREG-CMD (De-register command) sent by BS to SS as if it can change access state. There are many reasons to send it by BS; one of them main is leave transmission channel.

On the other hand, both 802.11 and 802.16 has own protection system abuse of command. Most renowned protection technique is HMAC with SHA-1 use for authentication message. Working pattern of HMAC firstly calculated message by using genuine message and shared secret key. Where 160 bit hash keyed contain.

After receiving message, recalculate again Hash message and shared secret key. Compare it with calculated hash. In order to ensure same hash message and secret key should be same. Its key cannot be compromised any condition, if it wrong contained message became changed.

Wimix standard is not free from De-authentication vulnerabilities. To prevent this some precautionary step should be initialized. For example to ensure secrecy when key sharing occurred BS and SS. This is not true for 802.11 due to security WEP flaw. If it exploit anyhow, authentication procedure became meaningless. Some security feature of Wimix standard is more strength compare to wireless LAN likely encryption method is secure enough then WEP. Moreover changing scope of encryption technique, it is either 128 bit TDES or RSA. Hash algorithm is secured cryptographic techniques which sense possibility of reduce attack to find our real key for decrypt each hash. [22]

**Man in Middle Attack**

It is also known as Access Point (AP) spoof. When attacker take place and look after all traffic between two nodes using this technique an attacker may concern all information of network. This attack became more potential on wireless network compare to wired network. Because in wired network require live access of medium. On the other hand, wireless network require only establish an Access Point, which use for association. After establish AP replicated SSID, MAC address etc.

In next stage victim may connect to rough access point. It can be occurred by two steps. First one is waiting for user to create connection themselves. Second one is legitimate access point using denial of service for reconnect it. As we know depend upon strength of signal, AP selected on 802.11 network.

It is a matter of fact that an attacker has to prove victim that signal strength of AP is more powerful. For this types of attacker make place his/her AP nearest to victim for legitimate AP. When rogue access point successfully establishes a connection for victim it reflects himself as a legitimate one and traffic is followed toward Attacker node. When completion this stage, attacker use different software to acquire password of victim. This way attacker ensures his/her presence as a authentic user on network.

Due to limitation of strong authentication on AP and node, these types of attack exist. As an all credential of AP broadcast on network make more to the eavesdropping on network. The WEP is also vulnerable where node uses to authenticate them on AP. Not only eavesdrop but also use crypt analyzer to accrued password.
802.16:

As far examined vulnerabilities in WiMAX access point exist same as 802.11 which may call BS spoof. In PKM to identify BS and SS each other use message exchange. To ensure strong authenticate of SS use below process. BS receive message from SS with X.509 which ensure authentic manufacture of SS. Second message also send by SS also contain x.509 certificate and public key, SAID and SSs certificates. It is used to ensure authorization of SS and public key use BS to able message replying. Third message is send when SS became authorized to the BS. It Indicate protocol no such requirement. [23][26][27]

Media Access Vulnerabilities

It is impossible to detect real Collision Detection (CD), if terminal became hide and access control to channel which interlinked one behind another virtual carrier sense and physical carrier sense, it uses attacker for exploit.

To make prioritize scheme on radio medium windows are defined four times. This step consist two main important things are short interface space and distributed coordination function inter frame space. When a frame decide to send on this time SIFS use as a part of exchange acknowledgement of previous frame whereas DIFS use as a part of initiate frame exchange. In order to avoid collusion after DIFS expire, it is divided two ways. Nodes who wish to transmit pick a slot with equal probability and transmit it randomly. Random exponential algorithm is used to collusion avoidance.

If waiting time of SIFS interval became longer, attacker send a short signal on this time before SIFS period expire. In 802.11b SIFS period only 20 microsecond and make disable access of network require 50,000 packet per second.

Serious vulnerabilities arise when mitigate collusion occurred by virtual carrier sense mechanism. The time duration of each channel is reserved at frame carriers. This value used for each node. As a network allocation vector (NAV). When value of NAV became zero, it indicate transmit is allowed. This mechanism is used by express RTS/CTS hand shake. When transmit is not done properly due to hidden terminal this time handshake is used synchronized channel access.

A small RTS frame send when start handshake but it duration is enough RTS/CTS sequence completing which include data frame, CTS frame, acknowledgement frame. The receiver node acknowledges RTS with CTS which contain new updated interval for elapsed time sequence. Each node might be near radio range or NAV in order to updated sender or receiver node. Future communication will defer all transmission. It is important to implementation when RTS/CTS are not used all time with respect virtual carrier sense.
Gradient part of attacker frame denote reserved time by duration field. Continuous send of attack frame prevent back to back nodes from sending legitimate frame.

Attacker can get scope as enough duration field which remove obstacle to gain access. Afterwards it help get access any frame as refer to control NAV include acknowledgement and RTS to get advantage. As a well behaved node response and RTS with CTS, attacker cooperate real node to spread attack next time as if its own. This result make attacker transmit flow extremely low either use directional antenna which means probability of locating being reduced.

NAV use null second on 802.11b network. In strategy shows an attacker need 30 times second for jamming channel. It becomes worth that CTS, RTS an ACK are unauthenticated. If they are authenticated then they available only non repudiation. According to design, impact some of all nodes channel at virtual carrier sense feature.

802.16

There are two different kinds of connection data transport connections. It is divided in to three sections management categories, basic and primary. When Management joint network basic connection became establish. On entry time network primary connection establishes but when delay tolerant occur it used this time for encapsulated message i.e. (DHCP, TFP) secondary connection is used. Transport connection is used according to demand.

In security model figure (23) during authentication and entry network is done by sequel. Moreover association and security key also establishing during this time. The following steps done network entry on MS [25]

- Negation of capability.
- Establishment of authenticate step (authorization, authentication).
- Synchronization between BS and downlink.
- Discover uplink vacancy channel.
Eavesdropping threat divided two way management message and user traffic. In management process which also unencrypted provides all necessary information to the attacker. This make interrupt on communication. No matter for attacker to resolve it without any technical problem. If we concern user prospective then eavesdropping management process is became expensive for the user. Although this attack use for mapping network, it is a critical threat for user and major threat for system.

Authentication techniques for MAC layer management are HMAC and OMAC. OMAC use AES algorithm for protection whereas HMAC is not used.

Impact on attack might be more crucial when it is on operation on communication by flooding more traffic to victim denial of service can execute. Though this reflect medium is on the system but highly on the user due to lower source to handle huge number of invalid message.

5.1.2 Potential vulnerabilities to meet in 802.16 standards:

IEEE 802.16 standard implementation is not properly done yet, we discuss potential vulnerabilities according to pervious research and implementation.

In order to make an attack attacker should capable to inject and transmit message. There are two problem for attack to take place the network first of all create message and secondary perfect time to inject message on network. In this section, we will make overview this problem and define some vulnerability.
Inject and message generates:

In 802.11 an attacker uses arbitrary message to gain the result. It is true that there was no potential techniques as user threats at beginning stage of 802.11 for this using arbitrary process take more time to discover.

As an 802.16 is newly invented technology and enough fashioned on network arena also real time implementation till test bed. So attacker still out of enough resource to breakdown its knee. But it is not true that they are not trying.

Commodity hardware is used in 802.11 frame stated by Bellardo and Savage. They use more buffers on network card by using debug port. Through this arbitrary message insert on network before control frame it sends.

![Diagram](image)

Figure 25: Use of AUX port to circumvent [24]

SAP is used in 802.16 communications between different protocol and control message. For this it is hard for arbitrary message to pass SAP. If we focus protocol stack of both 802.16 and 802.11 which already discuss previous chapter near about same.

Though specification and state full implementation is more difficult and it is our out of focus does access of interface device and firmware. Hardware implementation is
important to construct 802.16. If any product invents to provide debug access on firmware, its help attacker. Otherwise, 802.16 products still stand alone.

**Inject timing message:**

Likely arbitrary message, inject timing is another important issue which is not an easy job. Though it is a hard job but we have to consider not only injecting message but also victim affected by this message as real threat.

It happened by spoofed management message and cross time limit. Furthermore, attackers should have to inject message right time. Not only this we have consider synchronization and have in mind attackers tries to send message SS to BS using propagation delay. But it is true that delay encounter is negligible when try to send message as Base Station. It is also a principle that up to a certain time MAC considered specific message and in wrong time well formed message by victim cannot react anymore. Different specification of 802.16 use different transmission schedule and message injecting time also became different. There are two basic type of transmission system namely TDD and FDD. Below we provide short overview of both two categories.

- **TDD:** There is little probability to get chance at downlink. BS filled all sub frame of downlink. If there is any gap occurred null counted to fill criteria. For transmit to receive from BS to switch there is a little vacant frame which is allowed between uplink and downlink. In this case to consume power when BS send null, transmission is not allowed to SS. Gap between end uplink and next frame known as Rx/Tx delay time. Though it is not easy job to breakdown its strength but same frame is added as if SS can join uplink frame.

  ![TDD Frame Diagram](image)

  **Figure 26:** Inject message on TDD frame. [22]

- **FDD:** Different frequency use for uplink and downlink channel at FDD. Where downlink use as discrete bursts. Uplink and downlink scheduled as if it can support SS half duplex. Sometime up and downlink became idle. On this time attacker inject message. Downlink specifies transmission occurred between different modulation and FEC by BS. It cannot provide particular knowledge for specific SS. When attacker sending message SS always emphasis on downlink response. Using this facility when packet is not come from BS, attackers use this arbitrary. Though it is undefined priority success. Collusion is occurred at downlink when same time packet sends by both Bs and attacker. In crowded
network there is no gap to send message by attacker which make disappear to reach goal.

**MAC Layer:**

It provide well defined transmission step by step like as state machine provide state by state transmission. through this it archive power to discard message even if well defined. it can be clear through this example. If we allow the process as attacker, an authorization request send by SS from BS on initial time’s send to SS after checksum. When it valid on respect of network, BS send reply with authentication and authorization key.

When discard occurred any message by BS then re-authenticate it, SS have to stay. Auth-Reject is not a perfect toll to attack because it does not contain any authentic certification (HMAC, Serial no). When send an authorization request, MAC considered message just for limited time and auth reject also come on specific time. This time is stated and acted.

**5.1.3 Attacks on 802.16**

**RSP-RNG:**

Before joining network SS send BS a ranging request (RSP-RNG) which denote presence of BS for SS including frequency, power and transmission time profile. BS replied using same technique. Previous version of 802.16 SS send RNG request to Bs with period basis. If it cannot complete periodic stage to re-initialize MAC it removes from network. By using free time when SS don’t make any communicate with BS, attacker use transmitting this time. As a result SS became discard from network and when continue occurred this process after a certain time it is totally discard. The change is occurred at 802.16a where packets recive from SS use BS to adjust range. Though RSP-RNG use on transmission (Bs to Ss) till its vulnerable. The main feature is compare to SS RSP-RNG more tuning.

In order to change up and downlink RSP-RNG used by Bs to request SS, transmission power renew for re initialize MAC. As a unencrypted RSP-RNG became exploitable. Power level, timing and ranging required for 802.16 addresses.

Exploiting RSP-RNG many formula can use .one of the RSP-RNG send by attacker contains ranging field which can respect of abort.
To shift victim SS to another channel RSP-RNG can exploit. Using downlink frequency and uplink ID override attacker can send message once more time. When an attacker run behind a discrete channel on a rogue BS, SS might tune it with spoofed BS. When BS is empty on specified channel, SS move on original channel. Using Scan discard tech this process is done. When scan occurred by SS, idle frequencies discard. Unfortunately, attacker might also use same time slot when SS use 2 ms to scan channel and shift another.
Invalid Auth Attack:

PKM – Req and PKM-RSP used on management. Communication occurred between BS and SS via PKM-Req and PKM-RSP.

Auth state machine use on PKM, PKMs 8 bit use as serial key. Corresponding identifier include when PKM-RSP response by BS. Otherwise it ignore by depend on PKM message attributes can make varies. Attributes field basically contain error code, string of display and key lifetime. Same way PKM message make negative impact on authorization these are TEK invalid, auth invalid, auth request key. If use any one of them might chance to fall de-authentication attack. But sometime some of this require HMAC digest. Through it is harder to break HMAC.

Figure 28: Focused on invalid message at authorization state machine. [22]

So break down cryptography is the way for attacker to achieve network control. But it is also too hard. The reason for those message hamper authentication are follows: During wait state SS accept reject message for limited tie interval. In case of Key reject message. There is dependency between PKM identifier and SS. Moreover 256 numbers may choose from it. Without HMAC key reject message is invalid for attack. Last one is Auth invalid message. Presently it is not necessary to send current MAC time and cannot authenticate through HMAC. For a little time SS stay at auth wait state. Authorization valid occurred on this state. Moreover, it cannot involve PKM serial key. Probability became high to accept rogue message without PKM. Re auth occurred when auth invalid message received any SS and wait until new message from BS. If time expire before receive by SS from BS, it sends re-auth request on network if it till same state. Auth reject message is received by SS.
5.2 Security Threats specially meets of IEEE 802.16 in Mesh Mode

Threats especially meets on mesh mode are described below:

5.2.1 Topological Attack

Every Subscriber station broadcast MSH-NCFG network Descriptor message in the mesh network regularly. To obtain coarse synchronization in new SS, Every MSH-NCFG carries sensitive physical layer information. Moreover, it provides list of neighbouring SS and vacant BS of sender including nodes id of BS or neighbour and existing hop count. After initialization on network or signal loss, new SS try to explore MSH-NCFG: Network descriptor message. SS choose a sponsor node to obtain BS information and it help joining network on new SS.

The main obstacle of MSH-NCFG message is not encrypted and authenticated. It’s favour on topological attack to take place [30]. Wormhole and Sinkhole two leading topological attack on mesh mode.

Wormhole:

The main principle of this attack, without modifying and spoofing attacker use reply MSH-NCFG message

![Wormhole Attack Diagram](image)

Figure 29: Wormhole attack. As an attacker tunnel message through hidden channel, node A believe node B as neighbour. [30]
In figure 29, between nodes A and B attacker create a hidden channel. It use for tunnel MSH-NCFG from nodes and reply them. Through this node A and B trusted as a neighbour. Attacker monitor MSH-NCFG message at one place but shift and reply them different place. This leads breakdown network topology and creates harmful attack to routing protocol [31].

**Sinkhole:**

When a malicious node act as a sponsor node by calming a shorter path to BS and create Scope to entry traffic in local area.

![Figure 30: Sinkhole Attack](image)

Collecting information on network traffic, it’s possible for malicious node monitoring, modifying and spoofed Authorized information within BS and new nodes.

**Authorization threats**

To access mesh network, candidate node require authorization step. A handshake procedure between candidate and authorization canter through PKM-REQ achieved this.
As illustrated in Figure 31. Candidate node send PKM–REQ: auth info message and PKM-REQ auth request to authorization centre.

**Authentic verification**

When verification completed with replies PKM-RSP: auth reply message from authorization center including AK (Authorization key) with life time, Sequence number and OSS (including lifetime, sequence no) and SA.

When verification is denied it’s replied only PKM-RSP with error code and display string.

**Attack through malicious node**

In authorization step, when candidate node send data to sponsor node this time it can be modifying and intercepted by attacker. Moreover if sponsor node in unfaithful and malicious intension then its remain possibility to impersonate and eavesdropping attack.

Cryptographic capabilities are include in PKM–REQ auth req message. Use of strong cryptographic algorithm denotes secure traffic. Modifying PKM-REQ an attacker uses security rollback when weak cryptography algorithm is used on candidate and network communication.

**Open secret of OSS (operator shared secret)**

When different authorization process send authorization message to authorization centre it create problem to identify. This unclear identification of Auth SA gives advantage attacker to reply message.
In this illustrate example of open secret of OSS with reply attack. Attacker intercept PKM-REQ auth request message from ordinary node later reply it BS A or BS B. because similarity of original and reply message can’t distinguish by BS. As a result, attacker can disclose OSS.

**Auth Request message attack**

Before sending AK and related contents, message is send. To negotiate between cryptographic suites and request authorization key to BS, Auth request is use. When Security level are not same between BS and SS, it notified by BS as a perm auth reject to SS and through this SS goes silent stage of authorization state machine. Using this scope when malicious attacker modify security attributes in Auth request message, BS assume that SS unable to necessary cryptographic suits and causes permanent error condition on BS with perm auth reject message.[28]

**5.2.2 Threats to link Establishment**

In mesh mode any node can keep more than a single active link. In Figure 33, illustrate three way handshake between nodes i.e. A and B.

![Link Establishment process diagram](image-url)
Link process algorithm can work following way:

- \( A \rightarrow B: \text{HMAC}\{\text{Operator Shared Secret, frame number, Node ID of node A, Node ID of node B}\} \)

- \( A \leftarrow B: \text{HMAC}\{\text{Operator Shared Secret, frame number, Node ID of node B, Node ID of node A}\} \)

- \( A \rightarrow B: \text{Accept, Random unused link ID} \)

This process depends on secrecy of OSS security. If attacker disclose OSS can get access to the network as likely authorized node and create establishment link with other node.

When OSS shared by all nodes it can easily grabbed by attacker. Another way attacker can eavesdrop it new node acquired PKM-RSP auth reply message from sponsor node.

### 5.2.3 Threats to TEKs

Protect the message confidentiality HMAC digests are attached to the message. As HMAC digest are calculated from OSS. So any way attacker can intercepted or disclose OSS, message tempering is not impossible.

### 5.2.4 Traffic Threats

In the IEEE 802.16, only data traffic is encrypted. The generic MAC header and all MAC management messages are not encrypted and as a result forge or eavesdropping attack can be arrived. Two cryptographically methods are available to protect the data traffic, one is DES in CBC mode [IETF RFC 2405, 1998] and other is AES in CCM mode [IETF RFC 3610, 2003] where AES in CCM mode provides confidentiality by encrypting the MAC PDU payload with corresponding TEKs. AES-CCM provides confidentiality and authenticity for the MAC PDU payload.
Chapter Six: Conclusion and Possible Enhancements:

Wimax is a cutting edge technology in broadband wireless communication and focused attention service provider as if more promising and efficient. Ensure quality of service, low latency, last mile access ensure its reliability. Though it is not free from security weakness and still research is being continuous to overcome this limitation. In this thesis we tried to figure out chapter wise following issues:

- Characteristics of 802.16 standard which includes changing occurrence according to 802.16- 2001 to 802.16e- 2005.

- PMP and Mesh mode operation where man in middle attack occurred to fool other nodes and PMP mode access less resource to other nodes send fake request. Use PKMV2 instead of PKM. Proposed EAP at PKMV2 and RSA based authentication.

- Description MAC and Physical layer vulnerabilities.

- In chapter three, security snapshot of Wimax standard in mesh network to identify vulnerabilities. Which covers
  - Overalls picture of mesh network including protocol and authentication steps.
  - Exchange of key and cryptographic technique.
  - Secure certification.
  - Comparison between wireless and Wimax & explanation of vulnerabilities describe in chapter four which comprise
    - Identifying vulnerabilities and make comparison with 802.16 standard.
    - Countermeasure spoof, men in middle attack at wireless network and how possible enhancement at Wimax. MAC vulnerabilities, RTS & CTS handshake and how it can be substitute at Wimax through DHCP and TFT.
    - Focus on some potential vulnerabilities which meet 02.16 standard to inject message generate and inject timing message at TDD and FDD.
    - RNG-RSP, Invalid Auth attack (PKM) focus invalid message authorization state.
In chapter four we concentrate on Privacy key management protocol improve scheme proposed proposal to become more strength it.

6.1 Protection against the WiMAX attacks:

6.1.1 Mutual Authentication:

The absence of a BS certificate is the most critical security flow of IEEE 802.16 standards. The PKM-MSH protocol provides the mutual authentication to protect against forgery or man-in-the middle attack. In order to protect from the attacks it is necessary to replace one way authentication scheme by a scheme that supports mutual authentication.

6.1.2 Spreading technique for jamming:

Jamming is introduced to the physical layer attacks in WiMAX technology. Spreading techniques can be reduced the jamming attacks, e.g. FHSS or DSSS. It is easy to detect jamming with Radio monitoring equipment.

6.1.3 Data Protection Error:

DES-CBC is used for encryption in 802.16 std. To establish a secure WiMAX communication DES-CBC needs an IV (Initialization Vector). But, the security leak is that IV is predictable where an attacker would be able to achieve IV. In order to solve the problem a new per frame IV should be generated randomly and insert into the payload. This process will protect the data from decryption the data during traveling the network where the attacker will not be able to predict the IV.

6.1.4 Authorization Node Spoofing:

To enable a node authenticate, the PKM-MSH protocol provides the mutual authentication where a node can be recognized the attack in the authentication process. Additional CA certificates can be incorporated for a node to verify the Authorization nodes certificate. Certificate chain exchanging process defined in PKM-MSH.

6.2 Security Improvements:

6.2.1 Certificate Chain:

The Certificate chain Request and Certificate chain Reply message are added to enable a node for verifying the Authorizations node certificate where the messages provide to complete RSA authentication in the PKM-MSH.
6.2.2 RSA based authentication:

In the RSA-based authentication method carries its own certificate in the authentication reply message to prove its identity the handshake is as follows-

1) RSA. Request (SS → BS): MS_Random, MS_Certificate, SAID, SigSS.

2) RSA-Reply (SS ←→ BS): MS_Random, BS_Random, Encrypted pre-PAK, Key Lifetime, Key Sequence Number, Bs_Certificate, SigBS

3) RSA-Acknowledgement (SS → BS): BS_Random, Auth Result Code, Error-Code, Display-String, SigSS.

Here, random numbers are included in authentication message to prevent reply attacks. The method supports mutual authentication between SS and BS which is the consequential improvement to WiMAX.

6.2.3 Cryptographic issues:

With smaller key size Elliptic Curve Cryptography (ECC) performs as the same level of security of RSA. Compare with RSA [1] mentioned that 160-bit ECC provides security to 1024-bit RSA and 224-bit ECC provides security to 2048-bit RSA. In addition, ECC propose faster computational efficiency under the same level of security, energy and bandwidth savings and memory. Eventually, in future substitute of RSA based cryptography ECC can be incorporated in to IEEE 802.16.

6.2.4: Random number & Signature system:

In the PKM-MSH messaging system the random numbers prevents nodes from replay attacks. If an attacker steals a message and attack by the resending message then the repeated random number can be detected by the receiver. The receiver able to ignores the message for the mismatching random number subsequently.

If an attacker achieve the accurate random number, the random number, the random number must be verified by the signature. As a result, the attacker would not able to attack because he/she unable to create the signature for not having the private key.
6.3 Future work

Security description considered as future implementation of new products in market and meet new vulnerabilities. We propose some developing area which make more efficient and secured network.

- Integrity of both PMP and Mesh mode
- Instead of establish neighbour link have to evaluation strategies secure handshake.
- Use of message management likely Wi-Fi.

Research will be continuous to meet the face new application by manufactured and develop protocol and testify against it also explore hidden vulnerabilities.
## Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advance Encryption Standard</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>ARQ</td>
<td>Automatic Repeat Request</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BCID</td>
<td>Basic Connection Identity</td>
</tr>
<tr>
<td>BRH</td>
<td>Bandwidth Request Header</td>
</tr>
<tr>
<td>BS</td>
<td>Base Station</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CPS</td>
<td>Common Part Sublayer</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Checking</td>
</tr>
<tr>
<td>CS</td>
<td>Convergence Sublayer</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame Check Sequence</td>
</tr>
<tr>
<td>FDD</td>
<td>Frequency Division Duplexing</td>
</tr>
<tr>
<td>GMH</td>
<td>Generic MAX header</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
</tr>
<tr>
<td>KEK</td>
<td>Key Encryption Key</td>
</tr>
<tr>
<td>LOS</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MSH-NCFG</td>
<td>Mesh Network Configuration</td>
</tr>
<tr>
<td>MSPU</td>
<td>MAC Service Data Unit</td>
</tr>
<tr>
<td>NLOS</td>
<td>Non Line Of Sight</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OFDMA</td>
<td>Orthogonal Frequency Division Multiple Access</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PKM</td>
<td>Privacy Key Management</td>
</tr>
<tr>
<td>PMP</td>
<td>Point-to-Multipoint</td>
</tr>
<tr>
<td>PTP</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>QAM</td>
<td>Quadrature Amplitude Modulation</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>QPSK</td>
<td>Quadrature Phase Shift Keying</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SAIDL</td>
<td>Security Association Identity List</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Point</td>
</tr>
<tr>
<td>SS</td>
<td>Subscriber Station</td>
</tr>
<tr>
<td>SSID</td>
<td>Subscriber Station Identification</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>TDD</td>
<td>Time Division Duplexing</td>
</tr>
<tr>
<td>TDEA</td>
<td>Triple Data Encryption Standard</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TEK</td>
<td>Traffic Encryption Key</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WMAN</td>
<td>Wireless Metropolitan Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
</tbody>
</table>
Bibliography


20. Yun Zhou and Yuguang Fang, “Security of IEEE 802.16 Mesh Mode”, Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 Tel: (352)392-8576; Fax: (352)392-0044


23. M. Barbeau, 2005, “WiMAX/802.16 Threat Analysis” School of Computer Science Carleton University, 1125 Colonel by Drive. Ottawa, Ontario, Canada.


25. Michel Barbeau, “WiMax/802.16 Threat Analysis”, School of Computer Science Carleton University, 1125 Colonel By Drive Ottawa, Ontario, Canada


