DETECTION OF JAMMING ATTACK IN WiMAX BASED COMMUNICATION SYSTEMS

Enrolment No.	**:**	**122209**
Name of Student	**:**	**Tanu Bhardwaj**
Name of Supervisor	**:**	**Dr. Hemraj Saini**

May 2014

Submitted in partial fulfilment of the Degree of

Master of Technology

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT, DIST. SOLAN, (H.P), INDIA

CERTIFICATE

This is to certify that the work titled **"DETECTION OF JAMMING ATTACK IN WiMAX BASED COMMUNICATION SYSTEMS"** submitted by "TANU BHARDWAJ" in partial fulfilment for the award of degree of Master of Technology in Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor: .... 26th May 2014,

Name of Supervisor: **Dr. Hemraj Saini**

Designation: **Assistant Professor**

Department: **Computer Science & Engineering**

Date: 26-05-2014,

ACKNOWLEDGEMENT

This may seem long but the task of my thesis work both theoretically and practically may not have been completed without the help, guidance and mental support of the following persons.

I would like to thank my supervisor Assistant Professor, Department of Computer Science & Engineering, Jaypee University of Information technology, Waknaghat, **Dr. Hemraj Saini** sir for his constant help and guidance and provided me the idea and related material for the project proposal. He indeed guided me to do the task for my thesis in such a way that it seems to be research work. His continuous monitoring to support me and my research work encouraged me a lot for doing my thesis in very smooth manner.

In last, I would also like to take this opportunity to thank my friends and family, especially my parents for their continuous support and encouragement.

Signature of Student: ....T Bhardwaj.......

Name of Student: Tanu Bhardwaj

Date: .....24-05-2014....................

TABLE OF CONTENTS

Chapter 1 Introduction

Chapter 2 Preliminaries and Background

Chapter 3 Overview of IEEE 802.16 Layers

Chapter 4 Introduction To WiMAX

Chapter 5 Security Analysis At Media Access Control (MAC) Layer

Chapter 6 Security Analysis At Physical (PHY) Layer

Chapter 7 Detection of Jamming in WiMAX

Chapter 8 Theoretical Methodology

Chapter 9 Simulation

CERTIFICATE

This is to certify that the work titled **“DETECTION OF JAMMING ATTACK IN WiMAX BASED COMMUNICATION SYSTEMS”** submitted by “TANU BHARDWAJ” in partial fulfilment for the award of degree of Master of Technology in Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor: ....

Name of Supervisor: **Dr. Hemraj Saini**

Designation: **Assistant Professor**

Department: **Computer Science & Engineering**

Date:

DECLARATION

I declare that this thesis entitled **“DETECTION OF JAMMING ATTACK IN WiMAX BASED COMMUNICATION SYSTEMS”,** submitted by me for the award of degree of Master of Technology in Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat is original and it has not submitted previously to this or any other University for any degree or diploma.

Signature of Student: ....

Name of Student: Tanu Bhardwaj

Date: ....

ACKNOWLEDGEMENT

This may seem long but the task of my thesis work both theoretically and practically may not have been completed without the help, guidance and mental support of the following persons.

I would like to thank my supervisor Assistant Professor, Department of Computer Science & Engineering, Jaypee University of Information technology, Waknaghat, **Dr. Hemraj Saini** sir for his constant help and guidance and provided me the idea and related material for the project proposal. He indeed guided me to do the task for my thesis in such a way that it seems to be research work. His continuous monitoring to support me and my research work encouraged me a lot for doing my thesis in very smooth manner.

In last, I would also like to take this opportunity to thank my friends and family, especially my parents for their continuous support and encouragement.

Signature of Student: ....

Name of Student: Tanu Bhardwaj

Date: ....

Abstract

Wireless broadband play an important role in the growth of telecommunication industry, both wireless and broadband have emerged as the catalyst in the field of communication. WiMAX is a wireless technology for high speed broadband access in the agrestic areas and can provide the data rates as high as 100 Mbps for mobile user and 1 Gbps for fixed user using either line of sight (LOS) or non-line of sight (NLOS) type of propagation. It is based on the IEEE 802.16 standard, which specifies the Physical (PHY) and Media Access Control (MAC) layer for the WiMAX. The Physical (PHY) layer of WiMAX uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission scheme to enable high speed data, video and multimedia communication.

Wireless communications are considered to be more vulnerable to attacks than the wired communication and thus it also concerns to WiMAX. The Security is handled by the privacy sublayer within the WiMAX Media Access Control (MAC) layer. The security attacks are possible at the Media Access Control (MAC) layer and the Physical (PHY) layer of WiMAX. The two major attacks at the Physical (PHY) layer are jamming and scrambling attack. Jamming is an intentionally activity of transmitting radio signal to disrupt the communication. This thesis is devoted to develop a simple and efficient technique to detect jamming in WiMAX based communication system. The developed technique involves the metrics such as Signal to Interference plus Noise Ratio (SINR), Signal Strength, Packet Delivery Ratio (PDR) and Channel Sensing for detecting jamming in the WiMAX system. Finally, we conduct the simulation to evaluate the effectiveness of the developed technique.

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

WiMAX has been widely accepted as the next generation system for providing broadband communications in remote areas. It is based on IEEE 802.16 family of wireless network standard and formally consented by the WiMAX Forum. WiMAX Forum gives the certification to the vendors or service provider to sell fixed or mobile wireless products as WiMAX certified, thus guaranteeing a level of interoperability. The IEEE 802.16 standard covers the frequency bands between the range of 2 GHz – 66 GHz including both licenced and licenced exempt bands and specifies a metropolitan area networking protocol that will enable a wireless alternative for cable, DSL for last mile broadband access, as well as providing backhaul for 802.11 hotspots. WiMAX supports low latency applications such as data, Voice over Internet Protocol (VoIP) and IPTV service, provides broadband connectivity without requiring a direct line of sight (LOS) between subscriber station and the Base Station (BS) and will support hundreds of subscribers from a single Base Station (BS) [1, 2].

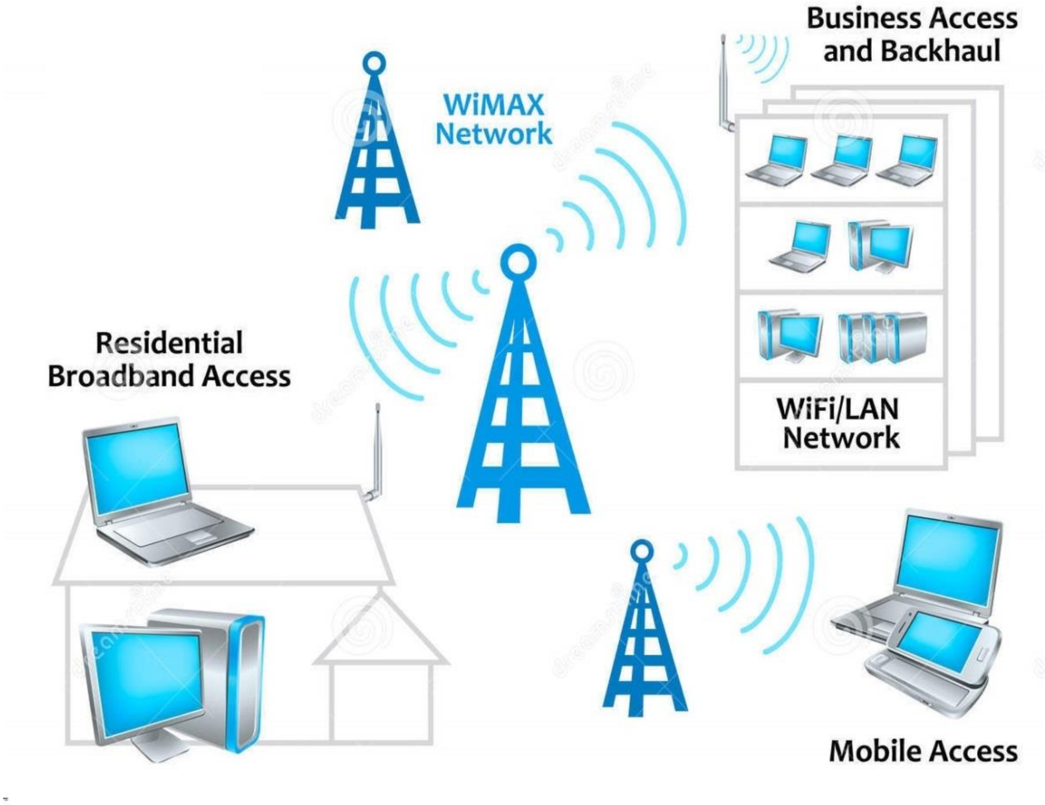


Figure 1.1: WiMAX Network

1.2 Motivation

WiMAX is an IEEE 802.16 specification designed to be an umbrella technology for future wireless broadband access. In countries such as India the possibilities for broadband access is extremely high, taking into account the trend of the internet requirements. Wire-lined technologies require Telephone/Cable lines to serve users over long distances. A viable complement to Cable/DSL based services is WiMAX, which connects users to the internet even in a remote area. At first glimpse WiMAX would seem similar to 3G cellular technologies, since both networks can transmit data and voice but by design cellular 3G is voice-centric while WiMAX is data-centric. It is an adopted global standard and has seen an increased interest because of its geographical flexibility, low cost and high performance wireless broadband access.

A question that comes intertwined with WiMAX is how secure the communication is in the network. As WiMAX is the future technology the security concern is very important. In future all the world is connected using WiMAX technology, so techniques should be developed and evolved to defend against the security threats and malicious attackers.

Jamming is major threats for the wireless communications especially in defence, this type of attacks have their roots in each type of communication from cellular to ad-hoc, from Wi-Fi to WiMAX. Jamming results in the disruption of communication among the users and making the system unavailable. It is one of the most threating attacks in wireless communication that lead to the Denial of Service (DoS), Distributed Denial of Service (DDoS) and etc. All these kind of attacks are also possible in WiMAX communication system.

1.3 Problem Statement

WiMAX is a state of art wireless technology, which is nearly a decade old technology that aims, is to provide high speed wireless broadband access in the rural area. The main motive behind the WiMAX is to replace the Cable and DSL. WiMAX has grown and evolved rapidly in the recent years this can be easily validated from the number of times it is amended.

Wireless technologies are more vulnerable to security threats than the wired technology this also applies to the WiMAX as it is completely wireless technology. In WiMAX several different types of security attacks are possible, based on the impact and risk to the system, attack severity is contemplated some are considered as major while some are regarded as obscure. For WiMAX, the list of possible attacks are very long and it primarily includes ranging attack, power saving attack, handover attack, replay attack, mesh mode attack, multicast/broadcast attack, jamming attack, scrambling attack, interleaving attack, masquerading, eavesdropping, downgrading of performance, draining out of battery and computational resources, denial of service attack, distributed denial of service attack and man-in-the-middle attack. As WiMAX is facing so many daunting challenges, industry and academic institutions are working hard to emerge new approaches, new device and new security techniques to encounter the challenges from the malicious attackers. These efforts results in the security consequences such as encryption, authentication, vulnerability checking, filter design, antenna enhancement and other measures.

Industry and academic institutions mainly focuses on the vulnerability in the initial network entry and the ranging procedure. The main reason of susceptibility to attack in the initial network entry and ranging is the unencrypting behaviour of management message by taking advantage of this behaviour an attacker can launch a number of attacks which would damage the normal communication in WiMAX. As most of the contribution is given in the encryption area, only some researcher works in the jamming scope, leaving it completely untouchable. Based on the impact to the system, jamming is considered to be very intense attacks.

In this thesis, the main focus is to detect jamming in WiMAX based communication system and to recover the communication system from jamming.

1.4 Organization of Thesis

This section will briefly describe how the rest of the thesis is organized. The thesis analysed different aspects of WiMAX communication system with the main focus of security in WiMAX communication system. The rest of the thesis is organized as follows:

Chapter 2: A brief description of computer network, types of computer network, IEEE 802 standard, IEEE 802.16 standard and the evolution of IEEE 802.16 standard is described in chapter 2.

Chapter 3: This chapter is an overview of IEEE 802.16 Media Access Control (MAC) layer, Physical (PHY) layer and Security layer.

Chapter 4: This chapter is whole about the WiMAX, especially its architecture and its features.

Chapter 5: This chapter analyse the various security attacks at the Media Access Control (MAC) layer and the schemes to secure the Media Access Control (MAC) layer from such attacks.

Chapter 6: This chapter analyse the various security attacks at the Physical (PHY) layer and the schemes to secure the Physical (PHY) layer from such attacks.

Chapter 7: This chapter describes the algorithm for detection of jamming at Downlink and Uplink channel and how to recover from it.

Chapter 8: The theoretical methodology for jamming and recovery from jamming is described and explained in this chapter.

Chapter 9: This chapter demonstrate the simulation and analysis of result for the jamming attack in WiMAX.

Chapter 10: This chapter present the conclusion of the thesis.

1.5 Summary

This chapter presented an introduction of WiMAX and set the stage for more detailed explanation in subsequent chapters.

- WiMAX is a next upcoming generation technology.
- WiMAX is used to provide broadband access in rural areas.
- WiMAX is based on a very flexible and robust air interface defined by the IEEE 802.16 group.
- Security breach in WiMAX is a serious problem especially jamming.
- Method is to be developed to make the WiMAX secure from the jamming attack.

Chapter 2

Preliminaries and Background

2.1 Computer Network

A computer network is a group of interconnected computers in order to share resources, exchange files or allow electronic communication. The computers in a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beam [3].

2.2 Types of Computer Network

The computer network is broadly categories into four types:

1. ***Personal Area Network (PAN)*** – A Personal Area Network (PAN) is a data network used for communication among data devices close to one person. The scope of PAN is of the order of a few meters, generally assumed to be less than 10m [3, 4].
2. ***Local Area Network (LAN)*** – A Local Area Network (LAN) enables a user to establish data connections within a local area. It is used for communication among data devices such as computer, printer, personal digital assistants (PDAs) and etc. [3, 5].
3. ***Metropolitan Area Network (MAN)*** – A Metropolitan Area Network (MAN) is a data network that covers up to several kilometres. MANs can serve as backups for wired LAN [3, 6].
4. ***Wide Area Network (WAN)*** – A Wide Area Network (WAN) is a data network covering a wide geographical area. WANs are based on the connection of LANs, allowing users in one location to communicate with users in other locations [3, 7].

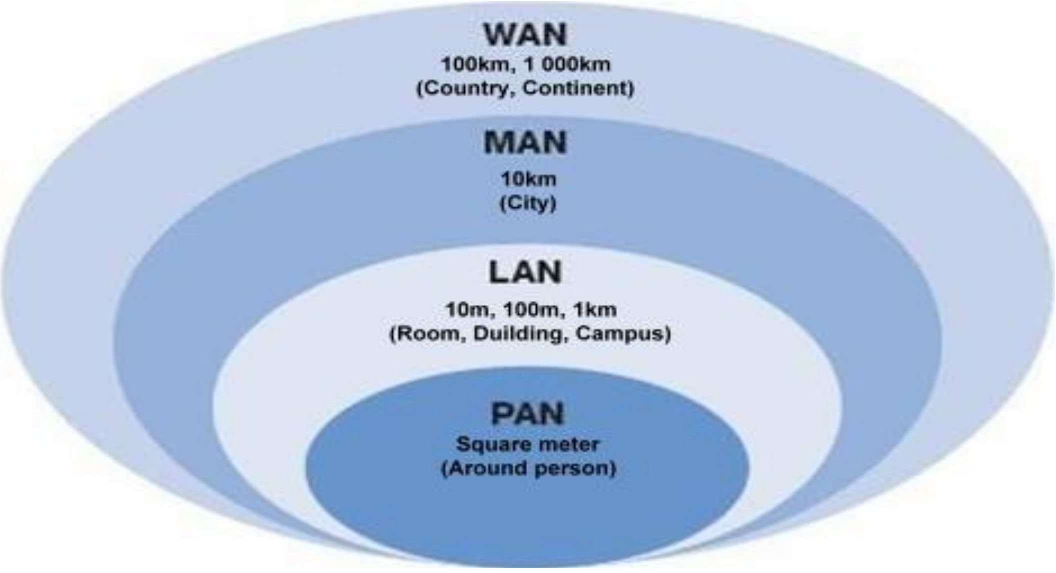


Figure 2.1: Types of Computer Networks

2.3 IEEE 802 Standards

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area network. The protocols and services specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model.

1. ***IEEE 802.1, Bridging and Network Management***

   IEEE 802.1 standard defines the 802 LAN/MAN architecture, link security, network management and internetworking among LANs, MANs and WANs [3].

2. ***IEEE 802.2, Logical Link Control (LLC)***

   IEEE 802.2 standard defines a Logical Link Control (LLC) sub-layer, which presents a uniform interface to the user of the data link service i.e. the network layer [3].

3. ***IEEE 802.3, Ethernet***

   IEEE 802.3 standard defines the physical layer and data link layer's media access control (MAC) of wired Ethernet. It defines the LAN access method using CSMA/CD [3].

4. ***IEEE 802.11, Wireless Local Access Network (WLAN)***

   IEEE 802.11 standard defines the Media Access Control (MAC) and Physical (PHY) layer specifications for implementing wireless local area network (WLAN) communication. IEEE 802.11 wireless network products are certified by Wi-Fi (Wireless Fidelity) consortium [3].

5. ***IEEE 802.15, Wireless Personal Access Network (WPAN)***

   IEEE 802.11 standard defines the Media Access Control (MAC) and Physical (PHY) layer specifications for wireless connectivity with fixed, portable and moving devices within or entering personal area network [3].

6. ***IEEE 802.16, Broadband Wireless Access (BWA)***

   IEEE 802.16 is a standard for broadband for wireless metropolitan area network. IEEE 802.16 wireless network products are certified by Worldwide Interoperability for Microwave Access (WiMAX) [3].

7. ***IEEE 802.20, Mobile Broadband Wireless Access (MBWA)***

   IEEE 802.20 standard is a packet-based air interface designed for Internet Protocol (IP) based services. It is mainly for high speed mobile devices and based on Flash Orthogonal Frequency Division Multiplexing (OFDM) [3].

8. ***IEEE 802.21, Media Independent Handover (MIH)***

   IEEE 802.21 standard defines the possibility of handover and interoperability between different wireless technologies or network type [3].

9. ***IEEE 802.22, Wireless Regional Area Network (WRAN)***

   IEEE 802.22 standard allow to access wireless broadband using cognitive radio and spectrum sharing in white space [3].

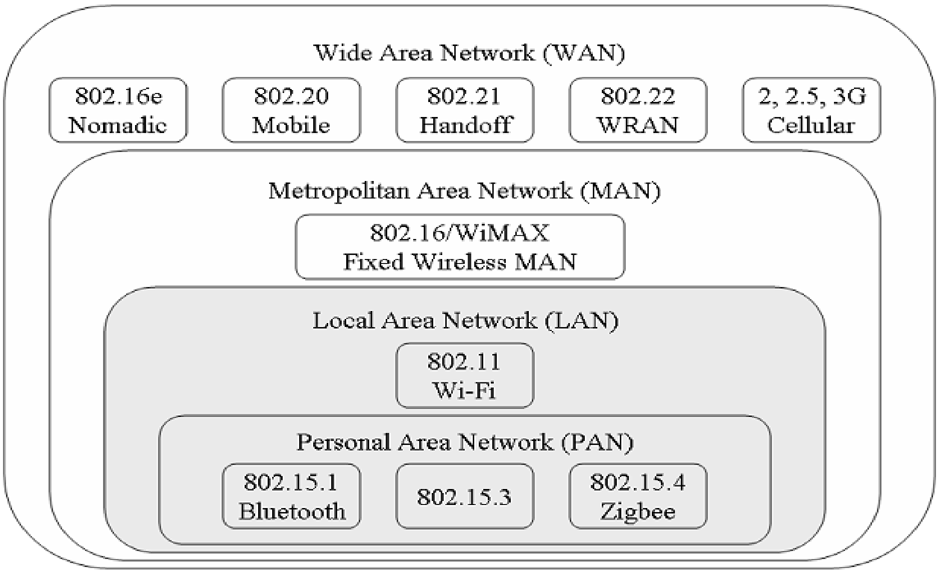


Figure 2.2: Family of IEEE 802 Standards

2.4 IEEE 802.16 Standard

IEEE 802.16 standard is developed to support the development and deployment of broadband Wireless Metropolitan Area Network (WMAN). It enables the deployment of innovative, cost-effective, interoperable multivendor broadband wireless access products and enlarging the competition in broadband access by providing alternatives to wired network such as Digital Subscriber Line (DSL) and cable modem This wireless access standard is capable of delivering megabits of data by supporting fixed, portable and mobile operation [1, 3].

The IEEE 802.16 standard covers the frequency bands between the range of 2 GHz and 66 GHz including both licenced and licenced exempt bands. It was designed in such a way that there are different PHY layer specifications dependent on the spectrum use and its associated regulation over a common MAC layer [3, 8].

2.5 IEEE 802.16 Reference Model

The IEEE 802.16 standard reference model is basically organized into two layers:

1. The Medium Access Control (MAC) Layer
2. The Physical (PHY) Layer

2.5.1 Medium Access Control (MAC) Layer

The MAC layer is composed of three sublayer and service access point (SAP):

1. ***Convergence Sublayer (CS)*** – CS is the layer that communicates with the higher layers to acquire network data into MAC Service Data Units (SDUs) [8].
2. ***Common Part Sublayer (CPS)*** – CPS basically provides the core MAC functionality and is responsible for the function such as bandwidth allocation, connection establishment and connection maintenance [8].
3. ***Security Sublayer*** – The security sub-layer provides the service such as authentication, authorization, encryption, key establishment, key distribution and key management [8].
4. ***Service Access Point (SAP)*** – Two types of service access point is defined in IEEE 802.16 standard: Management Service Access Point (M-SAP) and Control Service Access Point (C-SAP). Service Access Point (SAP) establishes communication between higher layer control and management entities.

   The C-SAP is defined for more time sensitive control plane primitives [2]:

   1. Service Flow Management.
   2. Radio Resource Management
   3. Subscriber Mode Management
   4. Handover Context Management
   5. Handovers Security Management
   6. Network Entry and Exit Management
   7. Media Independent Handover Management

   The M-SAP is defined for less time sensitive management plane primitives [2]:

   1. System Configuration
   2. Connections and Subscriber Accounting Management
   3. Notifications and Triggers Management
   4. Statistics Monitoring
   5. Subscriber Station Interface Management

The MAC layer has feature such as TDMA scheduled Uplink/Downlink frames, connection oriented, automatic retransmission request, support for adaptive modulation and automatic power control [2, 8].

2.5.2 Physical (PHY) Layer

The PHY layer includes multiple specification, each appropriate for a particular frequency range and application. The PHY layer supports both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) configurations. The PHY layer have features such as flexible channel widths, adaptive burst profiles, forward error correction, optional advanced antenna system, dynamic frequency selection and space time coding [2, 9].

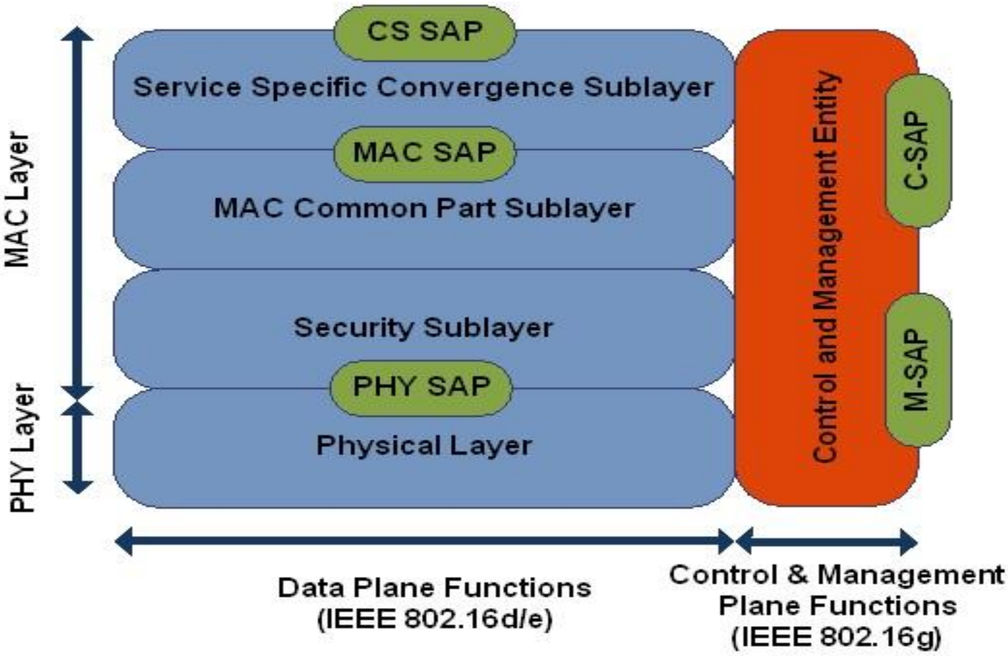


Figure 2.3: IEEE 802.16 Reference Model

2.6 Evolution of IEEE 802.16 Standard

IEEE 802.16 standard is a family of standards i.e. it is a collection of standards and not one interoperable standard. The IEEE 802.16 group was formed in 1998 to develop an air-interface standard for Broadband Wireless Access (BWA) and to support the development and deployment of wireless metropolitan area networks. The group released the first standard in December 2001. This standard was designed for 10 GHz – 66 GHz fixed frequencies that require line of sight (LOS) [10].

1. ***IEEE 802.16a***

   IEEE 802.16a standard is an amendment to the IEEE 802.16 standard, to include non-line of sight (NLOS) application in 2 – 11 GHz band instead of line of sight (LOS) 2 – 66 GHz. The IEEE 802.16a amendment to the standard opened up the opportunity for major changes to the PHY layer specifications to address the needs of the 2 – 11 GHz bands. This is achieved through the introduction of three new PHY layer specifications: Single Carrier PHY, 256 point FFT OFDM PHY and 2048 point FFT OFDMA PHY [10].

2. ***IEEE 802.16 – 2004***

   IEEE 802.16 – 2004 standard was the first practical standard of the IEEE 802.16 family and it is popularly called as fixed WiMAX. It specifies a standard for fixed access and the actual application supports nomadicity [10].

3. ***IEEE 802.16e***

   IEEE 802.16e standard is an amendment to the IEEE 802.16 – 2004 standard, in this standard support for mobility is added and it is often referred as mobile WiMAX. With this standard seamless handover and roaming are possible when users move from one place to another. This standard also added mutual authentication as part of the security [10].

4. ***IEEE 802.16 – 2009***

   IEEE 802.16 – 2009 standard is one of the major amendment to IEEE 802.16, it basically support the multi hop relay which added strength to the standard with the mobility feature [10].

5. ***IEEE 802.16 – 2012***

   IEEE 802.16 – 2012 standard is an revision version of IEEE 802.16 – 2009 standard, it is also known as Mobile WiMAX Release 2 as it supports the data rate as high as 100Mbps for mobile station and 1Gbps for fixed stations. The main aim of IEEE 802.16m – 2011 standard is to fulfil the ITU-R IMT-Advanced requirements on 4G systems [2].

6. ***IEEE 802.16 – 2013***

   IEEE 802.16 – 2013 standard is the current version of IEEE 802.16 standard. In IEEE 802.16 – 2013 standard, a new version of Privacy Key Management (PKMv3) is defined and also an enhanced mechanism for higher reliability networks is specified [11].

2.7 Summary

In this chapter, we attempt to understand computer network, IEEE 802 family of standard and IEEE 802.16 standard.

- Computer network are of four types: PAN, LAN, MAN and WAN.
- For every network type one standard is defined.
- IEEE 802.15 standard is defined for WPAN, WLAN is based on IEEE 802.11 standard and for MAN we have IEEE 802.16 standard.
- IEEE 802.16 standard supports line of sight (LOS) and non-line of sight (NLOS) type of communication in the frequency band of 2-66GHz range.
- The IEEE 802.16 standard is defined around Physical (PHY) and Media Access Control (MAC) layer and it is amended from time to time after its first release in 2001.

Chapter 3
Overview of IEEE 802.16 Layers

3.1 IEEE 802.16 Media Access Control (MAC) Layer

The primary task of IEEE 802.16 Media Access Control (MAC) layer is to provide an interface between the transport layer and the physical layer for controlling the access to the wireless medium. Operations defined in IEEE 802.16 MAC include network entry and initiation, PHY maintenance, Quality of Service (QoS), service flow, security, Automatic Repeat Request (ARQ) and Hybrid Automatic Repeat Request (HARQ) [3, 8, 10].

3.1.1 Network Entry and Initiation

When a Subscriber Station (SS) enters a network, it starts the network entry and initiation process. With this process the Subscriber Station (SS) obtains all the parameters required in communication. The network entry and initiation process consists of six phases described as follows:

1. ***DL channel scanning and synchronization:*** A Base Station (BS) transmits Downlink Channel Descriptor (DCD) and Uplink Channel Descriptor (UCD) messages to define the characteristics of a Downlink (DL) channel and an Uplink (UL) channel. The Subscriber Station (SS) scans the possible channels of the operating DL frequency band until a valid DL frequency is found. From the received DCD and UCD messages, the Subscriber Station (SS) determines the DL and UL transmission parameter [3, 8, 10].
2. ***Initial ranging and registration:*** The ranging process acquires the correct timing offset and power adjustment for a Subscriber Station (SS). The Base Station (BS) allocates initial ranging intervals which consists of slots, the mobile station select slot randomly and send a ranging request (RNG-REQ). The Base Station (BS) reply with a ranging response (RNG-RSP) specifying the timing offset and power level for the Subscriber Station (SS). After exchanging the RNG-REQ and RNG-RSP messages, two management connections is established between the Base Station (BS) and the Subscriber Station (SS) which is identified by unique connection identification (CIDs). One connection is used to exchange short and time urgent MAC management messages while the other connection is used to exchange longer and more delay tolerant MAC management messages [3, 8, 10].

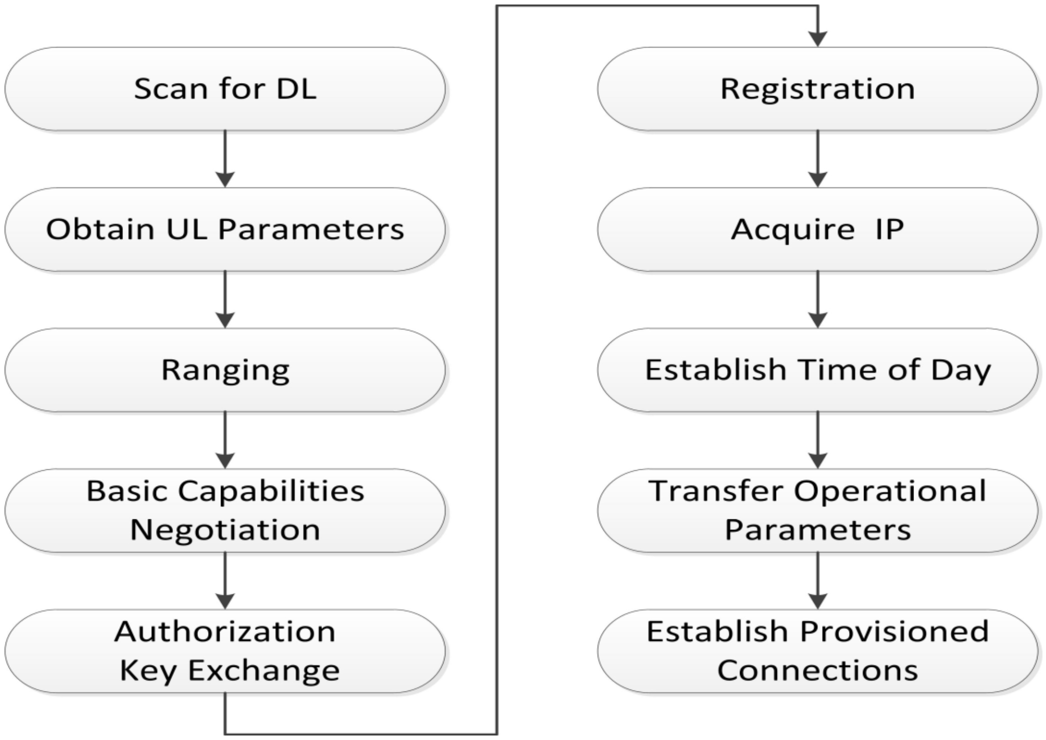

Scan for DL
Obtain UL Parameters
Ranging
Basic Capabilities Negotiation
Authorization Key Exchange
Registration
Acquire IP
Establish Time of Day
Transfer Operational Parameters
Establish Provisioned Connections

Figure 3.1: Initial Network Entry

3. ***Capability negotiation:*** A Subscriber Station (SS) inform the Base Station (BS) about its basic capabilities by sending the basic capability request (SBC-REQ), the Base Station (BS) respond using basic capability response (SBC-RSP) to the Subscriber Station (SS). The basic capability of Subscriber Station (SS) includes maximum transmit power, modulation schemes, Forward Error Correction (FEC) codes and bandwidth allocation scheme [3, 8, 10].
4. ***Authorization, Security Association (SA) Establishment and Key Exchange:*** A Subscriber Station (SS) after establishing the connection with the Base Station (BS) send the authentication information message for the authorization process which includes the Subscriber Station (SS) manufacturer's X.509 certificate. After this message an Authorization Request message is sent to the Base Station (BS), this message consist of (a) The manufacturer-issued X.509 certificate of the Subscriber Station (SS), (b) a description of the cryptographic capabilities of the Subscriber Station (SS) supports and (c) the Subscriber Station (SS) basic CID. In response to the above message, the Base Station (BS) validates the Subscriber Station (SS) identity, determine the encryption algorithm and create the authorization key (AK) [3, 8, 10].
5. ***IP Connectivity Establishment:*** Through the DHCP mechanism, a Subscriber Station (SS) obtains an IP address and other parameters to establish IP connectivity.

The Subscriber Station (SS) broadcasts a DHCP request, then the Base Station (BS) offer a list of DHCP server to the Subscriber Station (SS). After choosing the DHCP server, the Subscriber Station (SS) sends a DHCP request message to that server [3, 8, 10].

6. ***Dynamic Service Establishment:*** There are three types of dynamic service establishment: dynamic service addition (DSA), dynamic service change (DSC) and dynamic service deletion (DSD). Dynamic service establishment is exercised before any data delivery to activate the service flow [3, 8, 10].

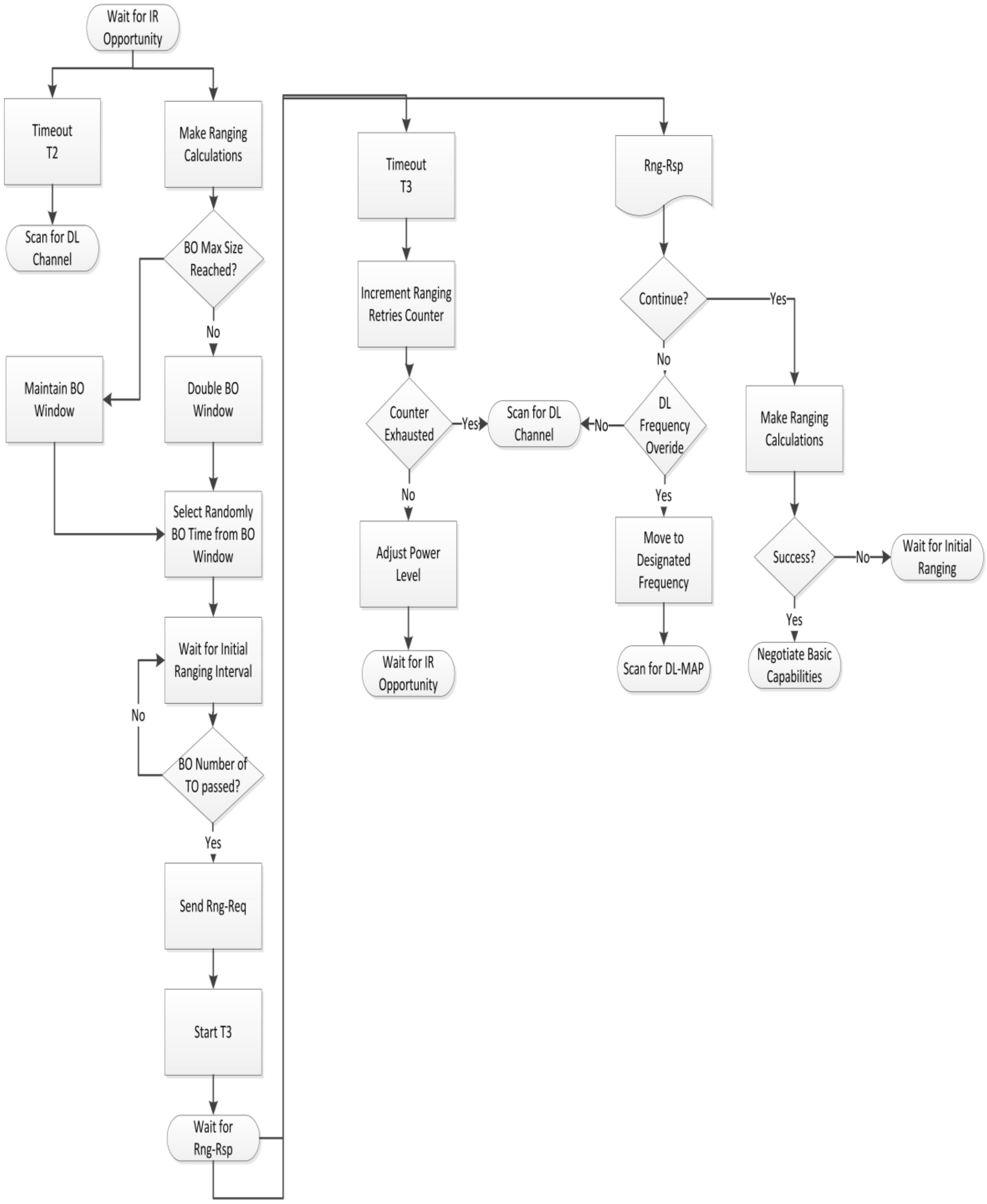


Figure 3.2: Flowchart of Initial Ranging Process

3.1.2 Automatic Repeat Request (ARQ)

Automatic Repeat Request (ARQ) [10] is a technique used for error control in data communication. It is a mechanism by which the receiver can request the retransmission of MAC PDU when received with error. In IEEE 802.16 standard, it is not mandate to use Automatic Repeat Request (ARQ), it is basically depend on the provider and the user to use this service. Automatic Repeat Request (ARQ) scheme support reliable delivery of data packet and consists of following module:

1. Error Detection
2. Feedback Policy
3. Retransmission Strategy
4. Retransmission Unit

3.1.3 Hybrid Automatic Repeat Request (HARQ)

Hybrid Automatic Repeat Request (HARQ) [10] is the enhancement of Automatic Repeat Request (ARQ), the main drawback of Automatic Repeat Request (ARQ) is the requirement of precise transmit power and data rate for the retransmissions. If this requirement is not fulfilled the link becomes underutilized or feels excessive packet errors. Hybrid Automatic Repeat Request (HARQ) is used to improve the robustness of data communication over the wireless channel. Like the Automatic Repeat Request (ARQ), Hybrid Automatic Repeat Request (HARQ) is also an optional feature of IEEE 802.16 Media Access Control (MAC) layer.

3.2 IEEE 802.16 Physical (PHY) Layer

The modulation and OFDM transmission aspects are the major building block of the IEEE 802.16 Physical layer. The IEEE 802.16 standard supports multiple physical layer specifications. IEEE 802.16 standard specifies four types of PHY layer specifications each provide interoperability. The four types of PHY layer specifications are:

1. ***WirelessMAN-OFDM*** – The WirelessMAN-OFDM uses the Orthogonal Frequency Division Multiplexing (OFDM) with a 256-point transform. This air interface is mandatory for license exempt bands and the access is done by using TDMA [2, 9].
2. ***WirelessMAN-OFDMA*** – The WirelessMAN-OFDM uses the Orthogonal Frequency Division Multiple Access (OFDMA) with a 2048-point transform. In WirelessMAN-OFDMA, multiple accesses are provided by addressing a subset of the multiple carriers to individual receivers [2, 9].

3. ***WirelessMAN-Single Carrier (SC)*** – The WirelessMAN-SC is intended for 10-66 GHz frequency band and designed for LOS channel. It does not support mobility but both TDD and FDD configuration are supported [2, 9].
4. ***WirelessMAN-SCa*** – The WirelessMAN-SC uses a single carrier modulation format and designed for NLOS channels. It supports spread BPSK, BPSK, QPSK, 16 – QAM, 64 – QAM and 256 – QAM modulation [2, 9].

3.2.1 Burst Profile

The burst profile is the basic building block of IEEE 802.16 standard; it is define as the set of parameters that define the Downlink and Uplink transmission properties associated with the interval usage code. Each burst profile consists of parameters such as modulation type, Forward Error Correction (FEC) type, preamble length, guard time and etc. [3, 10]

3.2.1.1 Downlink Burst Profile Parameters

Table 3.1: Downlink Burst Profile Parameters

Burst Profile Parameter	**Description**
Frequency	Downlink Frequency
FEC Code Type	Modulation and Coding Scheme; there are 20 MCSs in OFDM PHY and 34 MCSs in OFDMA PHY
DIUC Mandatory Exit Threshold	The CINR at or below where this burst profile can no longer be used and where a change to a more robust burst profile is required. Expressed in 0.25 dB units.
DIUC Minimum Entry Threshold	The minimum CINR required to start using this burst profile when changing from a more robust burst profile. Expressed in 0.25 dB units.
TCS_ enable (OFDM PHY only)	Enables or Disables TCS

3.2.1.2 Uplink Burst Profile Parameters

Table 3.2: Uplink Burst Profile Parameters

Burst Profile Parameter	**Description**
FEC Type and Modulation Type	There are 20 MCSs in OFDM PHY and 52 MCSs in OFDMA PHY
Focused Contention Power Boost	The Power Boost in dB of focused contention carriers
TCS_ enable	Enables or Disables TCS
Ranging Data Ratio	Reducing factor, in units of 1 dB, between the power used for this burst and the power used for CDMA ranging.

3.2.2 Duplexing Techniques

The physical layer of IEEE 802.16 standard supports two mode of duplexing:

1. Frequency Division Duplexing (FDD)
2. Time Division Duplexing (TDD)

Frequency Division Duplexing (FDD) – In FDD, the Downlink and Uplink channels are located on separate frequencies. For Downlink and Uplink transmission a fixed duration is used and is separated by the frequency offset. Frequency Division Duplexing (FDD) can be efficient in the case of symmetric traffic [3].

Time Division Duplexing (TDD) – Time Division Duplexing (TDD) is a communication technique allowing for two-way communication within the same frequency band by alternating the transmission times of a device. Time Division Duplexing (TDD) uses the same frequency for the Downlink and Uplink transmission but at different time [3].

3.3 IEEE 802.16 Security Sublayer

In IEEE 802.16, security has been considered as the main issue during the design of protocol but some issues still need to be solved on threats, risk and vulnerability in real situation.

3.3.1 Security Architecture for IEEE 802.16

The security sublayer has two main protocols as follows:

1. ***Encapsulation Protocol:*** An encapsulation protocol is used to secure packet across the fixed Broadband wireless access (BWA) network. Encapsulation protocol defines a set of cryptographic suites, i.e. pairing of data encryption and authentication algorithms and the rules for applying those algorithms to a MAC PDU payload [2, 3, 10].
2. ***Key Management Protocol (PKM):*** A key Management protocol (PKM) provides the secure mean for distributing the keying data from the Base Station (BS) to Subscriber Station (SS). The Base Station (BS) and the Subscriber Station (SS) synchronize the keying data using the key management protocol [2, 3, 10].

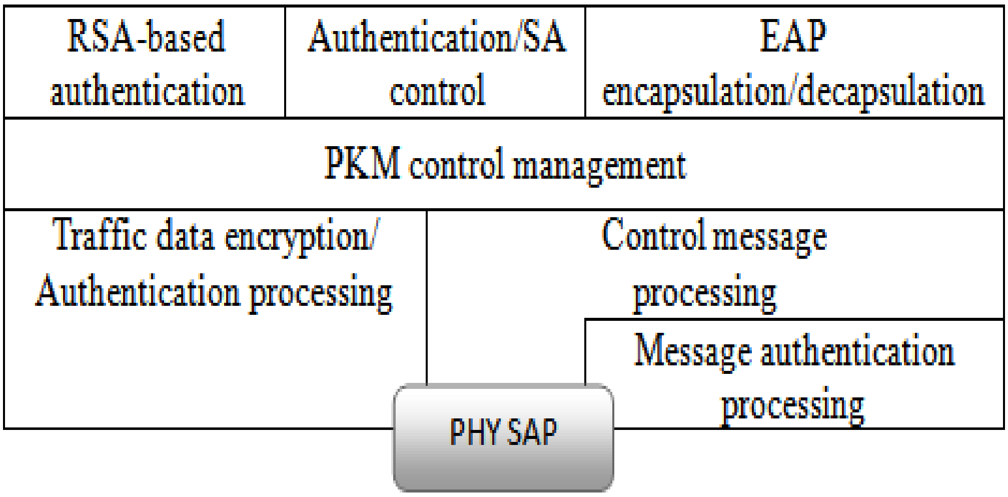

RSA-based authentication
Authentication/SA control
EAP encapsulation/decapsulation
PKM control management
Traffic data encryption/ Authentication processing
Control message processing
Message authentication processing
PHY SAP

Figure 3.3: Security Architecture

3.3.1.1 Key Management Protocol

Two version of Key Management Protocol (PKM) exists for providing security in IEEE 802.16: PKMv1 and PKMv2. The tasks of PKM protocol is broadly divided into three categories:

1**.** ***Authorization:*** It is the first step in PKM protocol, the main aim of this step is to authenticate the Base Station (BS) and the Subscriber Station (SS). The authorization process for the two versions is different, the difference lie in the message format that is exchange in this step.

In PKMv1, an authentication information message is sent from the Subscriber Station (SS) to the Base Station (BS), the message contain the Subscriber Station (SS) manufacturer's X.509 certificate. Authorization Request message is sent after the authentication information message from the Subscriber Station (SS) to Base Station (BS). This message consists of (a) The manufacturer-issued X.509 certificate of the Subscriber Station (SS), (b) a description of the cryptographic capabilities of the Subscriber Station (SS) supports and (c) the Subscriber Station (SS) basic CID. In response to the above message, the Base Station (BS) validates the Subscriber Station (SS) identity, determine the encryption algorithm and create the authorization key (AK) for the Subscriber Station (SS) and thus construct an Authorization Reply message.

It is clearly seen from the authentication process that the authentication in PKMv1 is one way i.e. the Base Station (BS) authenticate the Subscriber Station (SS) but the vice versa is not possible. This one way authentication result in vulnerability that becomes the cause of several attacks.

SS → BS: Authentication Information (*CertManufacturer*)
SS → BS: Authorization Request (*CertMS*, [Cryptographic Capabilities], Basic CID)
BS → SS: Authorization Reply (*Enc*(*AK*)*PK*, Sequence Number, Key Lifetime, [SAIDs])

Figure 3.4: Authorization Step of PKMv1 Protocol

The drop back of PKM first version is removed and a new version (PKMv2) is introduced. The authorization process is modified so that it support mutual authentication. The authorization process starts with the transmission of informative message followed by the Authorization Request message. The Authorization Request message includes: (a) The manufacturer's-issued X.509 certificate of the Subscriber Station (SS), (b) Description of the cryptographic algorithm supported by the Subscriber Station (SS), (c) Subscriber Station (SS) basic CID and (d) 64-bit random number generated by the Subscriber Station (SS). The Base Station (BS) responds with the Authorization Reply message, the Authorization Reply message includes: (a) The Base Station (BS) X.509 certificate, (b) the pre-PAK key, (c) a 4-bit PAK sequence number, (d) the PAK lifetime, (e) the identities, (f) 64-bit random number generated by Subscriber Station (SS), (g) 64-bit random number generated by the Base Station (BS) and (h) RSA signature over the entire message. Now the extra fields help in authenticating the Base Station (BS) thus the mutual authentication is achieved [2, 12].

SS → BS: Authentication Information (*CertManufacturer)*

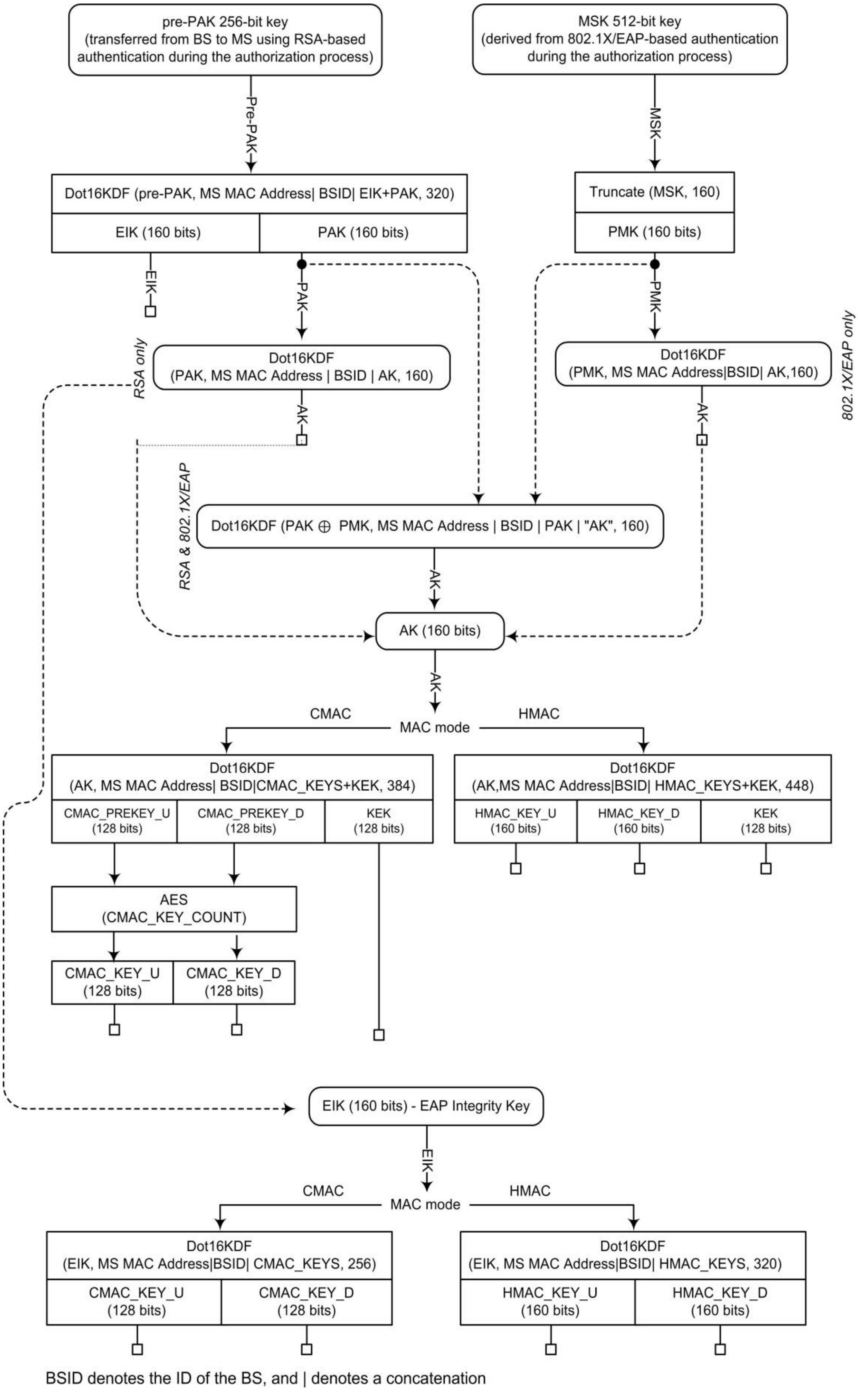
SS→BS: Authorization Request (*RadSS*, *CertSS*, [Cryptographic Capabilities], Basic CID, *SignatureSS*)

BS → SS: Authorization Reply (*CertBS*, *Enc*(*pre* − *PAK*)*PKSS*, Sequence Number, PAK Lifetime, [SAIDs], *RndSS*, *RndBS*, *SignatureBS*)

SS → BS: Authorization Acknowledgement (*RndBS*, Result Code, Error Code, Display String, *SignatureSS*)

Figure 3.5: Authorization Step of PKMv2 Protocol

2. ***Key Derivation:*** After the PKM authentication phase the Subscriber Station (SS) possess some keying material. The Subscriber Station (SS) derives the suitable keying material before the PKM protocol moves to another phase. In IEEE 802.16, the keys form a key hierarchy i.e. the higher level key is used to produce the lower level key. In PKMv2, the entire keys are created using the Dot16KDF function. The Dot16KDF function takes three arguments: (a) Keying material of a higher level, (b) String used to alter the output of the algorithm and (c) A number used to indicate the length of the generated key [2, 12].


pre-PAK 256-bit key
(transferred from BS to MS using RSA-based authentication during the authorization process)
MSK 512-bit key
(derived from 802.1X/EAP-based authentication during the authorization process)
Pre-PAK
MSK
Dot16KDF (pre-PAK, MS MAC Address| BSID| EIK+PAK, 320)
EIK (160 bits)
PAK (160 bits)
Truncate (MSK, 160)
PMK (160 bits)
EIK
PAK
PMK
RSA only
802.1X/EAP only
Dot16KDF
(PAK, MS MAC Address | BSID | AK, 160)
Dot16KDF
(PMK, MS MAC Address|BSID| AK,160)
AK
AK
RSA & 802.1X/EAP
Dot16KDF (PAK ⊕ PMK, MS MAC Address | BSID | PAK | "AK", 160)
AK
AK (160 bits)
AK
CMAC
MAC mode
HMAC
Dot16KDF
(AK, MS MAC Address| BSID|CMAC_KEYS+KEK, 384)
CMAC_PREKEY_U
(128 bits)
CMAC_PREKEY_D
(128 bits)
KEK
(128 bits)
Dot16KDF
(AK,MS MAC Address|BSID| HMAC_KEYS+KEK, 448)
HMAC_KEY_U
(160 bits)
HMAC_KEY_D
(160 bits)
KEK
(128 bits)
AES
(CMAC_KEY_COUNT)
CMAC_KEY_U
(128 bits)
CMAC_KEY_D
(128 bits)
EIK (160 bits) - EAP Integrity Key
EIK
CMAC
MAC mode
HMAC
Dot16KDF
(EIK, MS MAC Address|BSID| CMAC_KEYS, 256)
CMAC_KEY_U
(128 bits)
CMAC_KEY_D
(128 bits)
Dot16KDF
(EIK, MS MAC Address|BSID| HMAC_KEYS, 320)
HMAC_KEY_U
(160 bits)
HMAC_KEY_D
(160 bits)

BSID denotes the ID of the BS, and | denotes a concatenation

Figure 3.6: Message Exchange and Key Derivation

3**. *Handshake:*** The third phase is a three way handshake; the motive of this phase is to confirm that the Base Station (BS) and the Subscriber Station (SS) have the correct Authorization Key (AK) from the previous steps. The handshake phase also takes care of key activation, security association parameters negotiation, security parameter confirmation and etc. [2, 12].

BS → SS: PKMv2 SA-TEK-Challenge (*RndBS*, AK Sequence Number, AKID, Key Lifetime, HMAC/CMAC)
SS → BS: PKMv2 SA-TEK-Request (*RndBS*, *RndSS*, AK Sequence Number, AKID, Security Capabilities, Security Negotiation Parameters, HMAC/CMAC)
BS → SS: PKMv2 SA-TEK-Response (*RndBS*, *RndSS*, AK Sequence Number, AKID, SA TEK Update, Frame Number, SA-Descriptor, Security Negotiation Parameters, HMAC/CMAC)

Figure 3.7: Three Way Handshake of PKMv2 Protocol

4. ***TEK Transportation:*** Actually the TEK key is responsible for the encryption of traffic. The Base Station (BS) is solely in charge of creating the TEK key and thus it must transport securely to the Subscriber Station (SS). The two message pair PKM-REQ and PKM-REP is responsible for this purpose. The PKM-REQ message consist of the following fields: (a) Key Sequence Number, (b) the Identity of the Security Association whose TEK is requested, and (c) HMAC/CMAC digest over the entire PKM-REQ message payload. After checking the authenticity of the PKM-REQ message, the Base Station (BS) responds with a PKM-REP message. The PKM-REP message consist of the following fields: (a) Key Sequence Number, (b) SAID, (c) TEK-Parameters (Older), (d) TEK, Key Lifetime, (e) Key Sequence Number, (f) CBC-IV, (g) TEK-Parameters (Newer), (h) TEK, Key Lifetime, (i) Key Sequence Number, (j) CBC-IV, and (k) HMAC/CMAC digest over the entire message payload [2, 12].

5. ***Traffic Encryption:*** After the successful exchange of the TEK key between the Base Station (BS) and the Subscriber Station (SS), the Base Station (BS) and the Subscriber Station (SS) will be able to encrypt and decrypt the message [2, 12].

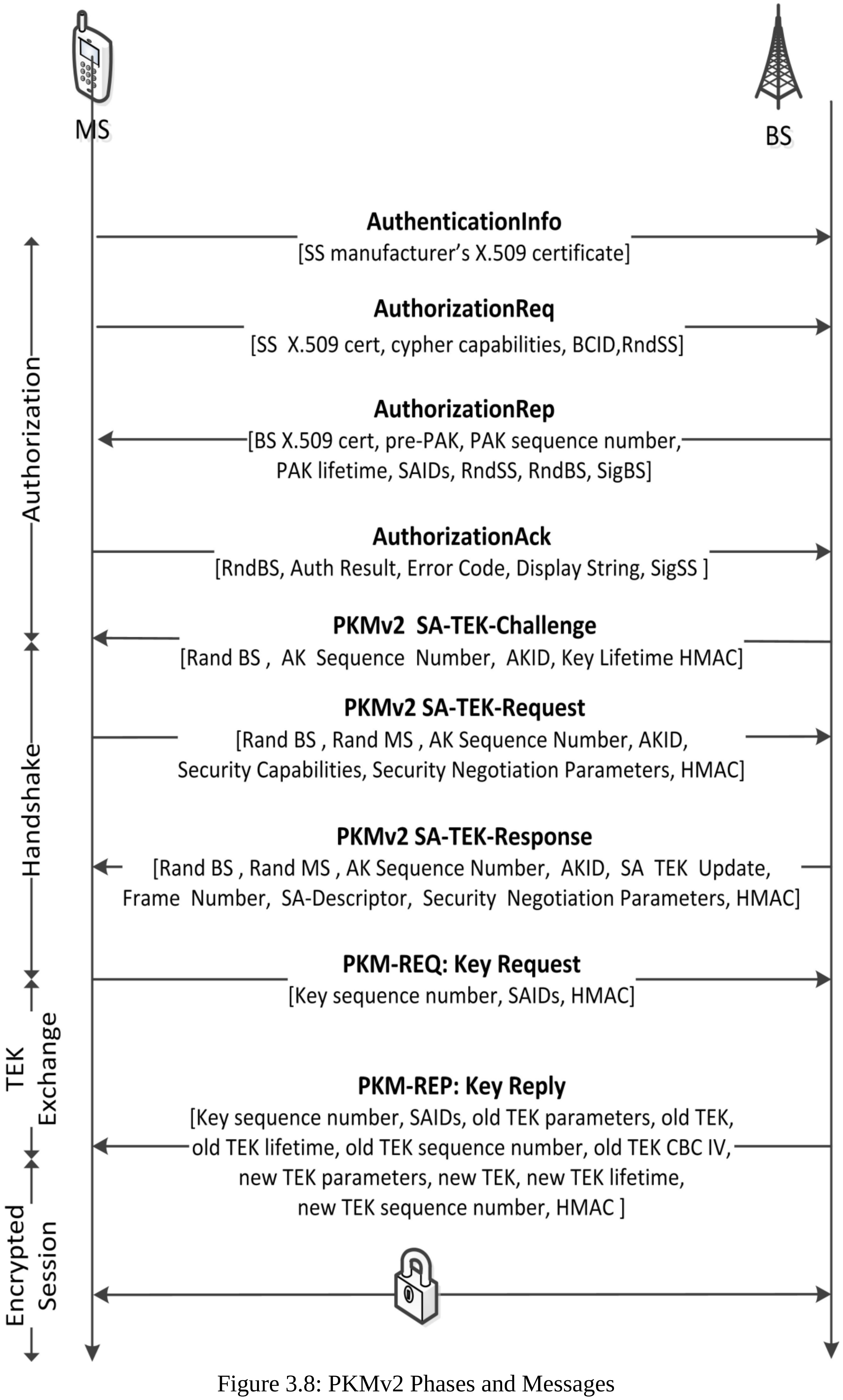

MS
BS
Authorization
Handshake
TEK Exchange
Encrypted Session
AuthenticationInfo
[SS manufacturer's X.509 certificate]
AuthorizationReq
[SS X.509 cert, cypher capabilities, BCID,RndSS]
AuthorizationRep
[BS X.509 cert, pre-PAK, PAK sequence number,
PAK lifetime, SAIDs, RndSS, RndBS, SigBS]
AuthorizationAck
[RndBS, Auth Result, Error Code, Display String, SigSS]
PKMv2 SA-TEK-Challenge
[Rand BS , AK Sequence Number, AKID, Key Lifetime HMAC]
PKMv2 SA-TEK-Request
[Rand BS , Rand MS , AK Sequence Number, AKID,
Security Capabilities, Security Negotiation Parameters, HMAC]
PKMv2 SA-TEK-Response
[Rand BS , Rand MS , AK Sequence Number, AKID, SA TEK Update,
Frame Number, SA-Descriptor, Security Negotiation Parameters, HMAC]
PKM-REQ: Key Request
[Key sequence number, SAIDs, HMAC]
PKM-REP: Key Reply
[Key sequence number, SAIDs, old TEK parameters, old TEK,
old TEK lifetime, old TEK sequence number, old TEK CBC IV,
new TEK parameters, new TEK, new TEK lifetime,
new TEK sequence number, HMAC]

Figure 3.8: PKMv2 Phases and Messages

3.4 Summary

This chapter described the Media Access Control (MAC), Physical (PHY) and Security layer of WiMAX. The detail provided is sufficient to comprehend the nature of the WiMAX Media Access Control (MAC), Physical (PHY) and Security layer, and understand the various aspects associated with the WiMAX layers.

- The WiMAX Media Access Control (MAC) layer has been designed from ground up to provide a flexible and powerful architecture that can efficiently support a variety of requirements.
- The WiMAX Physical (PHY) layer is based on OFDM, which is an elegant and effective technique for overcoming multipath distortion.
- The Physical (PHY) layer of WiMAX can adapt seamlessly, depending on the channel, available spectrum, and the application of the technology. Although the standard provides some guidance, the overall choice of various PHY-level parameters is left to the discretion of the system designer. It is very important for an equipment manufacturer and the service provider to understand the basic trade-off associated with the choice of these parameters.
- Robust security functions, such as strong encryption and mutual authentication, are built into the WiMAX standard.

Chapter 4

Introduction To WiMAX

4.1 WiMAX

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. It is based on wireless metropolitan area networking (WMAN) standard developed by the IEEE 802.16 group and adopted by both IEEE and the ETSI HIPERMAN group. The original idea of WiMAX is to provide users in rural areas with high speed communications as an alternative of cable and DSL for last mile broadband access. WiMAX supports low latency applications such as data, Voice over Internet Protocol (VoIP) and IPTV service, provides backhaul for 801.11 hotspots [10, 12].

4.2 Architecture of WiMAX

WiMAX architecture comprises of several components but the basic two components are BS and SS. Other components are MS, ASN, CSN and CSN-GW etc.

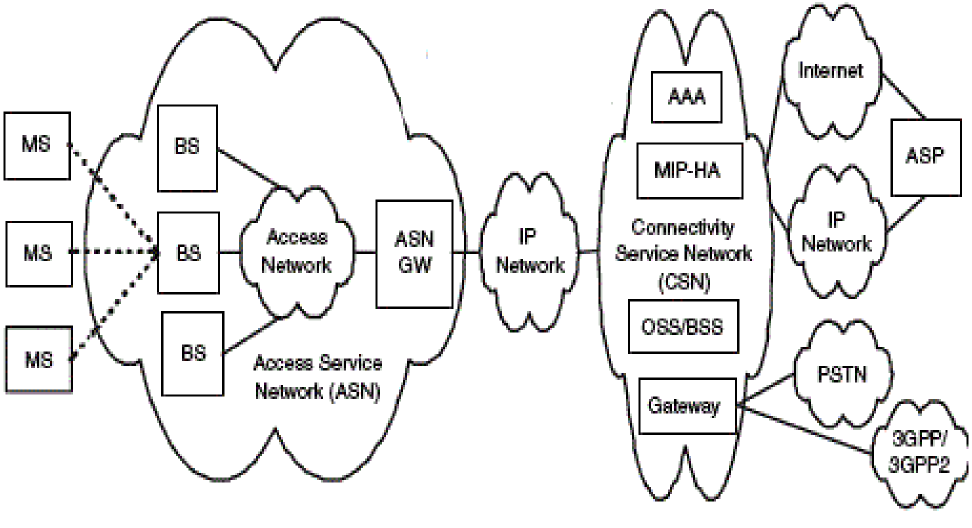


Figure 4.1: WiMAX Architecture

The components are defined as:

1. ***Base Station (BS):*** The Base Station (BS) is responsible for providing services to the Subscriber Station (SS). The other functions of the Base Station (BS) includes management functions such as handoff and tunnel establishment, radio resource management, providing Quality of Service (QoS), key management, session management, and multicast group management [2, 3, 8].

2. ***Mobile Station (MS):*** The Mobile Station (MS) is the end user who is receiving the services from the Base Station (BS). Mobile Station (MS) is a portable station able to move to wide areas and perform data and voice communication. It has the entire necessary user equipment's such as an antenna, amplifier, transmitter, receiver and software needed to perform the wireless communication [2, 3, 8].
3. ***Access Service Network (ASN):*** The Access Service Network (ASN) comprises one or more Base Stations (BSs) and one or more Access Service Network Gateways (ASN-GW) that form the radio access network. It provides all the access services with full mobility and efficient scalability [2, 3, 8].
4. ***Access Service Network Gateway (ASN-GW):*** The Access Service Network Gateway (ASN-GW) function includes intra-ASN location management, paging, radio resource management, admission control, caching of encryption keys and routing to the selected CSN. ASN-GW also controls the access in the network and coordinates between data and networking elements [2, 3, 8].
5. ***Connectivity Access Network (CAN):*** The Connectivity Access Network provides connectivity to the Internet, ASP, other public networks, and corporate networks. The connectivity access network functions includes authentication, IP address management, support for roaming between different network service providers, location management between access service networks and mobility and roaming between ASNs [2, 3, 8].

4.3 Features of WiMAX

1. ***Orthogonal Frequency Division Multiplexing (OFDM) Based Physical Layer:*** The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, OFDM offers good reluctance to multipath. It enables the WiMAX to operate in non-line of sight (NLOS).
2. ***Very High Peak Data Rates:*** WiMAX supports very high peak data rates, the data rates for mobile station is up to 100 Mbps and for fixed station it is up to 1 Gbps.
3. ***Scalable Bandwidth and Data Rate Support:*** WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth. The scalability is supported in the OFDMA mode, where the FFT (Fast Fourier Transform) size may be scaled based on the available channel bandwidth. The scaling is done dynamically to support user roaming across different networks.

4. ***Adaptive Modulation and Coding (AMC):*** WiMAX supports a number of modulations and Forward Error Correction (FEC) coding schemes and allows the scheme to be changed on per user and per frame basis, based on channel conditions.
5. ***Link-Layer Retransmissions:*** For connections that require enhanced reliability, WiMAX supports Automatic Repeat Requests (ARQ) at the link layer. Automatic Repeat Requests (ARQ) enabled connections require each transmitted packet to be acknowledged by the receiver. The unacknowledged packets are assumed to be lost and are retransmitted.
6. ***Support for Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD):*** IEEE 802.16 standards support Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD), as well as a half-duplex Frequency Division Duplexing (FDD) which allows for a low-cost system implementation. Time Division Duplexing (TDD) is favoured because of its following advantages:
    a. Flexibility in choosing Uplink-to-Downlink data rate ratios.
    b. Ability to exploit channel reciprocity.
    c. Ability to implement in non-paired spectrum.
    d. Less complex transceiver design.
7. ***Orthogonal Frequency Division Multiple Access (OFDMA):*** Mobile WiMAX uses OFDM as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones. OFDMA facilitates the exploitation of frequency diversity and multiuser diversity to significantly improve the system capacity.
8. ***Quality-Of-Service Support:*** The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services. The system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic [13].

4.4 Summary

This chapter has covered the WiMAX, its architecture and feature of WiMAX.

- WiMAX is based on the standard which is accepted by IEEE and ETSI HIPERMAN group.

- The main components of WiMAX architecture are Base Station (BS), Subscriber Station (SS), Mobile Station (MS), Access Service Network (ASN), Access Service Network Gateway (ASN-GW) and Connectivity Access Network (CAN) .
- WiMAX supports a number of advanced signal-processing techniques to improve overall system capacity. These techniques include adaptive modulation and coding, spatial multiplexing, and multiuser diversity.
- WiMAX has a very flexible MAC layer that can accommodate a variety of traffic types, including voice, video, and multimedia, and provide strong Quality of Service (QoS).
- WiMAX supports Automatic Repeat Request (ARQ) which helps in controlling error during communication.

Chapter 5

Security Analysis At Media Access Control (MAC) Layer

5.1 Security Attacks at Media Access Control (MAC) Layer

Security is an essential prerequisite for the success of every communication technology. Wireless communications are by nature more vulnerable to a number of different attacks such as man-in-the-middle, Denial of Service (DoS) and replay at the Media Access Control (MAC) layer.

5.2 Ranging Attack

Ranging is one of the main steps in initial network entry and the objective of ranging is to acquire correct timing and power offset between the Base Station (BS) and Subscriber Station (SS). The Base Station (BS) and Subscriber Station (SS) exchange ranging messages (RNG-REQ and RNG-RSP) to acquire the correct offset. An attacker may manipulate these ranging messages to affect the entire communication between the Base Station (BS) and the Subscriber Station (SS). The possible attacks during the ranging process are as follows:

1. ***RNG-RSP DoS Attack:*** In this attack, an attacker having a Base Station (BS) like equipment transmit RNG-RSP messages to a specific Subscriber Station (SS), the attacker forges an RNG-RSP message by setting the “Ranging Status” to “abort” which force the Subscriber Station (SS) to disconnect the connection from the network. Now if after some time the Subscriber Station (SS) attempt to reconnect to the Base Station (BS), the attacker again transmit bogus RNG-RSP message which leads to Denial of Service (DoS) [14, 15].
2. ***RNG-RSP Downgrading Attack:*** The RNG-RSP message can be manipulated in several manners by an attacker. The attacker simply alters the frequency field that result the Subscriber Station (SS) to operate on different channel. In this case, the Subscriber Station (SS) needs to rescan many frequencies until it finds the appropriate channel. The attacker may also alter the timing and power level. All this alteration leads to the downgrading of mobile station resources [16].
3. ***RNG-RSP Water Torture Attack:*** The modification to maximum value of power level adjust field in RNG-RSP message force the Subscriber Station (SS) to operate

on higher energy level thus making the drain of battery resources of Subscriber Station (SS) [16].

4. ***RNG-REQ Downgrading Attack:*** The RNG-REQ message can also be modified by the attacker. The attacker may change the optimal burst profile with the worst burst profile which results in downgrading the service of the Base Station (BS) [15, 16].

5.3 Power Saving Attack

The IEEE 802.16 standard supports the mobility, so it is important for the standard to include power saving features in order to extend the life of Subscriber Station (SS) battery. Subscriber Station (SS) can achieve power saving by functioning in sleep or idle mode. The state in which the Subscriber Station (SS) turns off various functions for a pre-negotiated time is known as Sleep mode. Sleep mode is characterised between the interval of unavailability and availability. During the sleep mode the Base Station (BS) shall not transmit any data to the Subscriber Station (SS), only in the availability interval the Subscriber Station (SS) receive data from the Base Station (BS). The sleep mode can be initiated by Subscriber Station (SS) or Base Station (BS) depending on the power saving class. MOB_SLP_REQ and MOB_SLP_RSP messages are used for power saving. The Subscriber Station (SS) initiates the sleeping mode by sending MOB_SLP_RSP message while the Base Station (BS) responds with a MOB_SLP_RSP message. The Base Station (BS) may transmit a MOB_TRF-IND message with a negative value for the availability interval which results in repetition of sleeping mode. The MOB_TRF-TND message with positive value from the Base Station (BS) indicates the termination of active state of power saving class. The idle mode is similar to power saving mode, the idle mode deals with the situation where an inactive Subscriber Station (SS) traverses a large geographic area. The concept of paging group is used when a Subscriber Station (SS) is in idle mode. Paging group is a set of Base Station (BS) that maintain the same list of Subscriber Station (SS) that are in idle mode, this eliminate the registration phase at a specific Base Station (BS) [12, 17].

1. ***Signalling DoS Attack:*** In this attack, an attacker generate negligible amount of traffic in the network for example TCP/IP packet having empty payload. The attacker sends these types of packets to several sleeping mobile station. On getting data for any Subscriber Station (SS), the Base Station (BS) shall have to wake up the Subscriber Station (SS). The Subscriber Station (SS) fall back into sleeping

mode after the inactivity timeout, by retransmitting such packet again and again the Subscriber Station (SS) get into the trap of an attacker and repeat the process of waking up and going back into sleep mode which results in great signalling load [17].

2. ***MOB_TRF-IND Water Torture Attack:*** The unauthenticated nature of MOB_TRF-IND messages may help the attacker to forge a valid MOB_TRF-IND message. The attacker frequently transmits the forged message to a sleeping Subscriber Station (SS) so that the energy resource of Subscriber Station (SS) is draining out soon [18].

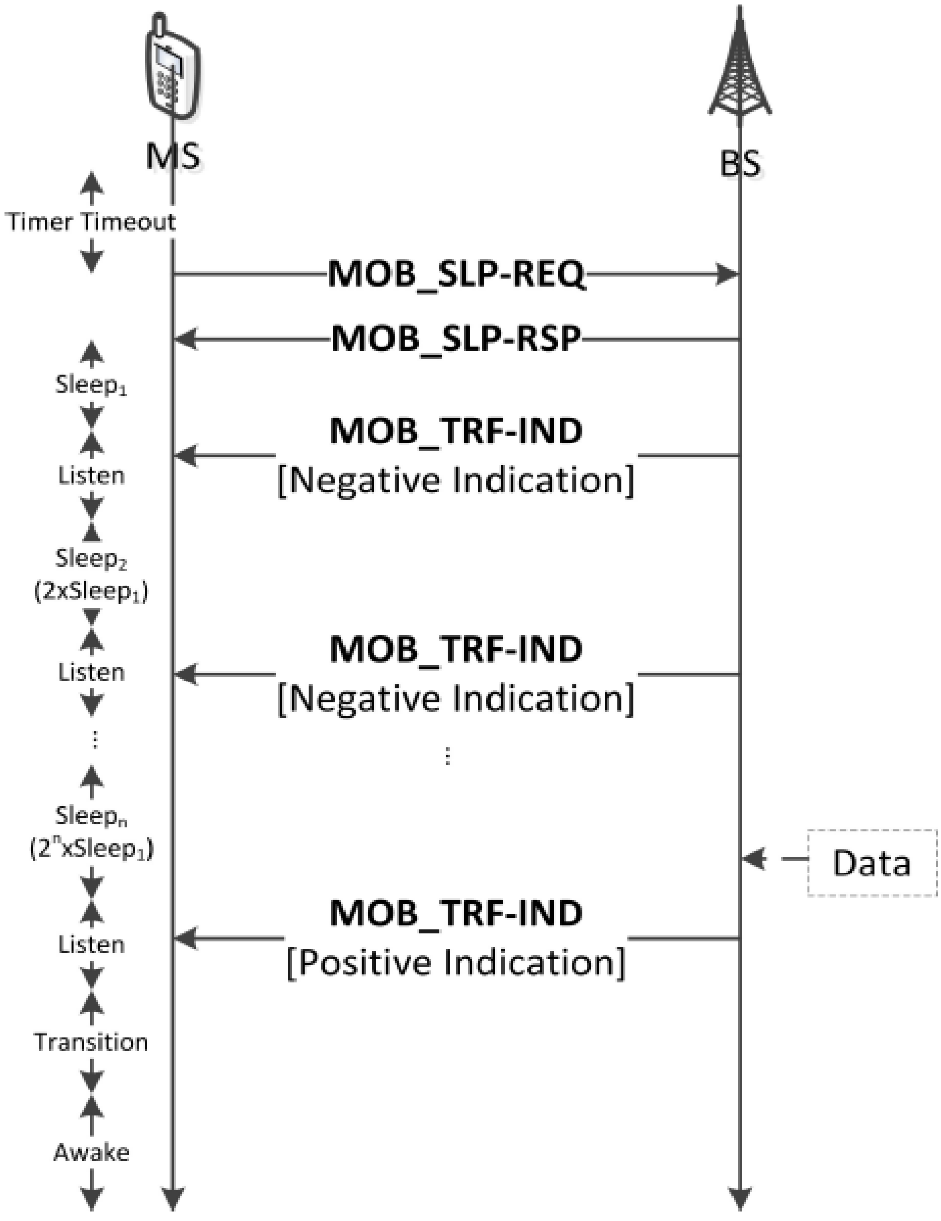


Figure 5.1: Subscriber Station (SS) Sleep Mode

5.4 Handover Attack

Handover is a multi-step process in which a mobile station is moved from its current Base Station (BS) to some other neighbour Base Station (BS). Handover is of two types: Soft Handover and Hard Handover. In soft handover the connection between the old Base Station (BS) and the Subscriber Station (SS) is terminated after the establishment of connection with the new Base Station (BS), while in hard handover first the connection between the old Base Station (BS) and the Subscriber Station (SS) is terminated and then a new connection is established. Handover process comprised of the following steps:

1. ***Cell Reselection:*** The Base Station (BS) periodically transmits a MOB_NBR-ADV message containing relevant information required by the Subscriber Station (SS). The Subscriber Station (SS) which want to perform handover identify all the neighbouring Base Station (BS) as candidate and choose any Base Station (BS) accordingly.
2. ***Handover Initiation:*** The handover process can be initiated either by the Subscriber Station (SS) or by the serving Base Station (BS). MOB_MSHO-REQ and MOB_BSHO-REQ messages are used to perform handover process these message proclaim the intention for handover.
3. ***Synchronization to New Base Station (BS):*** The Subscriber Station (SS) has to synchronize with the new Base Station (BS) and have to acquire the Downlink and Uplink parameter.
4. ***Ranging:*** Depending upon the information the new Base Station (BS) has about the Subscriber Station (SS) either the full initial network entry or handover ranging is performed.
5. ***Termination of Subscriber Station Context:*** The old Base Station (BS) shall terminate all the contexts regarding the Subscriber Station (SS) such as information in queues, counters, timers, header information [12, 18].

The following attack is possible during handover process:

1. ***MOB_NBR-ADV Downgrading Attack:*** As the MOB_NBR-ADV messages are not integrity protected. The attacker may change the message by removing information about neighbour Base Station (BS) from the appropriate fields which prevents the handover process and the Subscriber Station (SS) will believe that it is inaccessible. The Subscriber Station (SS) will have no option rather than to attach

with the serving Base Station (BS) and continue with the poor Quality of Service (QoS) [18].

2. ***MOB_NBR-ADV DoS Attack:*** In this attack, the attacker notifies the presence of a non-existing Base Station (BS) with better characteristics than the serving Base Station (BS). The Subscriber Station (SS) will detach from the serving Base Station (BS) and fall into the trap of the attacker as the new Base Station (BS) does not exist and thus the Subscriber Station (SS) is held back from the associated service [12, 16].

5.5 Interleaving Attack

Interleaving attack consists of two round in the first round the attacker imitate as a authenticated Subscriber Station (SS) and sends an authentication informative message followed by an authorization Request message which is grabbed from the previous session. The Base Station (BS) respond to this message with the Authorization Reply message, now the attacker has complete the authorization protocol by sending valid Authorization Acknowledgement response but the attacker cannot do so as it does not know the private key of the Subscriber Station (SS) which help in decrypting the Authorization Reply message. However the attacker perform both the round concurrently, in the second round the attacker act as a Base Station (BS) and force the Subscriber Station (SS) to initiate another protocol instance using the Authorization Reply of the first round. The legitimate Subscriber Station (SS) will provide the exact Authorization Acknowledgement message which the attacker transfers to the legitimate Base Station (BS) and finish the first round. So in this way the attacker behave as a Man-in-the-Middle entity and authenticate itself rather than the legitimate Subscriber Station (SS) and dodge the system into registering the wrong user [19, 20].

5.6 Multicast and Broadcast Attack

Multicast and Broadcast services is first introduce in the 802.16e specification, it allows the proclamation of data across multiple Subscriber Station (SS) of the network from a single centralized server. The key feature of multicast and broadcast service lies in its communication, multicast and broadcast service allow unidirectional type of communication in Downlink i.e. the Base Station (BS) can transmit message concurrently to all the members of the same group. To encrypt the message in the communication, a key is needed which is known as Group KEK (GKEK). GKEK is generated by the Base Station (BS) randomly and transmitted to all the Subscriber

Station (SS) of the same multicast/broadcast group, this key is encrypted by the KEK. The GKEK is used to encrypt the GTEKs which are sent by the Base Station (BS) to the Subscriber Station (SS) of same multicast/broadcast group. GTEK is issued by the Base Station (BS) when a Subscriber Station (SS) requested it by sending PKMv2 Key Request message and it acquire the key from the PKMv2 Key Reply message. A Base Station (BS) may update or assign keying material in predefined time intervals by sending two PKMv2 Group Key Update Command messages to all the members of the group. The two types of PKMv2 Group Key Update Command message are: GKEK Update Mode and GTEK Update Mode [12, 21, 22].

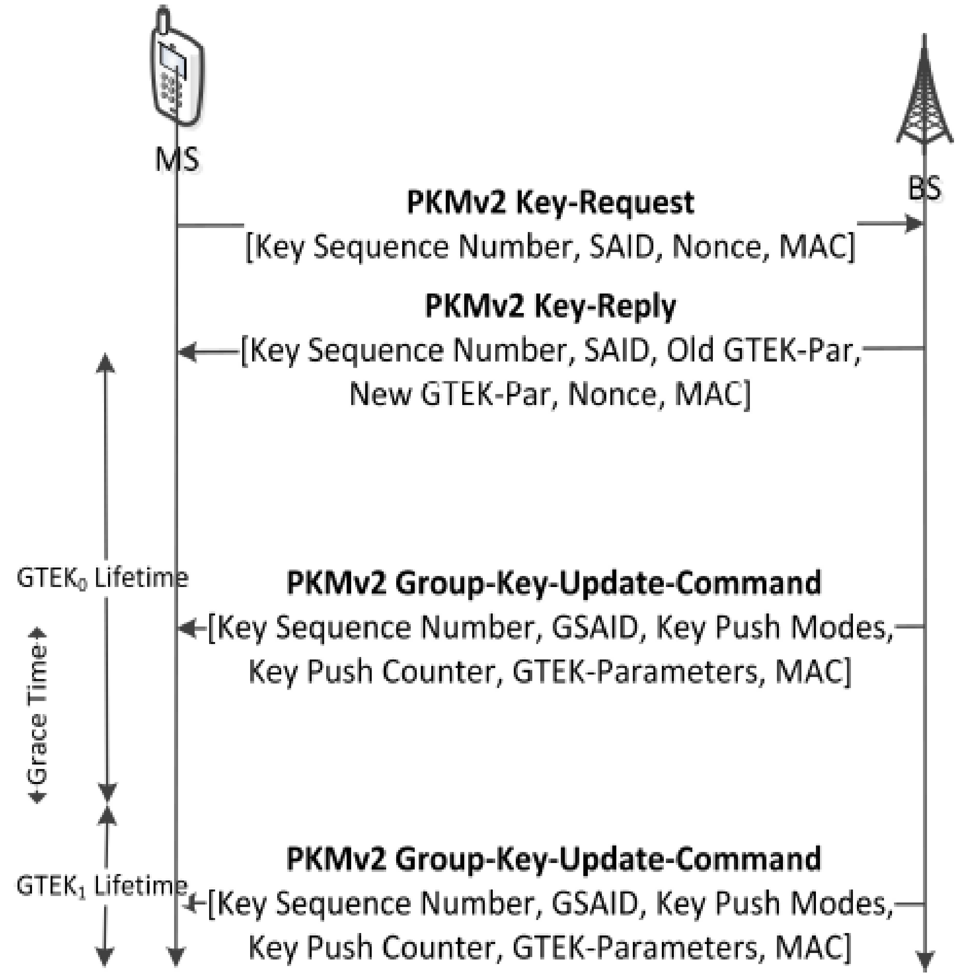

MS
BS
PKMv2 Key-Request
[Key Sequence Number, SAID, Nonce, MAC]
PKMv2 Key-Reply
[Key Sequence Number, SAID, Old GTEK-Par,
New GTEK-Par, Nonce, MAC]
GTEK$_0$ Lifetime
PKMv2 Group-Key-Update-Command
[Key Sequence Number, GSAID, Key Push Modes,
Key Push Counter, GTEK-Parameters, MAC]
Grace Time
GTEK$_1$ Lifetime
PKMv2 Group-Key-Update-Command
[Key Sequence Number, GSAID, Key Push Modes,
Key Push Counter, GTEK-Parameters, MAC]

Figure 5.2: Multicast and Broadcast Messages

1. ***Group Key Update Command:*** GTEK Update Mode DoS Attack: All the member of the multicast/broadcast group shared the same GTEK which is used to decrypt the message that is receive from the Base Station (BS). Since GTEK is a symmetric key one can encrypt or decrypt the message. Any adversary Subscriber Station (SS)

from the group can use this scope and can send an encrypted message within the group, the other group member will be able to decrypt the message but cannot identify that the message is coming from the legitimate Base Station (BS) or from any adversary Subscriber Station (SS). Another scenario can be understand when an adversary Subscriber Station (SS) from the group transmit fake GTEK encrypted with GKEK, upon getting the fake GTEK the entire group member replace their current keys. This makes the group member incapable of decrypting the incoming message except the attacker from the valid Base Station (BS) [21].

2. ***GTEK Theft of Service Attack:*** A current GTEK is given to a new member when it join the multicast/broadcast group which help him in decrypting the current traffic, but the new member can also use this key in decrypting the old traffic. Therefore the attacker may passively intercept the traffic and join the group as a legitimate member at the end of GTEK lifetime and decrypt the entire traffic [21, 22].

5.7 Mesh Mode Attack

Mesh mode is one of the prominent features of IEEE 802.16e – 2005, in mesh mode the traffic can be routed through other Subscriber Station (SS) rather than the sole Base Station (BS) and Subscriber Station (SS). Mesh mode provides the means for operations such as access control and authentication, so a centralized Base Station (BS) is needed to perform these tasks. If the Base Station (BS) is not directly accessible by any Subscriber Station (SS) present in the group that require authentication, then this Subscriber Station (SS) use the existing members of the group to reach the Base Station (BS). Now if a new Subscriber Station (SS) enters in a mesh network, it select one node that act as intermediate node between the Base Station (BS) and this new node and facilitates the authentication process. This intermediate node is known as sponsor node [12, 23].

1. ***Malicious Sponsor Node Attack:*** It is assumed that the sponsor node is loyal this creates a great risk, as a sponsor node is responsible for exchanging messages between the Base Station (BS) and the new node. A malicious sponsor node can easily forged the field in the PKM-REQ message which results in security Rollback attack, DoS attack and draining energy resource faster [23].
2. ***PKM-RSP Replay Attack:*** The authorization process between the Base Station (BS) and the new node is unilateral, which means that the Base Station (BS) authenticate

the new node but the opposite is not feasible Attacker can forge or replay PKM-RSP messages and act as a authentication centre or Base Station (BS) [24].

5.8 Security Against Media Access Control (MAC) Layer Threats

Many solutions have been proposed to remedy the vulnerabilities in WiMAX. Broadly the vulnerabilities in WiMAX can be broadly classified into three categories:

1. Securing Initial Network Entry
2. Improving Privacy Key Management Protocol
3. Enhancing Multicast and Broadcast Service
4. Enhancing Security for Mesh Mode

5.8.1 Securing Initial Network Entry

Initial Network Entry is the main part of WiMAX communication and securing initial network entry is very crucial. Many solutions have been proposed to secure initial network entry. The main reason of Denial of Service (DoS) attack is the unprotected behaviour of management message. The basic solution to this problem is the utilization of Diffie-Hellman (DH) key exchange algorithm for the unprotected/unencrypted management message of initial network entry. The Diffie Hellman algorithm is very secure because of its public/private key pair. The generation of public/private key pair involves the parameters like Basic CID (BCID) and initial ranging codes. These parameters ensure that the Base Station (BS) and Subscriber Station (SS) choose the right keys [16].

A new protocol has been developed by making changes in the Diffie-Hellman protocol, this new protocol is known as Secure Initial Network Entry Protocol (SINEP). In this protocol two variables (*p* a large prime number and *q* a primitive roots of *p*) are shared among Base Station (BS) and Subscriber Station (SS), when this challenge-response sequence is applied to the initial network entry process, it is able to provide security against DoS and Man-in-the-Middle attacks [14].

MS → BS: request

MS → BS: *H* (*H* (*IDSS*), *nonceBS*, *PKSS*), *PKSS*, *nonceSS*

BS → MS: *H* (*H* (*IDSS*), *nonceSS*, *PKBS*), *PKBS*)

Figure 5.3: SINEP Protocol

RObust and Secure MobilE WiMAX (ROSMEX) is another protocol that is developed by modifying the Diffie-Hellman. ROSMEX eliminates vulnerability from three process i.e. vulnerability from initial network entry, vulnerability from access network and vulnerability from handover is removed us ROSMEX. For eliminating vulnerabilities from initial network entry a modification in Diffie-Hellman is accomplished, the modification lies in a ranging process. One of the ranging codes is used as a prime number seed then a hash authentication is applied to the exchanging process for protecting man-in-the-middle attack. This can also protect SBC security parameters and PKM security contexts using the shared traffic encryption key (pre-TEK) during initial network entry process. For eliminating vulnerabilities in access network a key exchange method using a device-certificate is used. As every network devices in the Mobile WiMAX has a device certificate which can be used to make robust access to network domain based on PKI structure. In order to applying device certificate based approach to access network domain it is assumed that Mobile WiMAX devices are certified from public authority and they can verify certificates of each other using certificate chain. If Base Station (BS) would like to exchange management or control messages with ASN/GW, Base Station (BS) needs to generate a session encryption key for secure communication between Base Station (BS) and ASN/GW. Base Station (BS) first searches for an appropriate certificate to verify ASN/GW's identity and obtain public key. After getting public key, Base Station (BS) generates "asn-TEK" as a session encryption key for secure communication with ASN/GW. Using the "asn-TEK" BS encrypts a message and sends the encrypted message together with the encrypted "asn-TEK" key using ASN/GW's public key, Timestamp, and Authority's certificate to ASN/GW. When ASN/GW receives the messages from Base Station (BS), ASN/GW first tries to verify the authority's certificate and checks the validation time from Timestamp. If the verification process is successful, ASN/GW decrypts the "asn-TEK" key and the original message. The problem of insecure communication between Base Station (BS) and ASN/GW can be eliminated by using "asn-TEK" key as an encryption key between Base Station (BS) and ASN/GW. In the case of ASN-to-CSN, the above scheme generates a common encryption key called "asn-csn-TEK" using the same method as a way for Base Station (BS)-to-ASN/GW to establish secure connection. For eliminating vulnerability in handover process a new handover approach with embedded mutual authentication parameters is adopted. This new handover approach includes a few additional fields for the embedded parameters of providing mutual authentication such as Nonce, Certificate (Cert), Authorization Key (AK), and Acknowledgement (Ack). The challenge-response scheme with Nonce, Cert, and AK is used to provide Target BS authentication. And HMAC/CMAC tuple is used for SS authentication as well as message authentication. This scheme enhances security and performance factors during handover without full authentication process based on PKMv2 [25].

5.8.2 Improving Privacy Key Management

Privacy Key Management (PKM) protocol is another segment of IEEE 802.16 standard where most of the attack is identified so additional security is required. The main idea is to enhance the authentication phase of PKM. To protect from replay attack and Man-in-the-Middle attack, the PKMv2 protocol is enhanced by using a timestamp and signature over the message, this enhanced protocol also have advantage of having less signalling overhead as compare to PKMv2 [19].

The authentication process of IEEE 802.16 can also be enhanced by using Elliptic Curve Cryptography (ECC). A Wireless Public Key Infrastructure (WPKI) framework is adopted which uses ECC rather than RSA in order to reduce the computational power. Another variation lies in the X.509 where any redundant information is striped off so that less memory is consumed thus this authentication protocol is lighter in computational and memory resources comparing to the existing one [26].

A combination of user EAP-TLS authentication and device authentication based on ECDH-RSA forms a new type of authentication mechanism known as EAP-TLS-ECDH-RSA. In the first step, EAP runs but to acquire keys for building a TLS tunnel ECDH-RSA is executed. As it is proven that RSA is slow in key generation while ECDH-RSA takes most of its time in verifying the certificate, the combination is expected to boost the performance of the system. [27]

Key exchange phase of the PKM is an important phase of the protocol, but some modification to it ensures a high degree of security. Authenticated Key Exchange (AKE2) protocol is the result of alteration in key exchange phase so that the mobile station and the Base Station (BS) will contribute in the generation of TEK. This protocol achieves the mutual control of the keys between the Base Station (BS) and the Subscriber Station (SS) [28].

A very different scheme is also developed to improve the PKM, in this scheme the entire PKM protocol is based on the concept of a Trusted Third Party (TTP) for its implementation. It has two phases, in the first phase both the mobile station and Base Station (BS) register with the Trusted Third Party (TTP) server and in the second phase the Subscriber Station (SS) and the Base Station (BS) exchange there certificates. After these steps the two entities precede with the exchange of the session keys [29].

5.8.3 Enhancing Multicast and Broadcast Service Security

It is very important to enhance the security of multicast and broadcast service since it is seen above that there are many flaws in multicast and broadcast service. The multicast and broadcast service can be improved by unicasting the GTEK to each Subscriber Station (SS) within a group, and the GTEK is encrypted by KEK instead of GKEK. This deals effectively with the insider attacks since an adversary Subscriber Station (SS) would require knowledge of the KEK [16].

***Initial Keying*:** Not Considered

***Key Update*:**

(1) **BS → SS:** (*GTEK*) *KEK*

***Rekeying at Join Event*:** Not Considered

***Rekeying at Leave Event*:** Not Considered

Figure 5.4: Multicast and Broadcast Protocol 1

The main security breach in multicast & broadcast service is the forward and backward secrecy, so to solve this problem it is important to enhance the security of MBRA. A similar approach as above is adopted but with some modification, the modification lies in the initial key distribution. Initially N unicasts occur to distribute the GTEK, plus one broadcast which act as a notification. In this approach there is a provision for joining and leaving the group. The key refresh is done using a single broadcast of a key update notification. The Subscriber Station (SS) can itself produce the new GTEK by simply passing the old GTEK through a predefined hash function [22].

***Initial Keying*:**

(1) **BS → SS:** (*GTEK*) *KEK*

(2) **BS → SS:** *Update Notice*

***Key Update*:**

(1) **BS → SS:** (*GTEK*) *KEK*

***Rekeying at Join Event*:**

(1) **BS ⇒ SS:** *Update Notice*

Rekeying at Leave Event

(1) **BS ⇒ SS:** *Update Notice*

Figure 5.5: Multicast and Broadcast Protocol 2

The concept of subgrouping in the multicast and broadcast group can also enhance the secrecy. Elapse is a modified version of MBRA which is based on subgrouping. According to this protocol, the multicast and broadcast group are further divided into larger subgroups. The number of subgroups and number of Subscriber Station (SS) in each group is decided by the administrator with respect to the requirement of the application. The member of the subgroup have the same GTEK, the Subscriber Station (SS) in the subgroup also maintain a chain of Sub Group Key Encryption Keys (SGKEKs) rather than a single GKEK. M (the number of subgroup) is the total number of keys that to be maintained by the Subscriber Station (SS) and a single broadcast message rather than N unicast plus 1 broadcast is used to refresh the key [30].

***Initial Keying*:** Not Considered

***Key Update*:**

(1) **BS ⇒ SSs:** (*GTEK*) *S GKEK*1234

***Rekeying at Join Event*:**

(1) **BS → SS:** (*SGKEK*1234, *SGKEK*12, *SGKEK*2) *KEK*

(2) **BS ⇒ *SSSG*3:** (*SGKEK*1234) *SGKEK*34

(3) **BS ⇒ *SSSG*4:** (*SGKEK*1234) *SGKEK*34

(4) **BS ⇒ *SSSG*1:** (*SGKEK*1234, *SGKEK*12) *SGKEK*1

Rekeying at Leave Event

(1) **BS → SS:** (*SGKEK*1234, *SGKEK*12, *SGKEK*2, *GTEK*) *KEK*

(2) **BS ⇒ *SSSG*3:** (*SGKEK*1234, *GTEK*) *SGKEK*34

(3) **BS ⇒ *SSSG*4:** (*SGKEK*1234, *GTEK*) *SGKEK*34

(4) **BS ⇒ *SSSG*1:** (*SGKEK*1234, *SGKEK*12, *GTEK*) *SGKEK*1

Figure 5.6: Multicast and Broadcast Protocol 3

5.8.4 Enhancing Security for Mesh Mode

The basic idea for enhancing the security of mesh mode is the use of certificates for authentication in link establishment of neighbouring nodes. A Mesh certificate issued by the authorization centre during authorization is used in link establishment [31].

5.9 Summary

This chapter explains the security attacks at Media Access Control (MAC) layer and also analyse the security measures to defy against the attacks.

- In WiMAX, the security threats at Media Access Control (MAC) layer are possible in the Initial Network Entry, Privacy Key Management Protocol, Multicast and Broadcast Service and last in the Mesh Network.
- In Initial Network Entry, the attacks are mainly happened because of unencrypted management and control messages.
- Ranging, Power Saving and Handover attacks are the major security attacks that are possible in Initial Network Entry.
- The weak nature of group key leads to the Multicast and Broadcast attacks.
- Malicious Sponsor Node attack is the most significant attack possible in Mesh Network.
- Security functions, such as strong encryption and mutual authentication are used to secure the WiMAX.

Chapter 6

Security Analysis At Physical (PHY) Layer

6.1 Security Attacks at Physical (PHY) Layer

In IEEE 802.16 standard, Privacy sublayer resides on the top of Physical layer. So WiMAX networks are vulnerable to Physical (PHY) layer attacks, such as jamming and scrambling. The main objective of the Privacy sublayer is to protect service providers against theft of service, rather than guarding network users. The privacy layer only guards data at the data link layer while it does not protect physical layer from being intercepted. It is necessary to include technologies to secure physical layer and higher layer security for a converged routable network.

6.1.1 Jamming Attack

Due to the development of highly sophisticated encryption techniques, the decryption of enemy's messages is getting practically impossible. Since recovering the message is no longer possible, the only practical option left is to make it impossible for the enemy parties to communicate.

Jamming can be defined as an activity of transmitting a radio signal with the intention of disrupting the normal operation of network. It occurs when a very high frequency radio signal is transmitted over a low frequency channel. It results in reducing the capacity of the channel, throughput degradation, unavailability of channel and alteration of packets [32, 33].

6.1.1.1 Types of Jamming

There are two types of jamming:

1. Noise Jamming
2. Multicarrier Jamming

6.1.1.1.1 Noise Jamming

Noise Jamming can be defined as the insertion of interference signal in normal communication so that the wanted signal is completely submerged by the interference.

$$\frac{B_J}{B_{CS}} = \frac{Jammer\ Bandwidth}{Communication\ System\ Bandwidth}$$

Based on the relationship between the jammer bandwidth and the communication system bandwidth, the noise jamming can be categorised into narrow and wideband jamming. If the ratio B_J/B_{CS} is less than 0.2, the jamming is considered as narrow or spots jamming while it is greater than 1 the jamming is wideband jamming [24, 34].

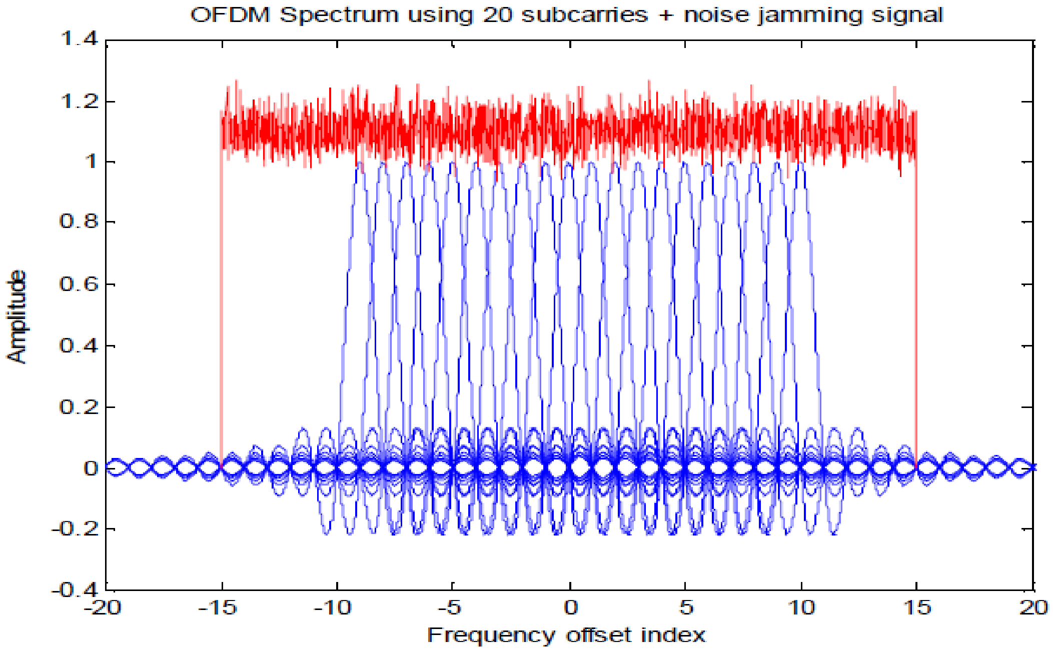


Figure 6.1: Noise Jamming

6.1.1.1.2 Multicarrier Jamming

In multicarrier jamming, the preselected carriers are jammed that have most effects on the overall performance of the system. The concept is to determine the most critical vulnerability of the system in terms of the carriers used and then inject a narrowband signal on those carriers [24, 34].

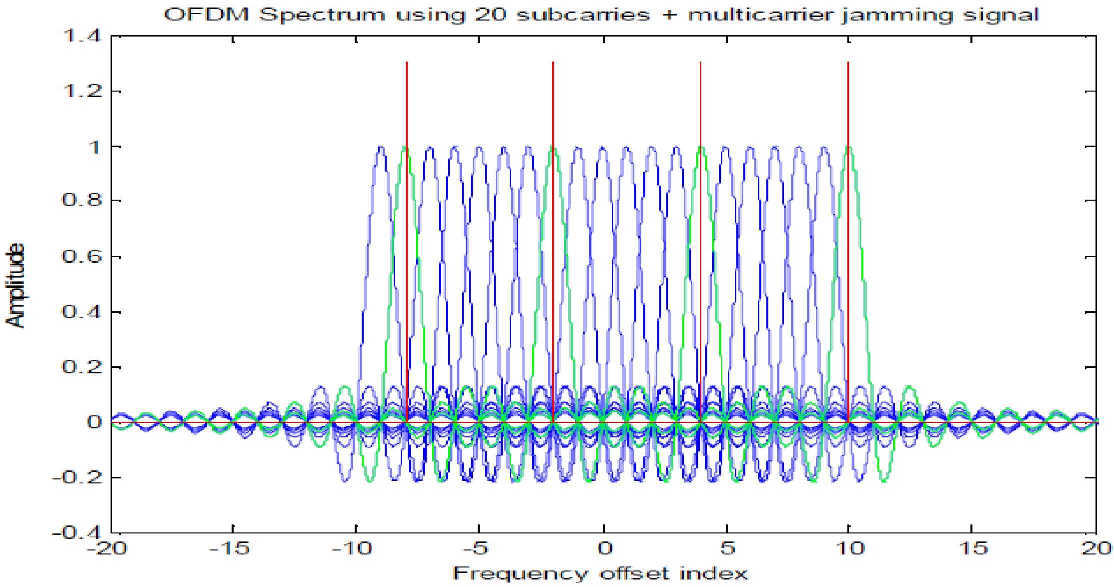


Figure 6.2: Multicarrier Jamming

In figure 6.2, a 20-carrier OFDM system with 4 pilot subcarriers is used. The multicarrier signal is inserted on the pilot subcarriers, these pilot subcarriers are critical vulnerability of the system.

6.1.1.2 Types of Jammer

There are several different attacks models that an adversary can use to jam the wireless channel:

1. ***Constant Jammer*** – The constant jammer is one that constantly transmitting the radio signals. Constant jamming can be achieved either using a waveform generator that continuously transmits the radio signal or by a wireless device that continuously sends out random bits to the channel. Thus the constant jammer prevents the legitimate source from sending packets [35].
2. ***Deceptive Jammer*** – The deceptive jammer is defined as the jammer that constantly placing the regular packet to the channel without any gap between the successive packet transmissions, as a result the legitimate receiver is misguided and believes that the packet are legal and authorized. The deceptive jamming is more difficult to identify than constant jamming because of its packet injecting property [35, 36].
3. ***Random Jammer*** – The random jammer is one that alternatively transmits radio signal between sleeping and jamming. The random jammer enters in the sleep mode after jamming the channel for a while and it starts jamming again after sleeping for a time. The random jammer saves its energy while working in this pattern [35].
4. ***Reactive Jammer*** – The reactive jammer is defined as the jammer that becomes active when it sense activity on the channel and become inactive when the channel is idle. The reactive jammer is more difficult to implement and the detection of reactive jamming is also a very challenging task [36].

6.1.2 Scrambling Attack

Scrambling attack is a special kind of jamming attack, in jamming attack a strong signal interference source is used to disrupt the normal radio communication while in scrambling attack a specific contention or frames is disrupted for short interval. It is very difficult to detect the scrambling attack since it focuses only on the specific frame leaving other frames unchanged. It solely depends on the scramblers choices which information (control or management) he/she want to affect to interrupt the normal operation of the network [34, 37].

6.2 Security Against Threats

Numerous solution have been proposed in past to mitigate jamming and scrambling attack. A simple link adaptation algorithm based on Carrier to Interference Ratio (CINR) is adopted to make the system resistance to jamming. In this algorithm Carrier to Interference Ratio (CINR) is selected as a channel quality metric for the link adaptation algorithm and the value of this channel quality metric is checked continuously. If the calculated value is beyond the specified range of the current operation mode, the system will adapt to some other stronger/weaker operation mode. The advantage of this algorithm is that there will be no overhead of CINR computation and to change the standard protocol as it is mandated by the standard [38].

For securing WiMAX Mesh network from jamming, a new framework based on multiple Base Stations (BSs) is developed. In the framework, multiple Base Stations (BSs) provides network survivability in case of jamming and Base Station (BS) demolition. Multiple Base Stations (BSs) are used so that the nodes can be routed to another Base Station (BS) under the jamming attack. The multiple Base Stations (BSs) frameworks need a distributed scheduling algorithm because there is no single point of control for performing centralised scheduling. A scheduling algorithm based on finite field initial slot assignment is used in this framework. Multiple Base Stations (BSs) not only help in network survivability under jamming but also improve the network throughput [39].

Antenna plays an important role in jamming, so to mitigate jamming a technique based on modification in antenna is invented. This technique uses a combination of a linear array antenna and parabolic reflector at the Base Station (BS), the array antenna behaves as an anti-jamming elements. The general idea is to have two receiver heads; one receiver head gets the transmitted signal and jamming signal while the other receiver head gets only the jamming signal. Then these two received signals are subtracted, the result which is obtained will be the transmitted signal [40].

Another technique base on antenna is elaborated in which a compact smart antenna is created which is capable of mitigating interference in the dense areas [41].

Digital filter can be used to alleviate the jamming effect. In wireless communication, a narrow spectral component is present in the received signal due to cycling behaviour, so a method based on digital filter at the receiver side is introduced to effectively destroy the narrow spectral component. In this method, the random and periodic jamming is considered and the effect of these jamming with and without the digital filter is evaluated and compared. The filtering method is very attractive because of the implementation simplicity as compared to traditional jamming defence methods. The drop back of this method is that it degrades the legitimate received signal and makes it more vulnerable to random noise of the communication channel and this approach results in higher error rate in non-jamming situation [42].

These approaches are traditional for mitigating jamming. A new viewpoint based on the location of the jammer is used for building strategies against jamming. In this framework, the network topology is divided into clusters and then the locations of multiple jammers is calculated successfully even when their jamming areas are overlapping. The localizing framework approach is highly effective in localizing multiple attackers with or without the prior knowledge of the order that the multiple jammers are turned on. The approach does not depend on measuring the received signal strength inside the jammed area nor does it require delivering information out of the jammed area, only it uses the disturbed network communication and derives node clusters for jammer localization grounded on network topology changes. For localizing, two new algorithms, namely Mirroring and Gauss - Newton Searching algorithms is used, these two algorithms are very effective in connected jamming area made by multiple jammers [43].

For securing communication system from scrambling attack a scheme based on control channel hopping is designed. In this scheme, the control channel, including frame control header (FCH), Downlink map (DL-MAP), and Uplink map (UL-MAP) are transmitted up to three symbols, so that the control channel length is three. According to this scheme, the control channel is hopped in the Downlink of each frame i.e. the start index of the control channel has a different symbol index within the Downlink at each frame [44].

6.3 Summary

This chapter explains the security attacks at Physical (PHY) layer and also analyse the security measures to defy against the attacks.

- Jamming and Scrambling attack are the two most serious attacks at WiMAX Physical (PHY) layer.
- Noise and Multicarrier types of jamming are possible and jamming can be procured using any type of jammer (constant, deceptive, random and reactive).

- Link adaptation, multiple Base Station (BS) and smart antenna technique is adopted to mitigate jamming.
- To secure WiMAX from scrambling, technique such as channel hopping is endorsed.

Chapter 7
Detection of Jamming in WiMAX

7.1 Attack Model and Assumptions

In this paper, our focus is on low power constant and deceptive jammers. We assume that the jammer has the following properties:

1. Partial band and full band jamming is considered while channel frequency and bandwidth of the targeted Base Station (BS) and Subscriber Station (SS) are known to an adversary.
2. The jammer is placed next to the Base Station (BS) or Subscriber Station (SS). With this, the jammer is able to distort packet destined to the Base Station (BS) or Subscriber Station (SS) and degrade or interrupts the communication. The jammer is continuously transmitting packet back to back, preventing the Base Station (BS) and Subscriber Station (SS) from accessing the medium.
3. The jammer is operating at very low power, such that the power of jammer is conserved and making the detection of the attack a difficult task.

7.2 Detection of Jamming Attack

In this work, the method of detecting jamming is based on the basic statistics strategy such as Received Signal Strength (RSS), Packet Delivery Ratio (PDR), Signal to Interference plus Noise Ratio (SINR) and Carrier Sensing.

7.2.1 Received Signal Strength (RSS)

Received Signal Strength (RSS) is defined as power present in the radio signal. The Signal Strength between the Base Station (BS) and the Subscriber Station (SS) must be strong enough to maintain signal quality at the receiver. Jamming can be detected by measuring the signal strength received at the Subscriber Station (SS), as in the presence of jammer the Received Signal Strength (RSS) is affected.

7.2.2 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) can be defined as the number of error free packet received from the total number of received packets. As the jammer corrupts the transmission between the Base Station (BS) and the Subscriber Station (SS), the Packet Delivery Ratio (PDR) can be used as a technique to detect jamming. The Packet Delivery Ratio (PDR) will be zero in presence of a jammer.

There are two places in WiMAX where Packet Delivery Ratio (PDR) can be measured:

1. ***At the Base Station (BS):*** The Packet Delivery Ratio (PDR) can be measured simply by keeping the track of the acknowledgement the Base Station (BS) receives from the Subscriber Station (SS).
2. ***At the Subscriber Station (SS):*** The Packet Delivery Ratio (PDR) can be measured using the ratio between the number of Cyclic Redundancy Check (CRC) packet and the total number of packet the Subscriber Station (SS) received from the Base Station (BS).

7.2.3 Signal to Interference plus Noise Ratio (SINR)

The Signal to Interference plus Noise Ratio (SINR) is a ratio use to compute the condition of the wireless connection.

The Signal to Interference plus Noise Ratio for Subscriber Station (SS) is defined as:

$$\mathrm{SINR}(\mathrm{x}) = \frac{P}{N+I}$$

where ‘x’ is some location of Subscriber Station (SS) in space, ‘P’ is the power of the received signal, ‘N’ is the noise caused by the medium in the incoming signal and ‘I’ is the interference caused by the jammer in the incoming signal.

7.2.4 Channel Sensing

When a Subscriber Station (SS) is losing its sending capability it is a clear sign that it is being jammed. A jammer prevent a legitimate Subscriber Station (SS) from sending out a packets because the channel appears constantly busy to the Subscriber Station (SS), using Channel Sensing as a technique we can determine whether the Subscriber Station (SS) is jammed.

In WiMAX, jamming can be detected at Base Station (BS) and Subscriber Station (SS). For detecting jamming at Subscriber Station (SS), we apply the method such as Signal to Interference plus Noise Ratio (SINR), Signal Strength and PDR for Downlink Channel and Channel Sensing for the Uplink Channel. For detecting jamming at Base Station (BS) same method can be applied.

7.3 Algorithm for Detection of Jamming At Dowlink Channel

```
Subscriber_Station _Downlink_Jamming_Detection
{
 SS_SINR=Measured_SINR      // Calculate the Current Signal to Interference plus Noise Ratio
  if (SS_SINR < SINR_Threshold)  then
      SS_PDR=Measured_PDR           // Calculate the Current Packet Delivery Ratio value
       if (SS_PDR < PDR_Threshold) then
           SS_SS=Measured_Signal Strength         // Calculate the Current Signal Strength value
            if (SS_SS > Signal Strength_Threshold) then
                SS_SC=Status_Compare (SS_PDR, SS_SS)   // Comparing the PDR value with
                                                        respect to Signal Strength value.
                 if (SS_SC==False)then
                     SS_Downlink_Jammed = 1    // Subscriber Station (SS) is Jammed
                                     end
                             end
                     end
             end
             }
```

7.4 Algorithm for Detection of Jamming At Uplink Channel

```
Subscriber_Station _Uplink_Jamming_Detection
{
    Uplink = 1;                 // Initially Uplink is idle so its value will be 1
    // When Subscriber Station has data to send
    z = Check (Uplink)     // Sense the Uplink when the subscriber station has data to send, the
                                            value of z will be 1 if  it is idle and 0 when it is busy.
   if (z==1) then
         Send (Data)
   end
   else
           SS_Uplink_Jammed = 1
    end
}
```

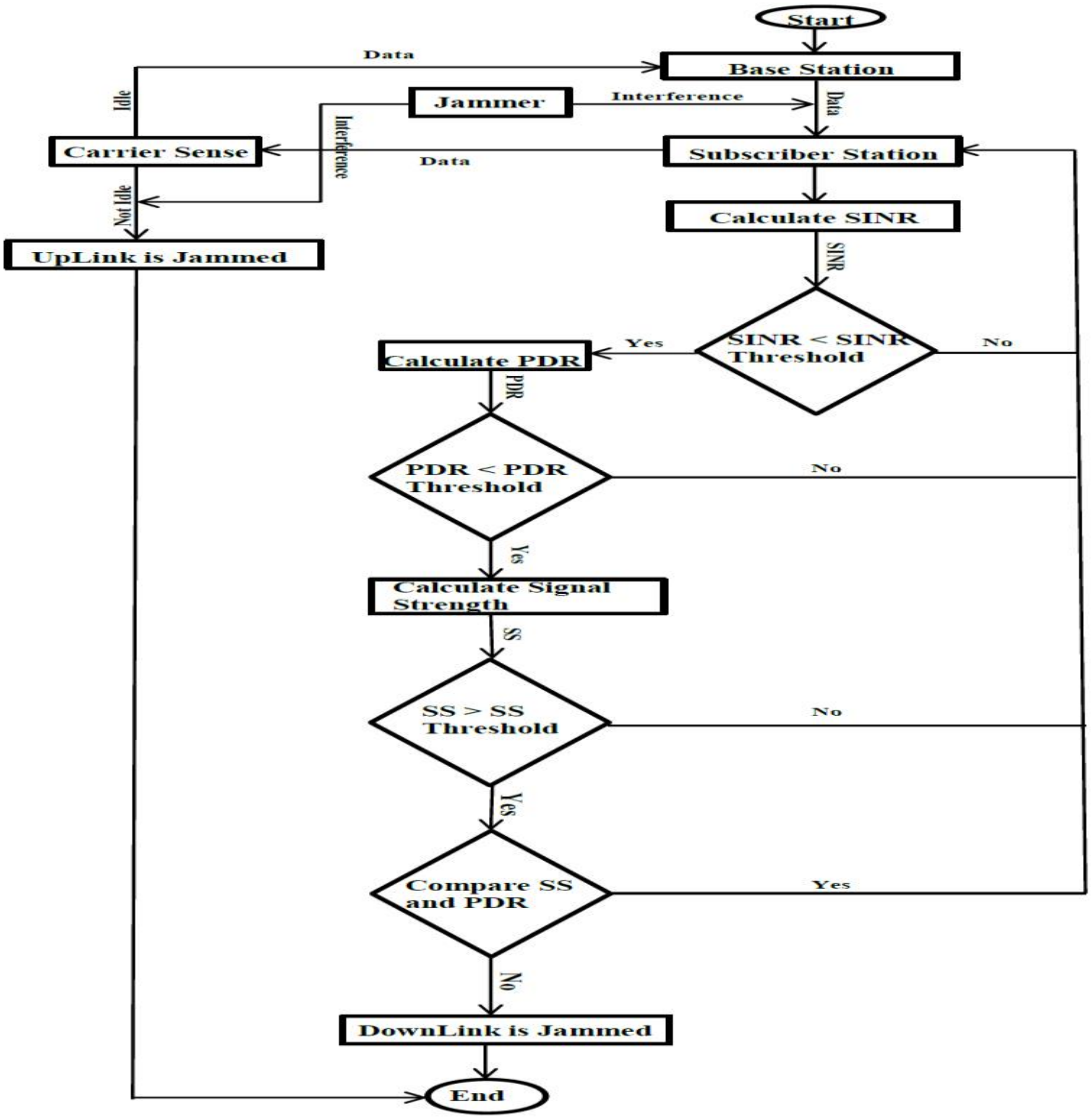


Figure 7.1: Flowchart For Detection Of Jamming At Downlink and Uplink Channel

7.5 Recovery from Jamming Attack

The recovery of jamming attack involves the step of network entry by scanning the Downlink frequency and searching for the appropriate Uplink frequency corresponding to the selected Downlink frequency in case of Downlink channel jamming while in the case of Uplink jamming only searching of new Uplink channel is needed. After selecting the new channel the old frequency is transferred to the Base Station (BS).

7.5.1 Algorithm for Recovery from Jamming Attack

```
Recovery _Of_ Subscriber_Station_From_Jamming
{
        SS_ULP = UL_Parameter            //Current Uplink Channel value.
        SS_DLP = DL_Parameter            //Current Downlink Channel value.
        if (SS_Downlink_Jammed) then
                Network_Entry        // Start the Network Entry Procedure for Subscriber Station (SS)
                Send (SS_DLP)            // After Network Entry, the Subscriber Station (SS)
                                         sends the Downlink Channel Frequency to the
                                         selected Base Station (BS).
         end
         else
                if (SS_Uplink_Jammed) then
                Search_Uplink_Channel_Descriptor     // If Uplink is jammed the Subscriber
                                                     Station (SS) start searching for new
                                                     Uplink Channel
                 Send(SS_ULP)        // After having new Uplink Channel, the Subscriber Station
                                     (SS) send the old Uplink Channel to the Base Station (BS).
        end
  end
```

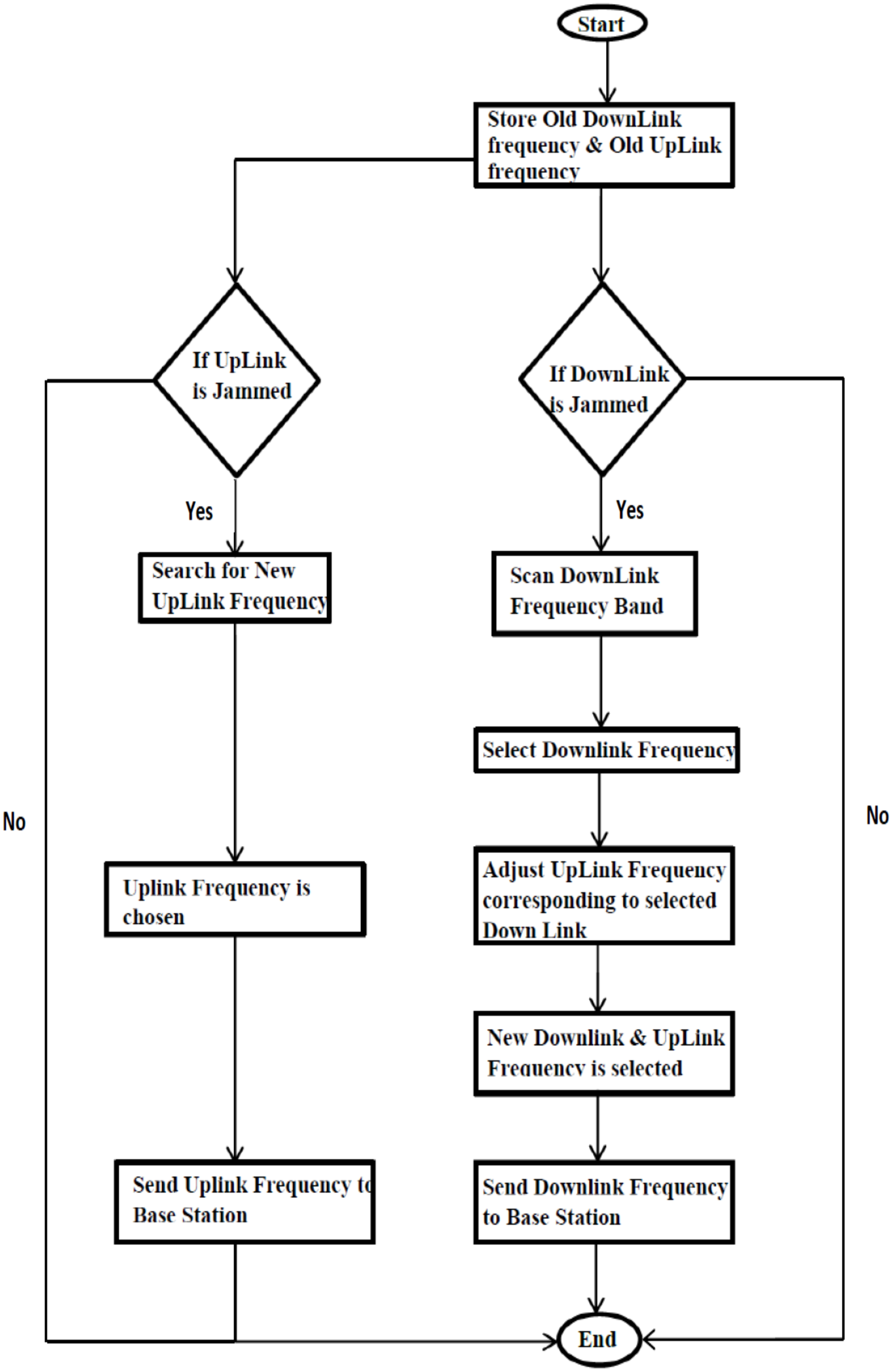

Start
Store Old DownLink frequency & Old UpLink frequency
If UpLink is Jammed
If DownLink is Jammed
Yes
Yes
Search for New UpLink Frequency
Scan DownLink Frequency Band
Select Downlink Frequency
No
No
Uplink Frequency is chosen
Adjust UpLink Frequency corresponding to selected Down Link
New Downlink & UpLink Frequency is selected
Send Uplink Frequency to Base Station
Send Downlink Frequency to Base Station
End

Figure 7.2: Flowchart For Recovery From Jamming Attack

7.6 Summary

This chapter presented a solution for detection of jamming attack in WiMAX.

- Jamming attack can be possible either on Uplink Channel, Downlink Channel or on both.
- Jamming can be detected using Received Signal Strength (RSS), Packet Delivery Ratio (PDR), Signal to Interference plus Noise Ratio (SINR) and Channel Sensing parameters.
- Received Signal Strength (RSS), Packet Delivery Ratio (PDR), Signal to Interference plus Noise Ratio (SINR) parameters are used to detect Downlink Channel jamming in WiMAX.
- Channel sensing parameter is used to detect Uplink jamming in WiMAX.

Chapter 8

Theoretical Methodology

8.1 Overview

In WiMAX, the connection is established before any communication between the Base Station (BS) and the Subscriber Station (SS).The connection channel between the Base Station (BS) and Subscriber Station (SS) is known as Downlink Channel, while between the Subscriber Station (SS) and Base Station (BS) is known as Uplink Channel.

Initially, the Subscriber Station (SS) scans the Downlink (DL) frequency band for the valid DL channel. Basically, this scanning is meant for the PHY synchronization and it will end when the Subscriber Station (SS) receives at least one DL-Medium Access Protocol (DL-MAP) message. The MAC remains synchronized till it get DL-MAP and Downlink Channel Descriptor (DCD) message for the channel. The Subscriber Station (SS) can determine the suitable Downlink channel from the information present in the DCD message. Similarly, the Subscriber Station (SS) acquire the Uplink Channel by searching the Uplink Channel Descriptor (UCD) message which is transmitted periodically from the Base Station (BS) [14]. After acquiring both the channels the communication gets started between the Base Station (BS) and the Subscriber Station (SS).

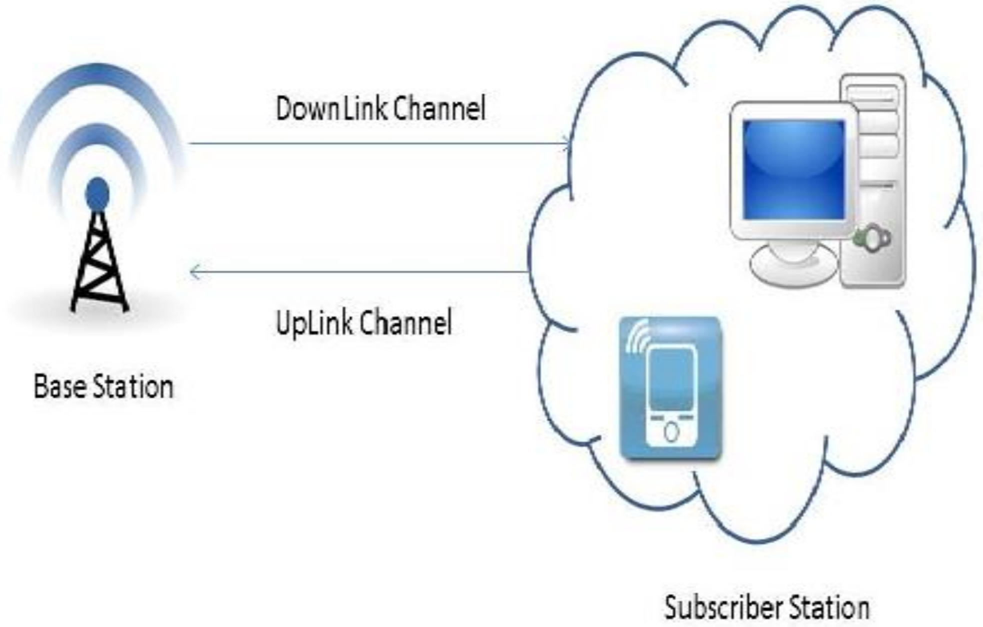


Figure 8.1: Communication In WiMAX

8.2 Jamming Attack at Downlink Channel

Consider a scenario when a jammer is trying to jam the communication on the Downlink Channel, so the communication between Base Station (BS) and Subscriber Station (SS) get affected which leads to performance degradation. Now our aim is to detect the jamming at the Subscriber Station (SS) for the Downlink Channel. At the Subscriber Station (SS), when a packet from the Base Station (BS) is received using the Downlink Channel the Signal to Interference plus Noise Ratio (SINR) is calculated and compare with the Signal to Interference plus Noise Ratio (SINR) threshold. If the value of the calculated Signal to Interference plus Noise Ratio (SINR) is less than the Signal to Interference plus Noise Ratio (SINR) threshold, then the other two parameters (Signal Strength and Packet Delivery Ratio) are checked. The current Packet Delivery Ratio (PDR) is measured and checked with the Packet Delivery Ratio (PDR) threshold value, if the measured Packet Delivery Ratio (PDR) is less than the threshold value then the current Signal Strength (SS) is calculated and compared with the Signal Strength (SS) threshold value, if the Signal Strength (SS) value is above the threshold value then the measured Packet Delivery Ratio (PDR) is compared with the current Signal Strength (SS) value. Now, if the current Signal Strength (SS) has a higher value and corresponding to that the Packet Delivery Ratio (PDR) value is low then we say that the Subscriber Station (SS) is under the jamming attack in the DownLink Channel. All the parameters are deterministic and there threshold value can be evaluated by performing the experiment. These parameters are solely dependent on several factors such as distance between the Base Station (BS) and the Subscriber Station (SS), interference caused by co-channel and adjacent channel, environment, noise, physical obstacle like helicopter.

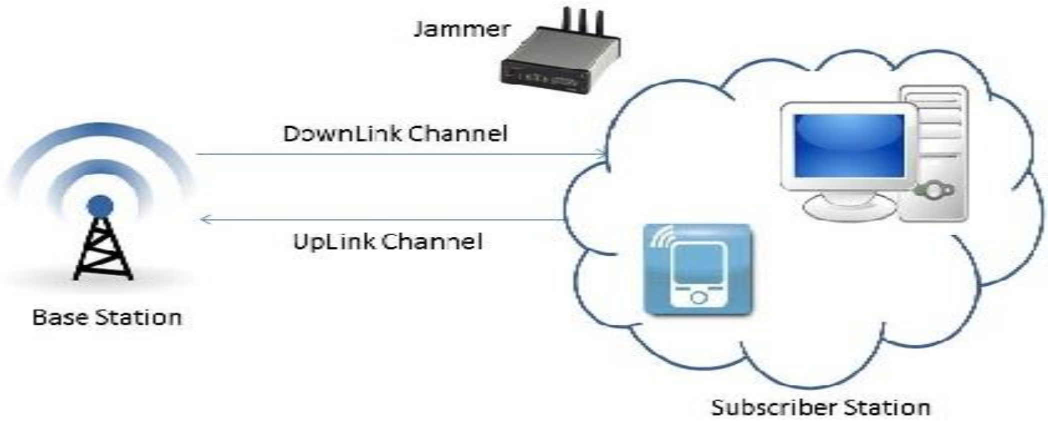


Figure 8.2: Downlink Jamming in WiMAX

8.3 Jamming Attack at Uplink Channel

Now consider the situation when a jammer is trying to jam the communication on the Uplink channel, so the communication between the Subscriber Station (SS) and Base Station (BS) get affected. Now our aim is to detect the jamming at the Subscriber Station (SS) for Uplink channel. At the Subscriber Station (SS), when the Subscriber Station (SS) is ready for sending data to the Base Station (BS), first the Subscriber Station (SS) checks the status of the Uplink channel by sensing the Uplink channel and on the status of the Uplink channel the Subscriber Station (SS) take the decision of sending the data. If the Subscriber Station (SS) found the Uplink channel idle it will start sending the data towards the Base Station (BS) and if it found the Uplink channel busy then it can’t send the data i.e. the Subscriber Station (SS) sending capabilities is losing and the Subscriber Station (SS) reported itself under the jamming attack. There is several techniques of sensing channel, the most simply one is to send the test signal and get the acknowledgment, the other methods includes matched filter and energy detection. The sensing of channel is beyond the scope of this work.

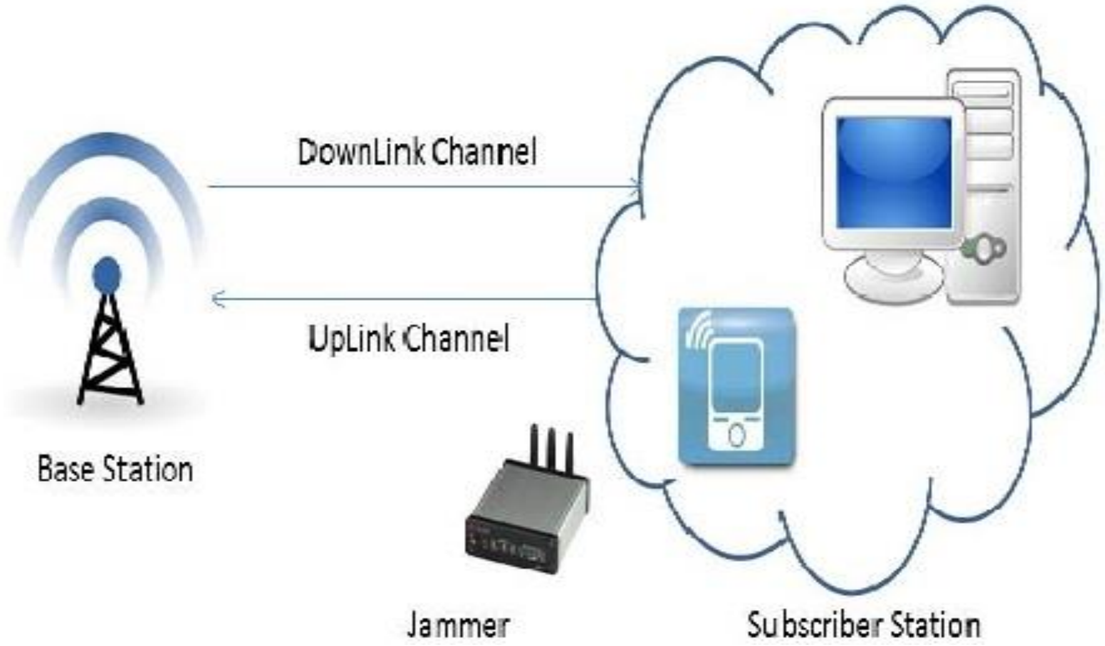


Figure 8.3: Uplink Jamming in WiMAX

8.4 Recovery from Jamming Attack

In WiMAX, the major task from the security point of view is to detect the jamming. After the detection of jamming the Subscriber Station (SS) need to be recovered from it. After jamming the Subscriber Station (SS) need to do the channel hopping or in other words the Subscriber Station (SS) need to be modulated to some other channel. There are separate methods of channel hopping for Downlink channel and Uplink channel. To recover from Downlink channel jamming, the Subscriber Station (SS) saves the current Downlink frequency and disconnect from the current Downlink channel. After disconnecting the connection the Subscriber Station (SS) start scanning the Downlink frequency band for the new Downlink channel and selects the most suitable Downlink channel. After the new Downlink channel is selected the Uplink channel corresponding to this Downlink channel is acquired between the Subscriber Station (SS) and the Base Station (BS).

To recover from Uplink channel jamming, the Subscriber Station (SS) saves the current Uplink frequency and then disconnects the Uplink connection and start searching for the new Uplink channel. The difference lies in selection of new connection with the Base Station (BS), when Downlink is changed the corresponding Uplink is also changed while when the Uplink is changed the Downlink remains the same. After making the new connection with the Base Station (BS) either the Downlink or Uplink the previous frequency saved by the Subscriber Station (SS) is transferred to the Base Station (BS), so that the Base Station (BS) would know in future that this appropriate frequency is vulnerable to jamming.

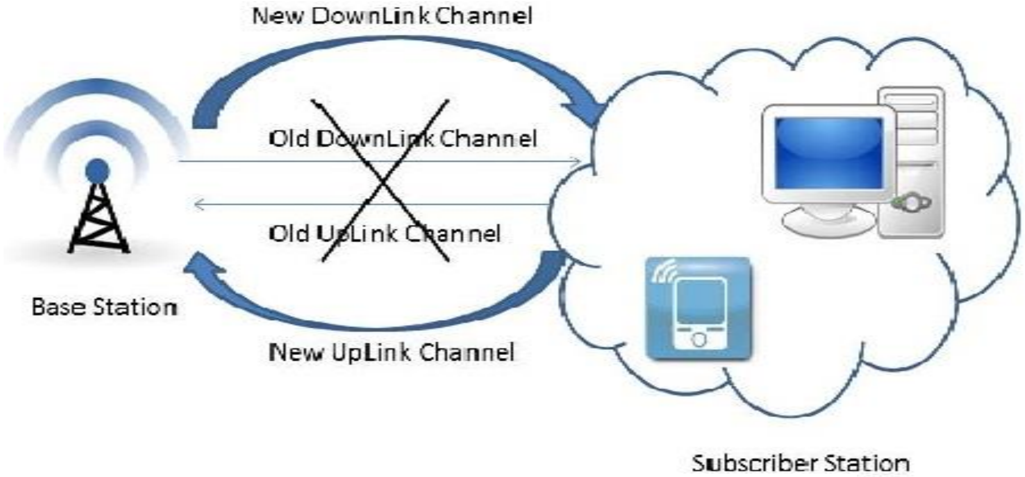


Figure 8.4: Communication in WiMAX After Recovery

8.5 Summary

This chapter describe the theoretical methodology of WiMAX.

- In WiMAX two connections Downlink and Uplink are established between Base Station (BS) and Subscriber Station (SS).
- The Subscriber Station (SS) is synchronized with the Base Station (BS) using DL-MAP messages.
- The Subscriber Station (SS) scans the frequency band and select the Downlink frequency and also acquire Uplink frequency corresponding to it.
- At the Subscriber Station, all the four Received Signal Strength (RSS), Packet Delivery Ratio (PDR), Signal to Interference plus Noise Ratio (SINR) and Channel Sensing parameters are checked to find out whether the Subscriber Station (SS) is jammed or not.
- The Subscriber Station (SS) uses the Initial Network Entry to recovered from jamming.

Chapter 9
Simulation

9.1 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a multicarrier transmission technique, based on the principle of transmitting several narrow-band orthogonal frequencies, known as OFDM subcarriers. These frequencies are orthogonal to each other and each frequency channel is modulated with a different modulation technique. The number of subcarriers is represented by *N*.

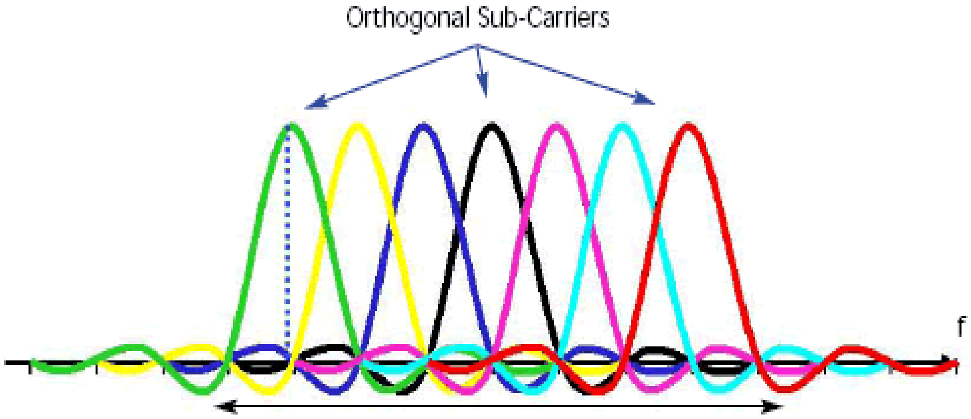


Figure 9.1: OFDM Signal

There are basically four types of subcarriers:

1. ***Data Subcarriers:*** It is used to transfer data.
2. ***Pilot Subcarriers:*** It is used to estimate the channel and perform synchronisation. There are eight pilot subcarriers.
3. ***Null Subcarriers:*** Null subcarriers are also known as guard bands.
4. ***Direct Current (DC) Subcarriers:*** The direct current subcarrier frequency is equal to the frequency of radio transmitting station.

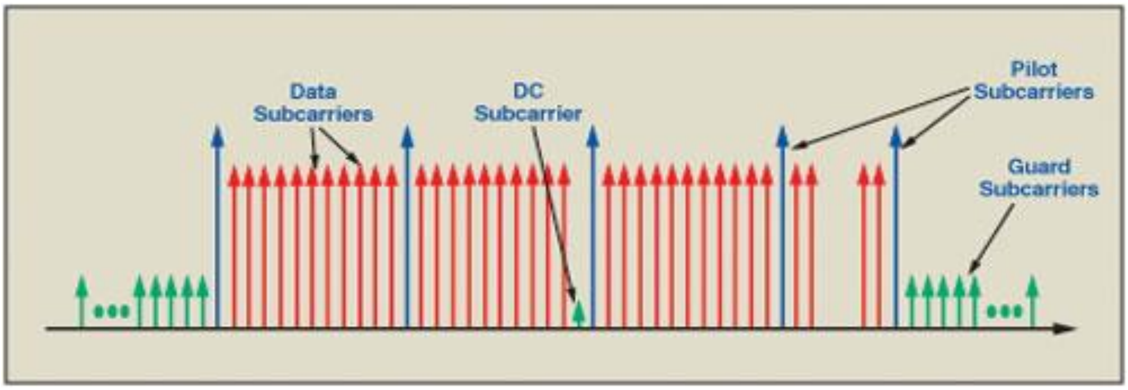


Figure 9.2: Subcarriers

9.2 OFDM Block Diagram

The modulation and transmission aspects are the major building blocks of OFDM. The data coming from the media access control (MAC) layer is first channel coded, whose main task is to prevent and correct the transmission error. The channel coding is composed of three steps: randomiser, forward error correction (FEC) and interleaving.

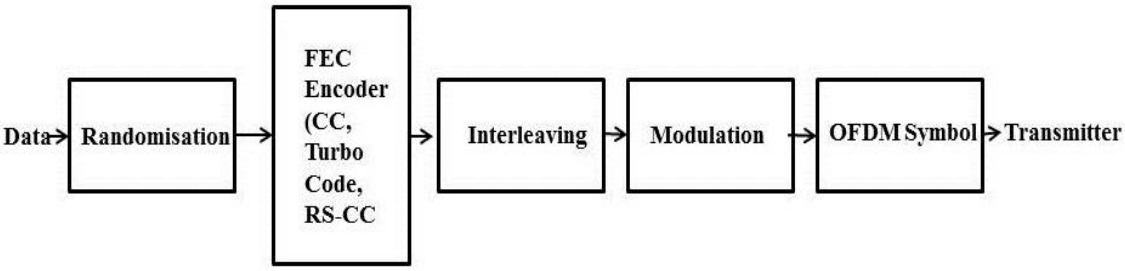


Figure 9.3: OFDM Block Diagram at Sender

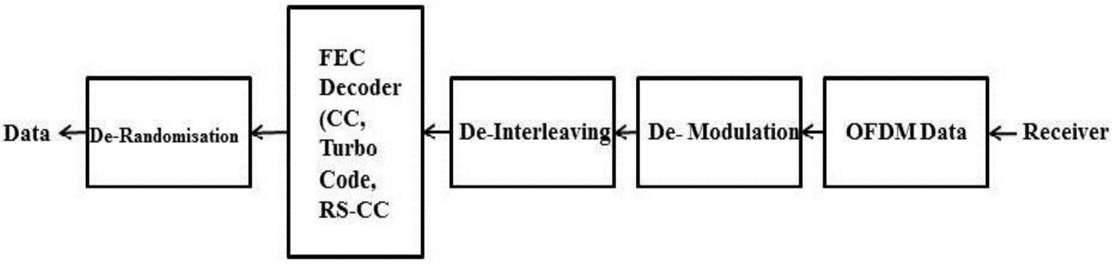


Figure 9.4: OFDM Block Diagram at Receiver

9.2.1 Randomisation

Randomisation is a process in which the transmitted bit sequence are pseudo randomly scrambled, resulting in a sequence known as pseudorandom bit sequence (PRBS). It provides protection using information theoretic uncertainty, avoiding long sequences of consecutive ones or consecutive zeros. For each burst of data of Downlink and Uplink, data randomization is performed. Each data byte to be transmitted enters sequentially into the randomiser with the Most Significant Byte (MSB) first.

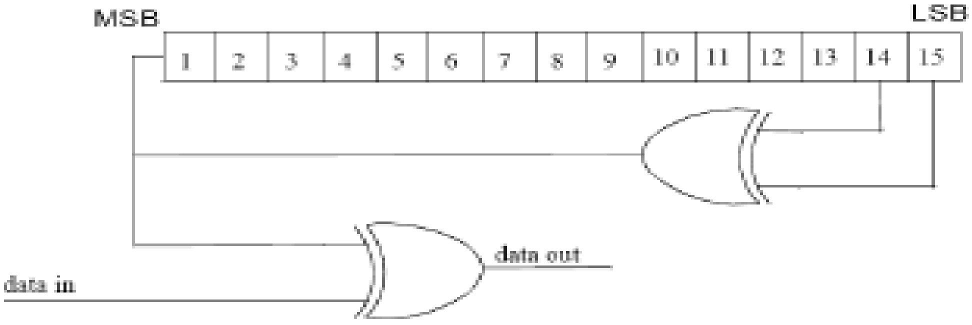


Figure 9.5: Pseudo-Random Binary Sequence (PRBS) generator

9.2.2 Forward Error Correction (FEC) Codes

Forward Error Correction is an error control code, which uses redundancy in finding errors and correcting them. For OFDM PHY, the FEC encodings are:

1. Concatenated Reed – Solomon Convolutional Code (RS-CC)
2. Convolutional Turbo Codes (CTC)
3. Block Turbo Coding (BTC)
4. Convolutional Code (CC)
5. Low Density Parity Check (LDPC) code

9.2.2.1 Reed – Solomon Convolution Code (RS-CC)

The Reed – Solomon Convolution encoding is performed by first passing the data in block through the Reed Solomon encoder and then passing through the convolution encoder. Reed – Solomon code is mandatory for both Downlink and Uplink.

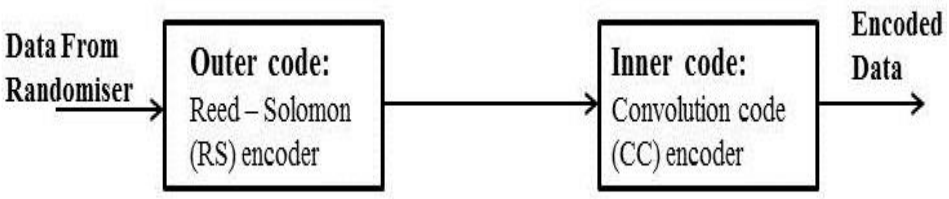


Figure 9.6: RS-CC encoder of OFDM PHY

9.2.2.2 Convolution Codes

A convolution code is generated by passing the information sequence to be transmitted through a linear finite – state shift register. In general, the shift register consists of K (k-bits) stages and n linear algebraic function generators. It is mandatory Forward Error Control (FEC) code for OFDM according to the IEEE 802.16 standard [3].

9.2.2.3 Block Turbo Codes

The Block Turbo Code is based on the product of two simple component codes, which are binary extended Hamming codes or parity check codes. It is optional Forward Error Control (FEC) code for OFDM according to the IEEEc802.16 standard [3].

9.2.2.4 Convolution Turbo Codes

The Convolution Turbo Code employ serial or parallel concatenated code with pseudo-random interleaving between the inner and outer code, it perform well at lower code rate. It is defined as optional FEC for OFDM and can be used to support Hybrid ARQ (HARQ) [3].

9.2.2.5 Low Density Parity Check (LDPC)

LDPC codes are the block codes, constructed using a sparse bipartite graph with parity-check matrices that contain only a very small number of non-zero entries. It is optional Forward Error Control (FEC) code for OFDM according to the IEEEc802.16 standard [3].

9.2.3 Interleaving

Interleaving is used to protect the transmission against long sequences of consecutive errors, which are very difficult to correct. The interleaver is made of two steps:

1. Distribute the coded bits over subcarriers. A first permutation ensures that adjacent coded bits are mapped on to nonadjacent subcarriers.
2. The second permutation insures that adjacent coded bits are mapped alternately on to less or more significant bits of the constellation, thus avoiding long runs of bits of low reliability.

9.2.4 Modulation

Modulation refers to the process of modulating the analogue signal with a digital sequence or vice versa in order to transport the sequence over a medium. Four types of modulations are support by the WiMAX.

9.2.4.1 Binary Phase Shift Keying (BPSK)

The Binary Phase Shift Keying (BPSK) is a binary digital modulation; it uses one bit to encode one modulation symbol and uses phase variation to encode bits. The phase of the Binary Phase Shift Keying (BPSK) modulated signal is ∏ or -∏ according to the value of the data bit.

9.2.4.2 Quadrature Phase Shift Keying (QPSK)

The Quadrature Phase Shift Keying (QPSK) can encode two bits per symbol; it can be used either to double the data rate compared with a Binary Phase Shift Keying (BPSK) system while maintaining the same bandwidth of the signal or to maintain the data rate of BPSK but having the bandwidth needed.

9.2.4.3 Quadrature Amplitude Modulation (QAM)

The Quadrature Amplitude Modulation (QAM) changes the amplitudes of two sinusoidal carriers depending on the digital sequence that must be transmitted, the two carriers being out of phase of +∏/2, this amplitude modulation is called quadrature. There are two type of Quadrature Amplitude Modulation (QAM): 16-QAM and 64-QAM. The 16-QAM transmits 4 bits for each modulation symbol while 64-QAM transmits 6 bits for each modulation symbol.

9.3 Jamming Analysis

The effect of jamming on the communication is greatly depends on the jamming strength. Basically for achieving the jamming effect on the communication one needs to increase the level of noise on the communication signal, so that the normal communication ceases. The quality of communication can be computed from the Signal to Interference plus Noise Ratio (SINR), which is a relation between the signal power received at the Subscriber Station (SS) and the interference plus noise:

$$\boldsymbol{SINR = \frac{Signal\ Power\ of\ Received\ Signal}{Interference + Noise\ in\ Received\ Signal}}$$

Now from the above formulae it can be easily infer that for a smooth communication the Signal to Interference plus Noise Ratio (SINR) value should be high enough. The level of noise in the communication signal will result in creating error in the packets. The level of error in the packets can be easily evaluated by the Packet Error Rate (PER), which is the ratio between the numbers of erroneous packets to the total number of packet sent:

$$\boldsymbol{PER = \frac{Number\ of\ Erroneous\ Packet}{Total\ Number\ of\ Packet\ Sent}}$$

9.3.1 Scenario 1

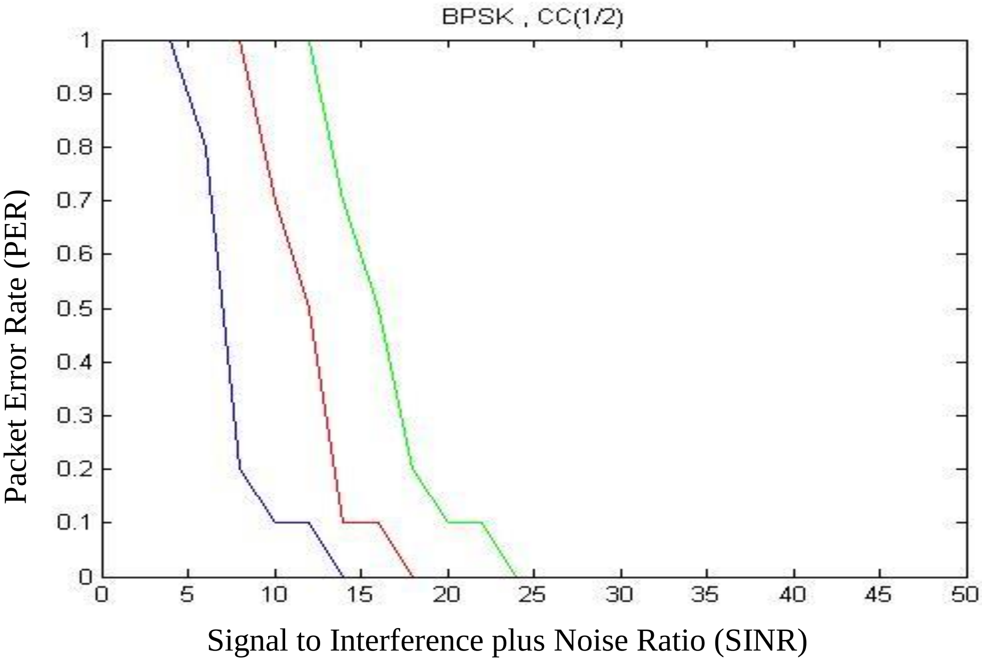


Figure 9.7: Graph using Binary Phase Shift Keying (BPSK) Modulation

In Scenario 1, a BPSK modulation technique with Convolution Code type of Forward Error Correcting (FEC) Codes is used to show the performance of WiMAX system under the jamming effect.

The performance of WiMAX system is analysed at three different noise levels. The blue line shows the system with very less or close to zero noise level, the red line shows the increase in the level of noise and the green line show further increase in the noise level. From the figure, it is clearly seen that to get zero per cent Packet Error Rate (PER) the value of Signal to Interference plus Noise Ratio (SINR) 14 dB, 18 dB and 24 dB is required.

9.3.2 Scenario 2

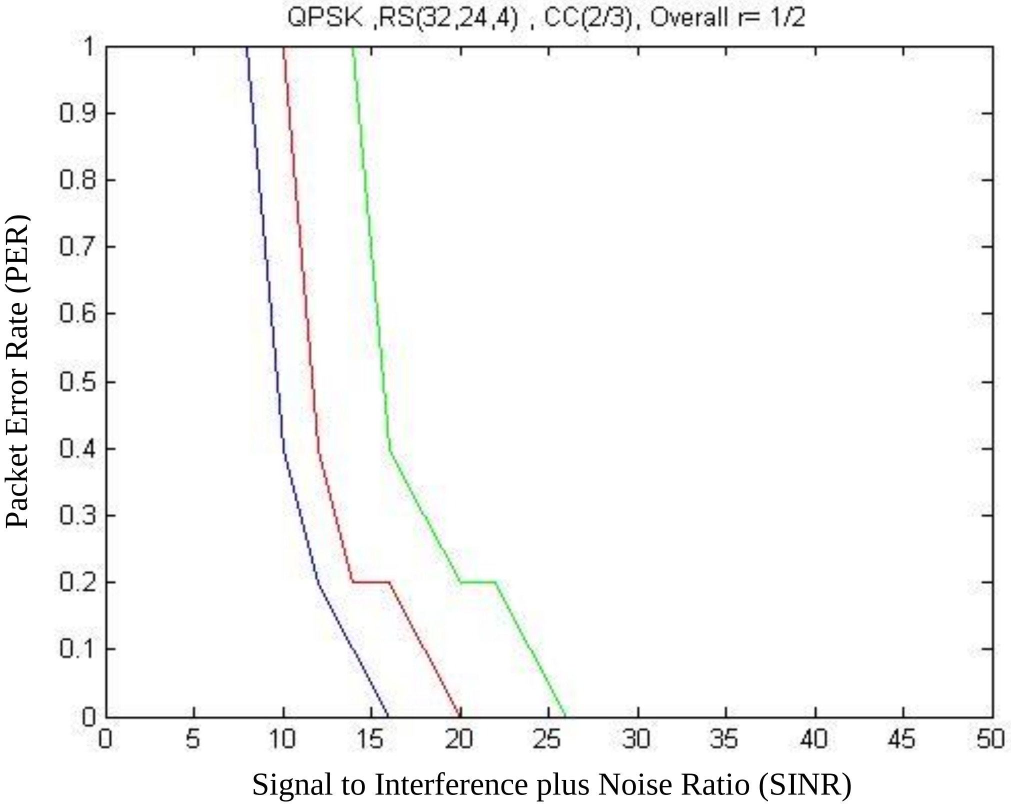


Figure 9.8: Graph using Quadrature Phase Shift Keying (QPSK) Modulation

In Scenario 2, a QPSK modulation technique with Concatenated Reed – Solomon Code type of Forward Error Correcting (FEC) Codes is used to show the performance of WiMAX system under the jamming effect. The RS (32, 24, 4) represents the Reed Solomon Code with 32 overall bytes after encoding, 24 data bytes before encoding and 4 data bytes which can be corrected by Reed – Solomon encoder decoder combination. The CC (2/3) represents the Convolution Code with 2/3 rate code.

Now in scenario 2, the performance of WiMAX system is again analysed at three different noise levels. The blue line shows the system with very less or close to zero noise level, the red line shows the increase in the level of noise and the green line show further increase in the noise level. From the figure, it is clearly seen that to get zero per cent Packet Error Rate (PER) the value of Signal to Interference plus Noise Ratio (SINR) 16 dB, 20 dB and 26 dB is required.

9.3.3 Scenario 3

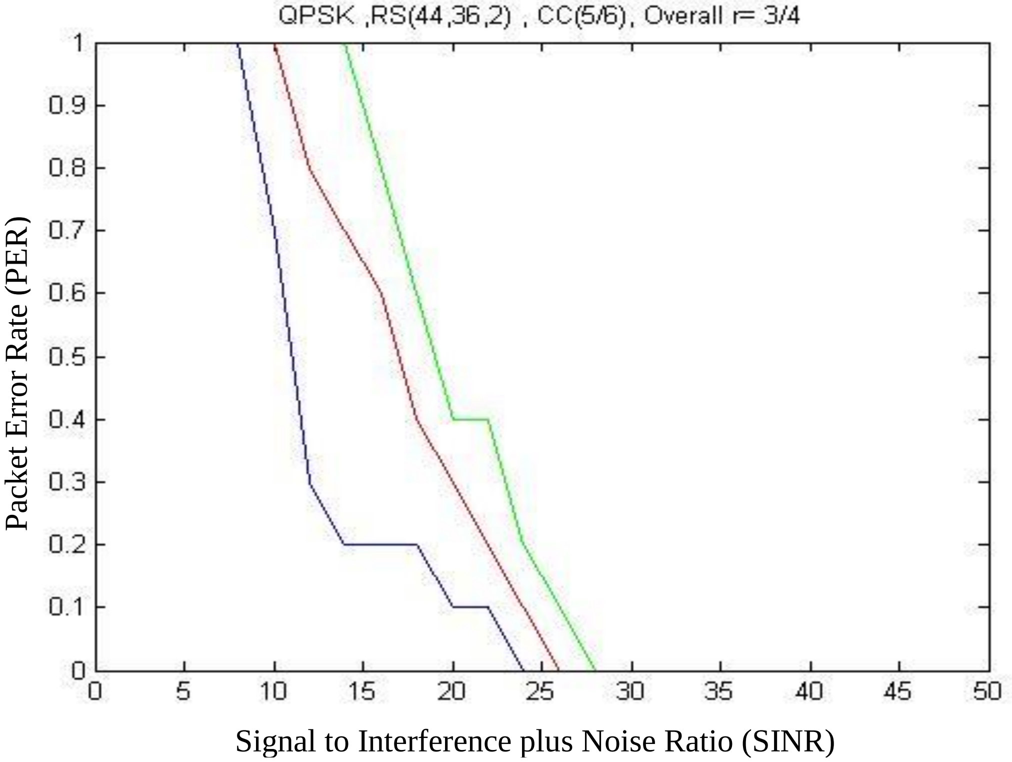


Figure 9.9: Graph using Quadrature Phase Shift Keying (QPSK) Modulation

In Scenario 3, a QPSK modulation technique with Concatenated Reed – Solomon Code type of Forward Error Correcting (FEC) Codes is used to show the performance of WiMAX system under the jamming effect. The RS (44, 36, 2) represents the Reed Solomon Code with 44 overall bytes after encoding, 36 data bytes before encoding and 2 data bytes which can be corrected by Reed – Solomon encoder decoder combination. The CC (5/6) represents the Convolution Code with 5/6 rate code.

Now in scenario 3, the performance of WiMAX system is scrutinized at three different noise levels. The blue line shows the system with very less or close to zero noise level, the red line shows the increase in the level of noise and the green line show further increase in the noise level. From the figure, it is clearly seen that to get zero per cent

Packet Error Rate (PER) the value of Signal to Interference plus Noise Ratio (SINR) 24 dB, 26 dB and 28 dB is required.

9.3.4 Scenario 4

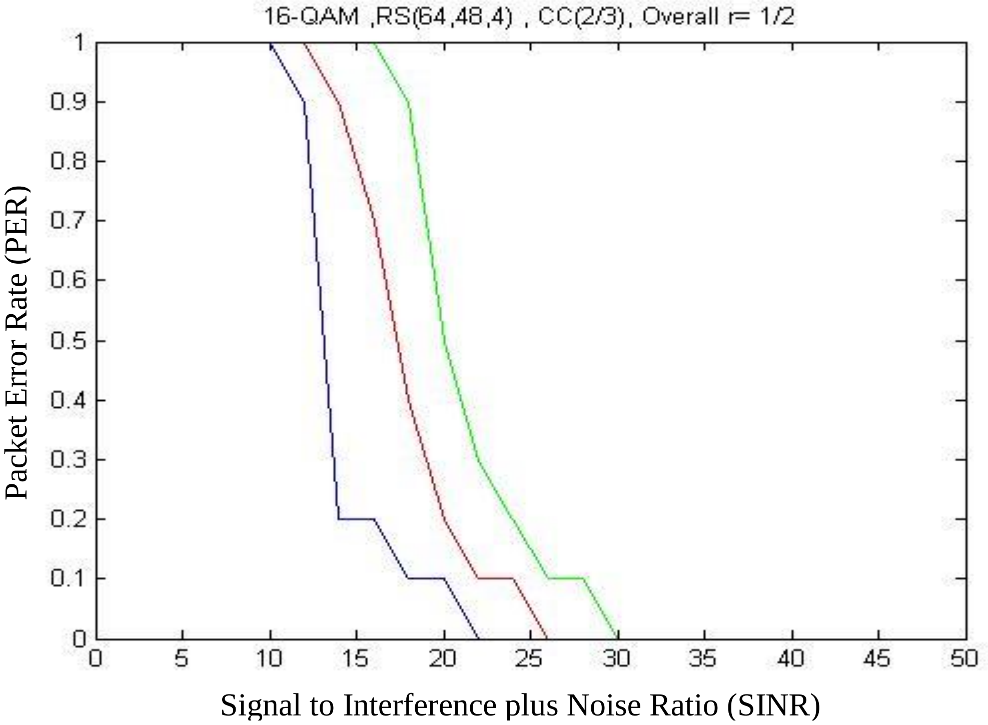


Figure 9.10: Graph using 16-Quadrature Amplitude Modulation (16-QAM)

In Scenario 4, a 16-QAM modulation technique with Concatenated Reed – Solomon Code type of Forward Error Correcting (FEC) Codes is used to show the performance of WiMAX system under the jamming effect. The RS (64, 48, 4) represents the Reed Solomon Code with 44 overall bytes after encoding, 36 data bytes before encoding and 2 data bytes which can be corrected by Reed – Solomon encoder decoder combination. The CC (2/3) represents the Convolution Code with 2/3 rate code.

Now in scenario 4, the performance of WiMAX system is scrutinized at three different noise levels. The blue line shows the system with very less or close to zero noise level, the red line shows the increase in the level of noise and the green line show further increase in the noise level. From the figure, it is clearly seen that to get zero per cent Packet Error Rate (PER) the value of Signal to Interference plus Noise Ratio (SINR) 23 dB, 26 dB and 30 dB is required.

9.3.5 Scenario 5

In Scenario 5, a 64-QAM modulation technique with Concatenated Reed – Solomon Code type of Forward Error Correcting (FEC) Codes is used to show the performance of WiMAX system under the jamming effect. The RS (108, 96, 6) represents the Reed

Solomon Code with 108 overall bytes after encoding, 96 data bytes before encoding and 6 data bytes which can be corrected by Reed – Solomon encoder decoder combination. The CC (3/4) represents the Convolution Code with 3/4 rate code.

Now in scenario 4, the performance of WiMAX system is scrutinized at three different noise levels. The blue line shows the system with very less or close to zero noise level, the red line shows the increase in the level of noise and the green line show further increase in the noise level. From the figure, it is clearly seen that to get zero per cent Packet Error Rate (PER) the value of Signal to Interference plus Noise Ratio (SINR) 34 dB, 36 dB and 40 dB is required.

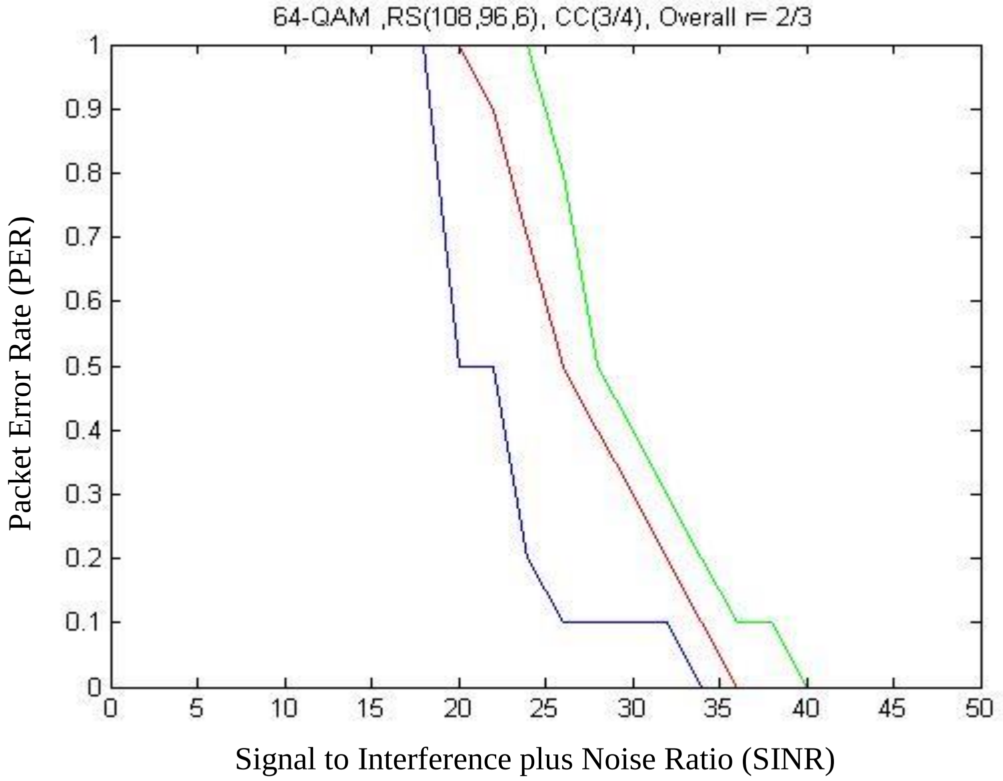


Figure 9.11: Graph using 64-Quadrature Amplitude Modulation (64-QAM)

9.4 Summary

This chapter describe the Orthogonal Frequency Division Multiplexing (OFDM) and its transmission chain for the sender and the receiver.

- The OFDM transmission chain includes Randomisation, Forward Error Correcting (FEC) codes, Interleaving, Modulation.
- There are four types of modulation techniques: Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), 16-Quadrature Amplitude Modulation (QAM) and 64-Quadrature Amplitude Modulation (QAM).

Chapter 10

Conclusion

The goal of this thesis was to evaluate how an IEEE 802.16 based WiMAX communication system operates in a hostile environment. In this thesis, first a technique is developed for detecting jamming in WiMAX based communication system then the performance of the developed technique is evaluated. The technique includes performance metrics such as Signal to Interference plus Noise Ratio (SINR), Signal Strength, Packet Delivery Ratio (PDR) and Channel Sensing for the detection of Downlink and Uplink jamming. The recovery mechanism from jamming is also mentioned, which involves the cache of old Downlink and Uplink frequency and then scan for the new Downlink and Uplink frequency in case of the Downlink channel jamming while in case of the Uplink channel jamming only new Uplink frequency is searched corresponding to the existing Downlink frequency.

The measurement were conducted and the vulnerability of the WiMAX system was tested on four modulation scheme BPSK, QPSK, 16-QAM, 64-QAM supported by the WiMAX system by jamming the pilot subcarriers. Signal to Interference plus Noise Ratio (SINR) values were compared with Packet Error Rate (PER) values for each modulation scheme.

Reference

[1] WiMAX Forum, “IEEE 802.16a Standard and WiMAX Igniting Broadband Wireless Access”, White Paper, Retrieved on: 09/08/2013, Available at: https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&ved=0CEUQFjAE&url=http%3A%2F%2Fwww.educationpermanente.fr%2Fpublic%2Farticles%2Fdownload.php%3Fid_document%3D3&ei=xfA7Us2bO8jirAfZ34GICw&usg=AFQjCNFtXt2iDfeEUrV7Zue-0Dub1szCsQ&bvm=bv.52434380,d.bmk.

[2] IEEE Standard Association, “IEEE 802.16-2012 Standard”, Retrieved on: 09/08/2013, Available at: http://standards .ieee.org/getieee802/download/802.16-2012.pdf.

[3] Nuaymi Loutfi, “WiMAX Technology for Broadband Wireless Access”, John Wiley & Sons Ltd, 2007.

[4] Wikipedia, “Personal Area Network”, Retrieved on: 02/05/2014, Available at: http://en.wikipedia.org/wiki/Personal_area_network.

[5] Wikipedia, “Local Area Network”, Retrieved on: 02/05/2014, Available at: http://www.wikipedia.org/wiki/Local_area_network.

[6] Wikipedia, “Metropolitan Area Network”, Retrieved on: 02/05/2014, Available at: http://en.wikipedia.org/wiki/Metropolitan_area_network.

[7] Wikipedia, “Wide Area Network”, Retrieved on: 02/05/2014, Available at: http://en.wikipedia.org/wiki/Wide_area_network.

[8] Xiao Yang, “WiMAX/MobileFi Advanced Research and Technology”, Auerbach Publications, 2008.

[9] Eklund Carl, Marks B. Roger, Stanwood L. Kenneth and Wang Stanley, “IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access”, IEEE Communications Magazine, Page(s): 98-107, 2002.

[10] Prasad Ramjee and Velez J. Fernando, “WiMAX Networks Techno – Economic Vision and Challenges”, Springer, 2010.

[11] “IEEE 802.16-2013 Standard”, Retrieved on: 23/08/2013, Available at: http: //standards .ieee.org/getieee802/download/802.16-2013.pdf.

[12] Kolias Constantinos, Kambourakis Georgios and Gritzalis Stefanos, “Attacks and Countermeasures on 802.16: Analysis and Assessment”, IEEE Communication Surveys and Tutorials, Vol.: 15, Issue: 1, Page(s): 487-514, 2013.

[13] Andrews G. Jeffrey, Ghosh Arunabha and Muhamed Rias, “Fundamentals of WiMAX: Understanding Broadband Wireless Networking”, Prentice Hall Communications Engineering and Emerging Technologies Series, 2007.

[14] Han Tao, Zhang Ning, Liu Kaiming, Tang Bihua and Liu Yuanan, “Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions”, 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Pages(s): 828-833, 2008.

[15] Bhargava Bharat, Yu Zhang, Nwokedi Idika, Leszek Lilien and Mehdi Azarmi, “Collaborative Attacks in WiMAX Networks”, Security and Communication Networks, Vol.: 2, Issue: 5, Page(s): 373-391, 2009.

[16] Naseer Sheraz, Younus Muhammad and Ahmed Attiq, “Vulnerabilities Exposing IEEE 802.16e Networks to DoS Attacks: A Survey”, 9th IEEE ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Page(s): 344-349, 2008.

[17] Lee Patrick PC, Tian Bu and Thomas Woo, “On the Detection of Signaling DoS Attacks on 3G/WiMAX Wireless Networks”, Elsevier Journal of Computer Networks, Vol.: 53, Issue: 15, Page(s): 2601-2616, 2009.

[18] Ibikunle F.A, “Security Issues in Mobile WiMAX (IEEE 802.16e)”, IEEE Conference on Mobile WiMAX Symposium, Page(s): 117- 122, 2009.

[19] Xu Sen and Huang Tser Chin, “Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions”, 3rd International Symposium on Wireless Communication Systems, Page(s):185-189, 2006.

[20] Altaf A., Javed M.Y. and Ahmed A., “Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005”, 9th IEEE ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Page(s): 335-339, 2008.

[21] Kambourakis Georgios, Konstantinou Elisavet and Gritzalis Stefanos, “Revisiting WiMAX MBS security”, Elsevier Journal of Computers & Mathematics with Applications, Advances in Cryptography, Security and Applications for Future Computer Science, Vol.: 60, Issue: 2, Page(s) 217-223, 2010.

[22] Xu Sen, Huang Tser Chin and Matthews M. Manton, “Secure Multicast in WiMAX”, Journal of Networks, Vol.: 3, Issue: 2, Page(s): 48-57, 2008.

[23] Kwon Bongkyoung, Lee P. Christopher, Chang Yusun and Copeland A. John., “A Security Scheme for Centralized Scheduling in IEEE 802.16 Mesh Networks”, IEEE Conference on Military Communications, Page(s): 1-5, 2007.

[24] Kwon, Bongkyoung, Raheem A. Beyah, and John A. Copeland, “Key Challenges in Securing WiMAX Mesh Networks”, Security and Communication Networks, Vol.: 2, Issue: 5, Page(s): 413-426.

[25] Shon Taeshik, Koo Bonhyun, Park Hyuk Jong and Chang Hangbae, “Novel Approaches to Enhance Mobile WiMAX Security”, EURASIP Journal on Wireless Communications and Networking, 2010.

[26] Liu Fuqiang and Lu Lei, “A WPKI-Based Security Mechanism for IEEE 802.16e”, International Conference on Wireless Communications, Networking and Mobile Computing, Page(s): 1-4, 2006.

[27] Zaabi Al J., Chilamkurti N., Zeadally S. and Kim Jongsung, “A Proposed Authentication Protocol for Mobile Users of WiMAX Networks,” 3rd IEEE International Conference on Human-Centric Computing, Page(s): 1-6, 2010.

[28] Tian, Haibo, Liaojun Pang, and Yumin Wang, “Key Management Protocol of the IEEE 802.16e”, Journal of Natural Sciences, Vol.: 12, Issue: 1, Page(s): 59-62, 2007.

[29] Li Ruixue, Fang Zhiyi, Xu Peng, Xiao Wei and Wang Wei, “Experimental Research on a New Authentication Protocol for Wireless Communication Network Based on WiMAX”, 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Page(s): 1-4, 2008.

[30] Huang Chin-Tser, and Chang Morris J., "Responding to Security Issues in WiMAX Networks", IEEE IT Professional Journal & Magazine, Vol.: 10, Issue: 5, Page(s): 15-21, 2008.

[31] Zhou Yun and Fang Yuguang, "Security of IEEE 802.16 in Mesh Mode", IEEE Conference on Military Communications, Page(s): 1-6, 2006.

[32] Bogdanoski Mitko, Latkoski Pero, Risteski Aleksandar and Popovski Borislav , "IEEE 802.16 Security Issues: A Survey", 16th Telecommunications Forum, Page(s): 199-202, 2008 .

[33] Nasreldin Mahmoud, Asian Heba, El Hennawy Magdy and El Hennawy Adel, "WiMAX Security", 22nd IEEE International Conference on Advanced Information Networking and Applications - Workshops, Page(s): 1335-1340, 2008.

[34] D. Curtis Schleher, "Electronic Warfare in the Information Age", Artech House, 1999.

[35] Wenyuan Xu, Ke Ma, Trappe Wade and Zhang Yanyong, "Jamming Sensor Networks: Attack and Defence Strategies", IEEE Network Journal & Magazine, Page(s): 41-47, 2006.

[36] Ioannis Broustis, Konstantinos Pelechrinis, Dimitris Syrivelis, Srikanth V. Krishnamurthy and Leandros Tassiulas, "A software framework for alleviating the effects of MAC-aware jamming attacks in wireless access networks", Springer Wireless Network, Page(s): 1543-1560, 2011.

[37] Chi Wen Po and Lei Laung Chin, "A Prevention Approach to Scrambling Attacks in WiMAX Networks", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, Page(s): 1-8, 2009.

[38] Li Juan and Haggman Sven Gustav, "Performance of IEEE 802.16-2004 Based System in Jamming Environment and its improvement with Link Adaptation", 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Page(s): 1-5, 2006.

[39] Makarevitch Boris, "Jamming Resistant Architecture for WiMAX Mesh Network", IEEE Military Communication Conference, Page(s): 1-6, 2006.

[40] Jormakka Jorman and Jormakka Henryka, “Antenna Selection for Brigade Level Headquarter Use of WiMAX”, IEEE Military Communication Conference, Page(s): 1-7, 2007.

[41] Yikun Huang, Tidd Will, Olson Andy and Wolff Richard S, “A Compact Smart Antenna for WiMAX Radio”, IEEE Symposium on Mobile WiMAX, Page(s): 169-173, 2009.

[42] DeBruhl Bruce and Tague Patrick, “Digital Filter Design for Jamming Mitigation in 802.15.4 Communication”, IEEE Computer Communications and Networks, Page(s): 1-6, 2011.

[43] Liu Hongbo, Liu Zhenhua, Chen Yingying and Xu Wenyuan, “Localizing Multiple Jamming Attackers in Wireless Networks”, IEEE International Conference on Distributed Computing Systems, Page(s): 517-528, 2011.

[44] Jung Junwoo, Jeung Jaemin and Lim Jaesung, “Control Channel Hopping for Avoidance of Scrambling Attacks in IEEE 802.16 Systems”, IEEE Military Communications Conference on Cyber Security and Network Operations, Page(s): 1225-1230, 2011.

List of Publication

1. **Bhardwaj Tanu and Saini Hemraj**, “Effective Detection of Jamming in WiMAX Communication System”, IEEE International Conference on Recent Advances & Innovations in Engineering, 2014.