



Issues In WiMax Handover

Badar Munir kamal 830227-4454

badar_kamal@hotmail.com

Mukhtar Muhammad Yasir 800315-3437

its_yasir@hotmail.com

This report is presented as a part of the thesis for the
Degree of Master of Science in Electrical Engineering

Blekinge Institute of Technology
School Of Engineering
June 2009

Supervisor : Popescu Alexandru

Examiner : Popescu Alexandru

ACKNOWLEDGMENT

We want to thank Mr. Alexandru Popescu for guiding us through the thesis and the time and patience he showed towards us for the completion of this document. We also want to thank all staff and members of BTH for all the knowledge we collected through their interest and hardwork done until the graduation process.

Last but not the least we want to acknowledge the support given by Mikael Asman and Lina Magnusson during all study period.

ABSTRACT

WiMax, the Worldwide Interoperability for Microwave Access is a new technology dealing with provision of data over long distance using wireless communication method in many different ways. Based on IEEE 802.16 WiMax is claimed as an alternative broadband rather than cable and DSL. In our thesis study we will find out the phenomenon and factors involved in WiMax handover and their effect on overall quality of service. We also intend to look into the solutions possible for those problems effecting WiMax QoS in handover. Handover is the main theme of wireless technology and it makes interoperability between different network technologies and provides mobility. However there are some problems during handover and the problem in our focus will be handover delay. Handover delay if longer than expected makes the communication faulty and introduces errors and packet loss which in turns degrade QoS in WiMax.

Motivation

A significant lift up in the Broadband Wireless Access networks as the requirement for broadband and mobile services has got into demand in last few years. Broadband Wireless Access is gradually acquiring a good deal of reputation as an alternative technology to DSL and cable modems.

There is a large number of existing technologies for wireless transmission. These technologies are distributed over different families of networks with respect to the scale of the network, examples of such technologies are PAN, WLAN, WMAN and WAN. With the addition of sophisticated services in mobile wireless and internet world high data rate is the focus demand of wireless deployments. The technologies which promise a high data rate are the core attraction for vendors as well as operators. One of the most promising technologies in this area is WiMAX.

With the start of broadband wireless access network (BWAN) technology, mobile high-speed data service is more in demand then ever. IEEE standard, called 802.16d, was released in 2004, which defines wireless access but was fixed. Which means that user device is supposed to be in a specific geographical area. More recently, the alteration of 802.16d specification addresses the issue of mobility.

Earlier standards defined for wireless broadband systems offer fixed or nomadic access which means there is no handover when user device moves between different cells (or access points)of the network.

LIST OF ABBREVIATIONS

- 3GPP** Third Generation Partnership Project
- 3GPP2** Third Generation Partnership Project 2
- AAA** Authentication, Authorization, and Accounting
- AC** Admission Control
- AF** Application Function
- AK** Authorization Key
- AKA** Authentication and Key Agreement
- AK SN** - Derivation from PMK and PMK2 SN
- AM** Authorization Module
- APC** Anchor paging Controller
- APCF** Anchor paging controller function
- API** Application Program Interface
- AR** Access Router
- ARQ** Automatic Retransmission Request
- AS** Authentication Server
- ASN** Access Service Network
- ASP** Application Service Provider
- BE** Best Effort
- BS** Base Station
- BSID** Base Station Identifier
- CCoA** Collocated Care of Address
- CID** Connection Identifier

COA Change of Authority

CoA Care of Address

COS Class of Service

CS Convergence Sublayer

CSN Connectivity Service Network

DAD Duplicate Address Detection

DHCP Dynamic Host Configuration Protocol

DL Down Link

diffserv Differentiated services

DNS Domain Name Service

DoS Denial of Service

DP Decision Point, Data Path

DSL Digital Subscriber Line

EAP-PSK Extensible Authentication Protocol - Pre Shared Key

EAP-SIM EAP Subscriber Identity Module to be used with SIM

EMSK Extended Master Session Key

FA Foreign Agent

FBSS Fast Base Station Switching

FRD Fast Router Discovery

FWA fixed wireless access

GPRS General Packet Radio Services

GRE Generic Routing Encapsulation

GSA Group Security Association

GW Gateway

HA Home Agent

HO Handoff

HoA MS Home Address

HSDPA High Speed Downlink Packet Access

HTTP HyperText Transfer Protocol

IE information elements

IEEE Institute of Electrical and Electronics Engineers

IID Interface Identifier

IP Internet Protocol

IPsec IP Security

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

LBS Location Based Services

LSB Least Significant Byte

MAC Medium Access Control

MDHO Macro Diversity handoff

MIP Mobile IP (Refers to both Mobile IPv4 and Mobile IPv6)

MIP6 Mobile IP version 6

MM Mobility Management

MMS Multimedia Messaging Service

MS Mobile Station

MSID Mobile Station Identifier

MSK Master Session Key

NA Neighbor Advertisements

NAI Network Access Identifier

NAP Network Access Provider

NAS Network Access Server

NAT Network Address Translation

NMS Network Management System

NRM Network Reference Model

NS Neighbor Solicitation

NSP Network Service Provider

PA Paging Agent

PC Paging Controller

PDG Packet Data Gateway

PDU Packet Data Unit

PKM Privacy Key Management

PoA Point of Attachment

PtP Peer to Peer

QoS Quality of Service

RA Router Advertisement

RP Reference Point

RRA Radio Resource Agent

RRC Radio Resource Controller

RRM Radio Resource Management

SA Security Association

SFA Service Flow Authorization

SFID Service Flow ID

SHO Soft Hand Off

SI Subscriber Identity

SLA Service Level Agreement

SMTP Simple Mail Transport Protocol

SNMP Simple Network Management Protocol

SS7 Signaling System 7

SSL Secure Sockets Layer

SS Subscriber Station

TBS Target BS

TCP Transmission Control Protocol

TE Terminal Equipment

UID user-identity

UMTS Universal Mobile Telecommunications System

VLAN Virtual LAN

VoIP Voice over IP

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

Wi-Fi Wireless Fidelity, refers to 802.11 standards, including 802.11b, 802.11a, and 802.11g

WLAN Wireless local area network based on IEEE 802.11 and related standards

LIST OF FIGURES

FIGURE 1.1	18
FIGURE 1.2	19
FIGURE 1.3	21
FIGURE 1.4	23
FIGURE 1.5	24
FIGURE 1.6	26
FIGURE 1.7	27
FIGURE 1.8	29
FIGURE 2.1	33
FIGURE 2. 2	35
FIGURE 2. 3	37
FIGURE 2. 4	38
FIGURE 2. 5	39
FIGURE 2. 6	40
FIGURE 2. 7	40
FIGURE 3.1	45
FIGURE 3. 2	46
FIGURE 3. 3	47
FIGURE 3. 4	48
FIGURE 3. 5	50
FIGURE 3. 6	51
FIGURE 3. 7	52
FIGURE 3.8	53
FIGURE 3.9	54
FIGURE 3.10	55
FIGURE 3.11	56
FIGURE 3.12	57
FIGURE 4.1	61
FIGURE 4.2	62
FIGURE 4.3	63
FIGURE 4.4	66
FIGURE 4.4	68

TABLE OF CONTENT

ACKNOWLEDGMENT	8
ABSTRACT	9
Motivation	10
LIST OF ABBREVIATIONS	11
TABLE OF CONTENT	17
Chapter 1	19
INTRODUCTION	19
Introduction	20
1.1 Mobile WiMax Networks	23
1.1.1 Orthogonal Frequency Division Multiple Access (OFDMA)	24
1.1.2 IEEE 802-16e-2005 MAC Layer	27
1.1.3 Duplex Techniques	30
1.1.4 Mobility Management in 802.16-2005	31
1.2 RF Frequencies for WiMAX	31
CHAPTER 2	33
WIMAX NETWORK ARCHITECTURE	33
Mobile WiMax Network Architecture	34
2.1 Architecture Design Principles	34
2.2 Network Reference Model	35
2.2.1 Reference Points	36
2.2.2 Access Service Network (ASN)	37
2.2.3 Connectivity Service Network (CSN)	39
2.3 Protocol Layering	41
2.4 Discovery And Selection of Network	42
2.4.1 NAP Discovery	43
2.4.2 NSP Discovery	43
2.4.3 NSP Enumeration And Selection	43
2.4.4 NSP Attachment	43
2.5 IP Addressing	43
CHAPTER 3	45
MOBILITY MANAGEMENT	45
Mobility Management	46
3.1 Power Management	46
3.1.1 Awake mode	46
3.1.2 Sleep mode	47
3.1.3 Idle mode	49
3.2 Handover	51
3.2.1 Hard handover (HHO)	53
3.2.2 Macro diversity Handover (MDHO)	54
3.2.3 Fast Base Station Switching (FBSS)	55
3.3 Process of Handover	57
3.3.1 Cell Re-selection	57
3.3.2 Handover Decision and Initiation	58
3.3.3 Synchronization with the target BS	58

3.3.4 Ranging	59
3.3.5 Re authorization	59
3.3.6 Re registration	60
3.3.7 Termination of MS context with previous BS	60
CHAPTER 4	61
SOLUTION FOR HANDOVER PROBLEM	61
Fast Handover Schemes and Solutions of Problems causing Handover delay	62
4.1 Handover Topology	62
4.2 Redundancies in MAC Layer Handover Process	66
4.3 Cost-Effective Target BS Selection Scheme	67
4.4 Fast Ranging and Pre-registration	69
4.5 Security Issues in WiMax	70
4.6 Loop holes in WiMAX security and Their Solutions	70
PHY layer problem	70
Threats to the MAC layers	71
Conclusion	73
Future Work	73
References	74

Chapter 1

INTRODUCTION

Introduction

Now a days there exists number of wireless technologies and a lot are under rapid development, Based on the network scale technologies they fall under different network families in the figure 1.1 is shown wireless technologies

Bluetooth, Zigbee, RFID are some examples of Personal Area Network. The range in such network is mostly 10 meters but in some cases it can be more, PAN devices work in range of 2.4 GHz .

For computer devices like itself computers, printers, scanners etc Local Area Network is used for communication in small area like home, office. Hardware like hubs, cables, NIC used for local area network is inexpensive comparatively.

As the name states Metropolitan Area Network provides coverage upto several kilometers usually MAN is comprised of number of LANs. It can be for a large campus or a university area. Number of MAN can be connected to WAN.

Wide area network is a network which is comprised of number of LANs and WANs. It allows users of one area to connect with the users of other area. Number of switches and routers are used in WAN. Present example of WAN is internetwork.

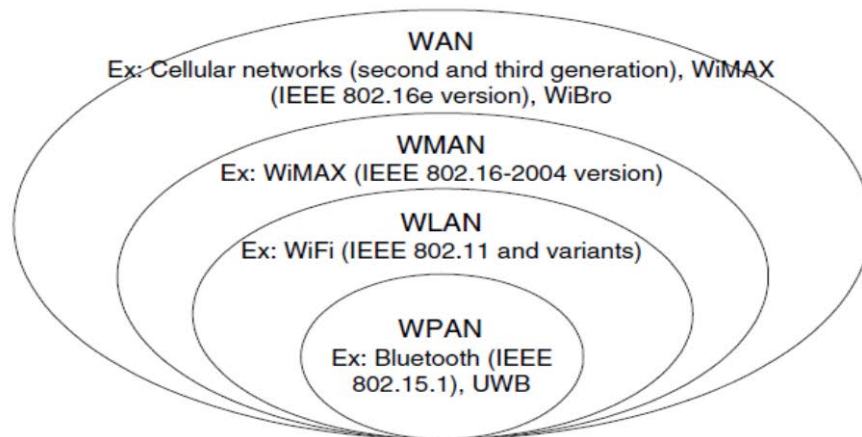


Figure 1.1 classical representation of wireless technologies[1].

Broadband wireless access system are well known high data rate wireless MAN in which data rate is in mega bits per second which is its significant feature. In the beginning BWA applications had high data rate but fixed position the usage could be the application of huge data rate i-e TV, internet and video on demand etc. Actually it was not mobile but the initial target was of wireless DSL.

IEEE 802.16 standard first came in year 2001 and later it was published in year 2006. way before this time there always was a need for wireless broadband and before 1990 many companies were using proprietary wireless broadband equipment but those products were not interoperable . when IEEE 802.16 standard came these products were claimed that they are based on 802.16 standard but wimax interoperability test was started in 2006 so it was not possible to verify later these products were called pre-wimax systems.

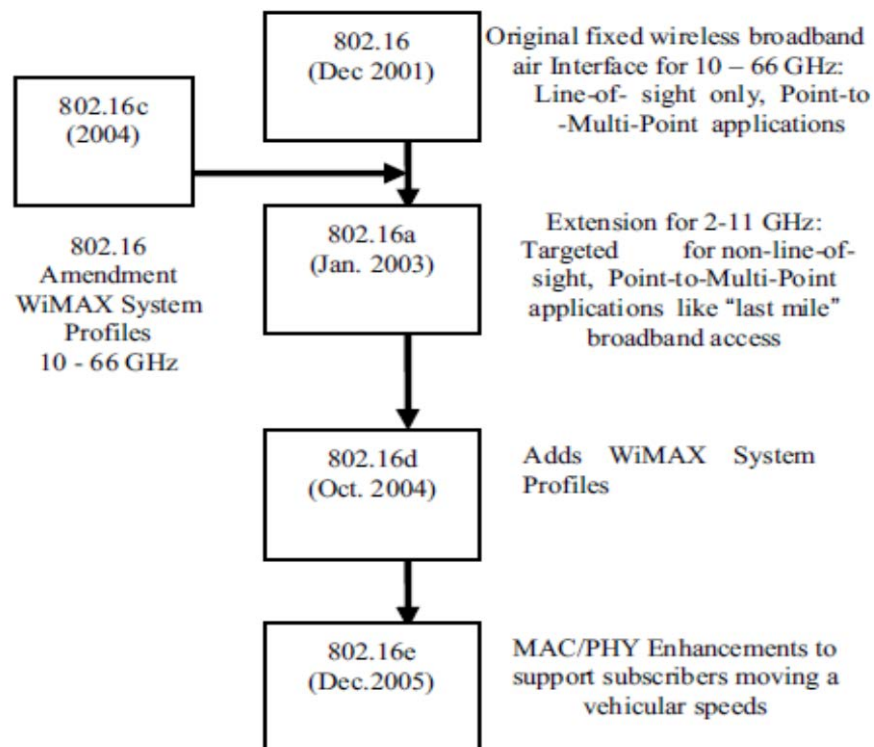


Figure 1.2: Evolution of IEEE 802.16 [3]

WiMAX stands for “Worldwide Interoperability for Microwave Access” and is a well known technology in telecommunication in different ways which provide wireless data, varies from [point-to-point](#) links to full mobile cellular type access [2]. Depending on [IEEE 802.16](#) standard WiMax is considered as an alternative to DSL and cable technologies and its name was given by WiMax forum. The WiMax forum was formed in June 2001 for the promotion of standards for conformance and interoperability. The WiMax supports voice, video as well as other digital data like internet. The cell radius of WiMax typically has a coverage area of three to ten kilometers radius. The standard WiMAX Forum Certified™[3] have normally a capacity of up to 40 Mbps per channel both for fixed and portable access. Whereas deployments concerning Mobile networks are expected to provide radius of three kilometers coverage area and is able to provide upto 15 Mbps capacity [3]. Extra channels can be added in case of increase in demand of bandwidth.

Wimax works in the same manner as WiFi but the difference between them is high speed, larger distance and large number of users in case of WiMax [4] thus making it possible for the areas having no or less coverage of internet and telecommunication.

Considering a typical WiMAX system, it consists of two main constituents, a WiMax tower or transmitter and a WiMax receiver. The WiMax receiver and antenna can be present in a shape of stand alone equipment or integrated inbuilt equipment inside the target usage equipment just like WiFi equipment.[1]

A high bandwidth wired connection e.g. a T3 line is normally used in order to directly connect the WiMax tower to the internet. For interconnection between different WiMax towers in line of sight the microwave link can also be used, in such a case the connection is known as backhaul. This refers to two types of wireless communication in case of WiMax i.e. line of sight and non line of sight service. The non line of sight service occurs at the user end where a small inbuilt receiver antenna is present inside the stand alone WiFi Receiving module or inbuilt receiving module as well. The non line of sight mode utilizes low frequency range i.e. 2 – 11 GHz. The known purpose of using lower wave length is to avoid disruption in case of obstacles, the waves in return get better ability to turn and diffract.[1]

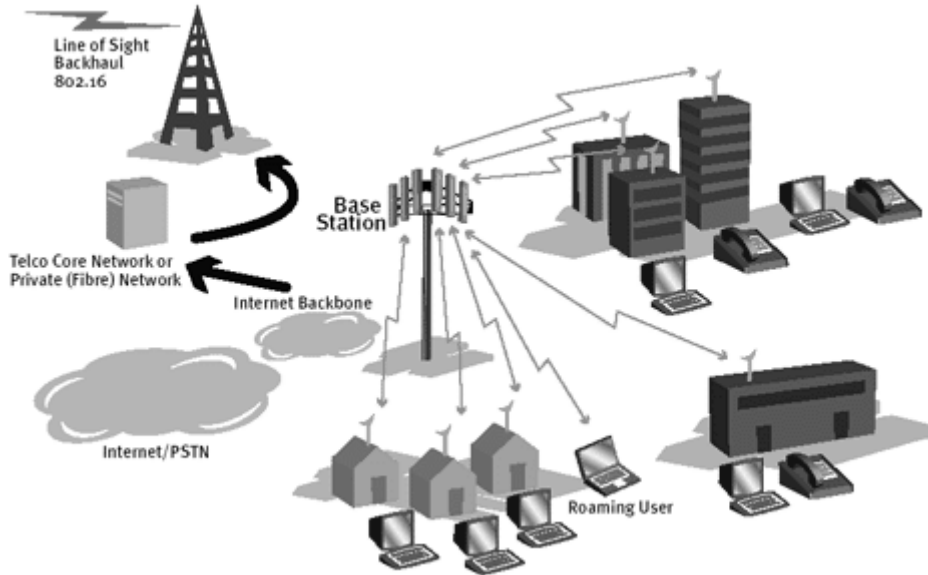


Figure 1.3 WiMax network [4]

1.1 Mobile WiMax Networks

Physical and MAC layer properties of mobile WiMax 802.16e-2005 are introduced in this part of chapter. Handover mechanism and quality of service Qos are discussed at basic level because mobility and handover has its own dedicated chapter later in this report. To keep the context right some of the matters which play important role in the making of WiMax mobile are discussed here. Most part of this chapter is based on references.

Three various physical layers are defined by 802.16e specification which are : Single-carrier transmission, OFDM (Orthogonal Frequency Division Multiplexing) and OFDMA (Orthogonal Frequency Division Multiple Access). Among these physical technologies, OFDMA is used mobile services in WiMax.[5]

1.1.1 Orthogonal Frequency Division Multiple Access (OFDMA)

Mobile WiMax has scalable FFT size from 128 to 2048 when a bandwidth is increased the FFT size also increases respectively whereas the spacing of subcarrier is 10.94KHz. Due to the OFDM duration of symbol scaling has reduced effect on higher layers, Scalability factor keeps the cost low. In mixed environment of fixed and mobile wimax, spacing of 10.94KHz is a balance between delay and Doppler spread. When operating at 3.5GHz at speed of 125 Km/h subcarrier supports 20 micro seconds delay spread values. Mobile WiMax can have more bandwidth profiles but following FFT are used (128, 512, 1024, 2048) with respect to the bandwidth (1.25MHz, 5MHZ, 10MHz, 20MHz).[6]

<i>Parameter</i>	<i>Values</i>			
Channel bandwidth (MHz)	1.25	5	10	20
FFT size (N_{FFT})	128	512	1024	2048
Subcarrier frequency spacing	10.94 kHz			
OFDMA symbol duration ($T_s = T_b + T_g$)	102.9 μs			
CP time ($T_g = T_b/8$)	11.4 μs			
Useful symbol time (T_b)	91.4 μs			

Table 1.1 : OFDMA parameters [8]

As compared to CDMA (Code Division Multiple Access) OFDMA (Orthogonal Frequency Division Multiple Access) has both advantages and deficiencies. In OFDMA there is tolerance to fading and efficiency is a lot better. In both Uplink and Downlink channels various users are combined. On the the other hand manufacturing is expensive and CCI (Co Channel Interference) is more which can be reduced by using Fractional Frequency Reuse.

When managing various devices and different type of antennas, OFDMA provides flexibility to mobile WiMax. Factors which are necessary for mobile devices like omni directional antenna and NLOS (non line of sight) features, OFDMA reduces interference for user devices. These factors provide operator with more flexibility for managing the bandwidth and transmit power.[7]

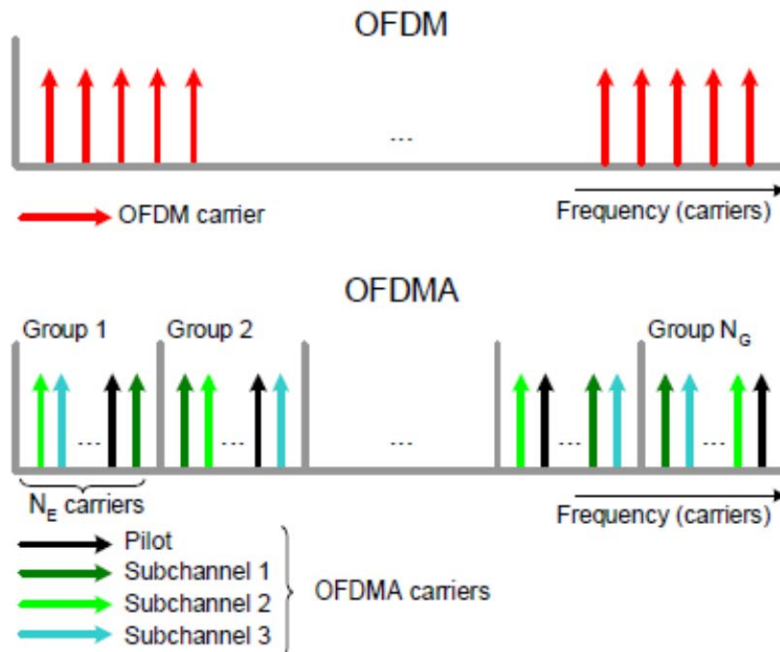


Figure 1.4: OFDM and OFDMA [7]

Carriers are transmitted in parallel and at same amplitude in OFDM, which then divides the carrier in N_G groups, each N_G group has N_E carriers. While in OFDMA when using 2048 FFT for downlink $N_E = 32$ and $N_G = 48$ and in uplink N_E is same and $N_G = 53$. for every sub channel modulation ,coding and amplitude are different.[7]

The scalable Orthogonal Frequency Division Multiple Access (SOFDMA) gives more advantages over OFDMA. To keep the constant carrier spacing among the bandwidth of different channels it scales the size of FFT to the channel bandwidth. Due to which the efficiency of spectrum is high in wide channels and cost is low in narrow channels.[7]

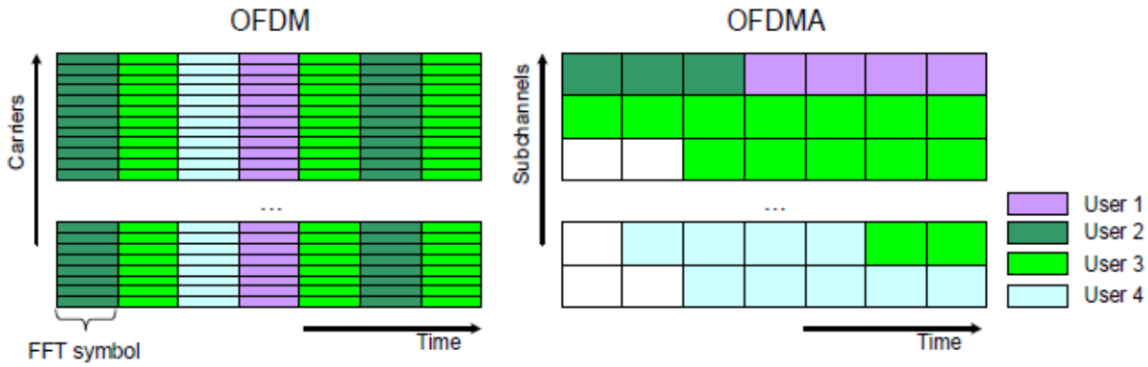


Figure 1.5 OFDM & OFDMA uplink [7]

1.1.1-a Cyclic Prefix

A cyclic prefix is sent during the guard time. The purpose of this extra transmission is to resolve echoes from multipath effects before the actual data to be processed.

Other payback obtained using a CP includes frequency domain equalization and prevention from inter block interference.

1.1.1-b OFDMA Symbol Structure

There are three types of sub-carriers in OFDMA symbol data sub-carrier, pilot sub-carrier and null sub-carrier.

Data subcarrier is responsible to handle data transmission while pilot sub-carrier are used for synchronization and estimation purposes while processing and null sub-carrier are sent for guard periods and DC currents but they have no transmission. Following figure explains the structure of an OFDMA symbol.

1.1.1-c Other Improved features of WiMAX physical layer

There are some other improvements in physical layer of Mobile WiMAX. It uses adaptive modulation and coding like 16QAM, 64QAM, Convolution turbo codes and block turbo codes.

It also uses Fast feedback channel technique.

Hybrid automatic repeat request is also a salient improvement used. In this way it is versatile in data ranges, reliable in transmission and in connection performance.

1.1.2 IEEE 802-16e-2005 MAC Layer

To provide an interface between physical layer and higher layers is the key role of MAC layer. MAC layer of Mobile WiMAX takes data from physical layer in form of data packets called MAC service data units and before sending these data units to higher layers these are organized to MAC Protocol data units (PDU).

WiMAX provides two mechanisms for air interface Point-to-Multipoint networking and mesh networking.

1.1.2-a Addressing

Point-to-Multipoint

In Point-to-Multipoint networks every air interface is given a unique MAC address. The address is used with initial ranging processing and in addition with authentication process connection between MS and BS is identified with CID, s. Connection are available for three different QoS levels

- Basic is intended to use for short and urgent time message services
- Primary can be used for long and more delay tolerant services
- Secondary connection is used for standard based messaging services which are more delay tolerant than any of above two service types

Mesh

Mesh networks also use MAC address, but in this case authentication is not a matter of concern. Here the node and the network identify each other. After knowing each the node

receives a node Identifier from the mesh BS. Additionally the nodes create Link Identifiers between neighboring nodes.

MAC Protocol Data Unit format

PDU, s begins with generic MAC header file with a fixed length. Pay load and CRC follows this header. The format is shown in diagram

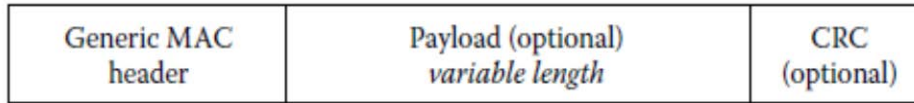


Figure 1.6: MAC protocol data unit format

1.1.2-b Quality of Service (QoS) Support

Due to the unpredictable characteristics of wireless network , to promise a quality of service (Qos) is was more difficult as compared to wired networks. Scheduling and bandwidth adaptation are the methods which are adopted for efficient use of wireless resources.

Qos is provided in WiMax at MAC level , which uses the concept of flow of service which provides signaling mechanism to the uplink and downlink channels. Since BS broadcast messages on downlink channel to all the MS which are registered with it so transmission in downlink is comparatively simple, MS just picks those packets which are specifically sent for it.

Now in the case of with uplink channel, All associated MS transmits to the BS using TDMA mechanism. Time slot is predefined for MS to send data which are managed by BS through uplink MAP. In uplink MAP there are IEs and time slots. BS allocates bandwidth requested by MS and also monitors the Qos for the MS which are currently connected.

Grant Per Connection (GPC) and Grant Per Subscriber Station (GPSS) are two methods used by BS to provide bandwidth to the requesting MS [10]. BS grants bandwidth to the

connection in case of GPC and MS uses the grant only bandwidth. On the other hand in 10 to 66 GHz PHY layer the only allowed method is GPSS, which is more quick to the variations in Qos requirements. The whole bandwidth is given to the MS which should be smart enough to manage the resources for service flows and Qos.

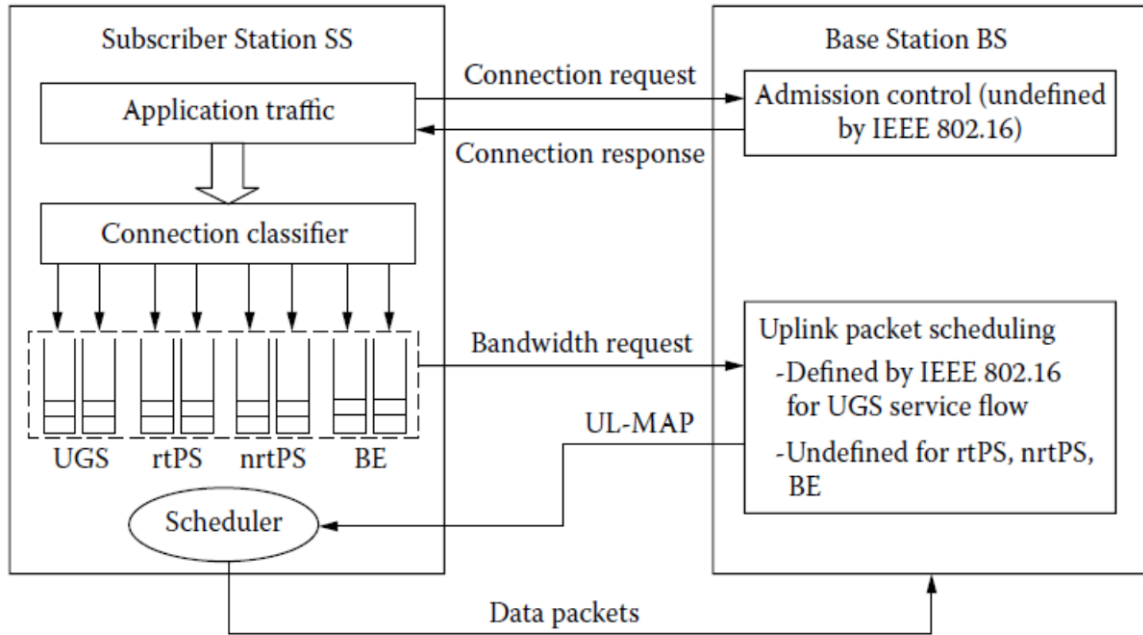


Figure 1.7 : Architecture of Qos [8]

A particular identifier is allocated to every connection by BS. By two or three way handshake process the connections can be created , deleted, and changed through Dynamic Service addition (DSA), Dynamic Service Delete (DSD) , and Dynamic Service Change (DSC). BS has authorization module which performs the activation of service flow.

Admission control is responsible for accepting or rejecting the connection according to the available bandwidth that satisfies the connection and guarantees the required QoS without degrading the QoS for other existing connections. Admission control is not defined in the standard, although many propositions are made by different authors to establish admission control in the BS [11,12,13].

MAC protocol is connection oriented first the connection with BS and other service flows (UGS, rtPS , nrtPS, BE) is established. To setup a connection request and response messages are sent between MS and BS. If the resources are available BS sends back the response message in reply to the request message from MS and connection is established.

1.1.3 Duplex Techniques

There are two types of duplex techniques used in WiMax, TDD (Time Division Duplex) and FDD (Frequency Division Duplex). The brief description is given as follow:

1.1.3-a FDD (Frequency Division Duplex)

Two different channels are used to transmit and receive so MS can transmit and receive at the same time, For this purpose the duration frame used is of fixed size for both the uplink and downlink transmission. Due to this reason the mechanism used for bandwidth allocation is less complicated.

1.1.3-b TDD (Time Division Duplex)

In this technique same channel is used for both the uplink and downlink , figure 1.7 illustrates the decomposition of TDD frame into downlink subframe and uplink subframe. Obviously the bandwidth allocation mechanism is complicated comparatively but TDD has number of advantages that's why this technique is preferred. The design of transceiver for TDD is less complicated so cost is low. TDD only need single channel for both transmitting and receiving so use of resources is efficient ,

Collisions are avoided by Transmit Transition Gap (TTG) and Receive Transition Gap (RTG).

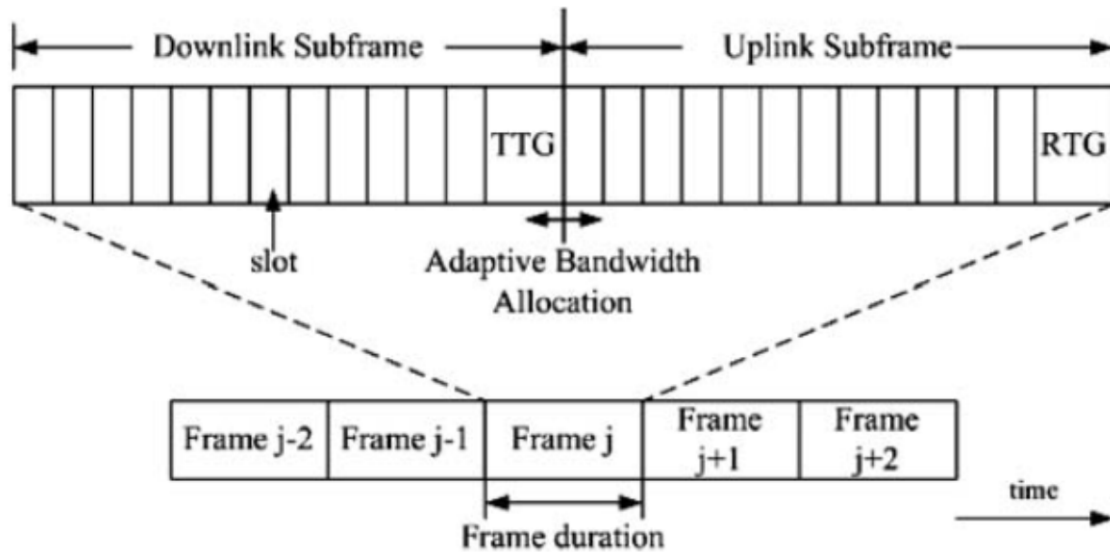


Figure 1.8:TDD frame structure [9]

1.1.4 Mobility Management in 802.16-2005

Mobile WiMAX supports seamless connection handovers up to the speed of 100 km/h [2]. For mobile communications handover process power handling is also an issue.

WiMAX provides two modes for power management,

- Sleep Mode
- Idle Mode

Mobility Issues are addressed in more details in following chapters.

1.2 RF Frequencies for WiMAX

802.16 which is the most recent version of WiMAX has the spectrum range starting from a minimum of 2 GHz up to almost 66 GHz range, which infact is a big range. [14]

The International standard of 3.5 GHz in general, 5.8 GHz USA free spectrum, Licensed spectrum at 2.5 GHz in USA and in other countries is used normally for testing of interoperability.

It is also possible to extend the technology to lower frequencies including the spectrum of valuable 700 MHz range. Most probably the frequencies in the upcoming products will be including 2.3 GHz range (used in Korea and the US) and also the new 4.9 GHz public safety band. The 700 MHz range, partly due to Flarion's technology may also grab some more attraction. The 900 MHz unlicensed bands may also become the point of focus for long term.

CHAPTER 2

WIMAX NETWORK ARCHITECTURE

Mobile WiMax Network Architecture

To have an interoperable wireless network , simply MAC and PHY alone are not enough. The purpose is to deal with the aspects like IP connectivity , Qos, security and mobility management. End to end network aspects are developed and standardized by Network Working Group (NWG) of WiMax forum. Three stage development process has been adopted by WiMax NWG for the development of end to end network architecture.

Stage 1:

List of case scenario and service requirements.

Stage 2:

Architecture that meets the service requirement.

Stage 3:

Details of associated protocols with architecture.

NWG has finished three stages of release 1 and version 4 has come out recently whereas release 1.5 is under development so we are going to discuss stage 2 of release 1 in this chapter.

2.1 Architecture Design Principles

the intention of the NWG was to have an architecture aligned with wired access networks but also with the high speed mobility support. The WiMax architectural design has followed number of tents. Where design principles of IP networks are taken into account. Some important design principles are as follow:

- Functional Decomposition
- Modularity of deployment
- Usage model support
- De coupling of access and connectivity services
- Support for different business models
- Extensive use of IETF protocols
- Incumbent operator service access support

2.2 Network Reference Model

The logical representation of Network Reference Model (NRM) is shown in the figure 2.1. The NRM is decomposed into four logical parts : Mobile Station (MS) , Network Access Provide (NAP) , Network Service Provider (NSP), and Internet .

Reference points are actually conceptual and they represent huge number of protocols same as in IP network interface.

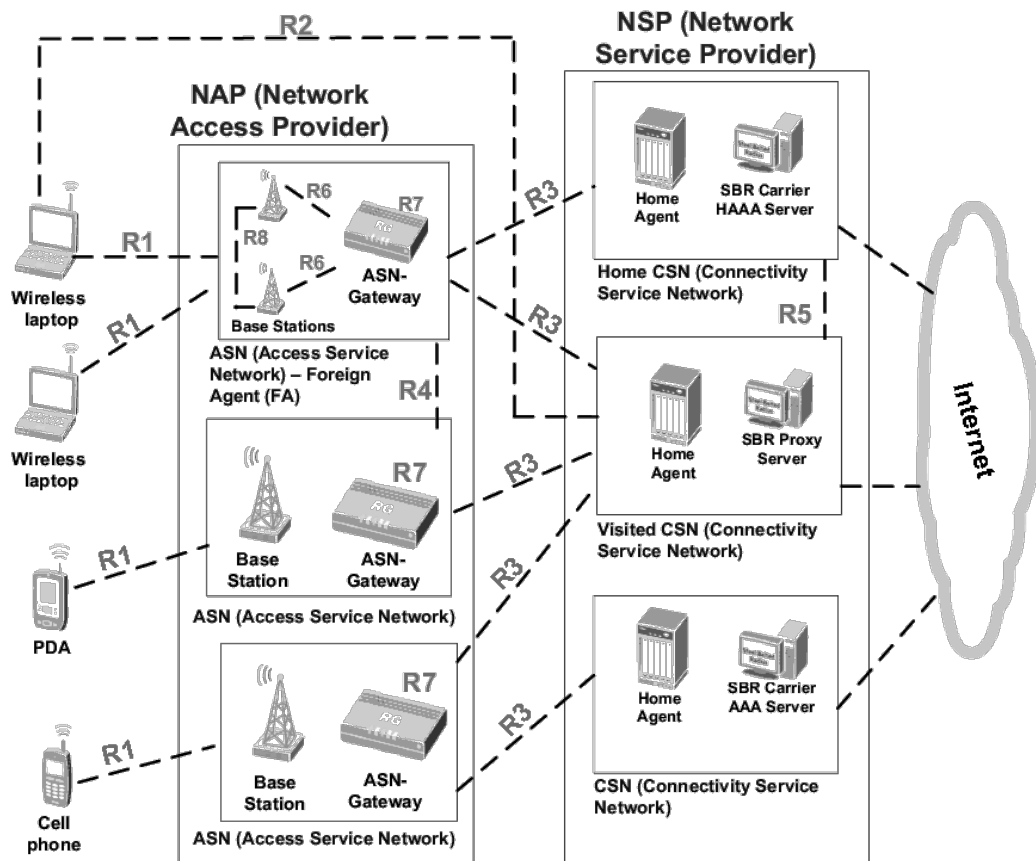


Figure 2.1 : Network Reference Model[15]

- **MS (Mobile Station)**
All subscribers and mobile devices e.g. cellular phones and laptops etc.

- **NAP(Network Access Provider)**

It provides wireless access functionality, consists of BS (Base Station), ASN-GW and FA (Foreign Agent).

- **NSP (Network Service Provider)**

This entity provides IP connectivity, the functions with in NSP are : AAA servers, HA, CSN, Authentication, Authorization, Mobility, IP management.[15]

- **Internet**

Provides connectivity to NSP and internet service to the user.

2.2.1 Reference Points

Reference point as already stated above are, conceptual links, which are number of protocols between functional entities. In the following section reference points which connect different functional entities, are discussed.

- **RF1**

It consists of various protocols and procedures for the air interface between MS and ASN.[15]

- **RF2**

Protocols regarding authentication, authorization , and IP host configuration between MS and CSN[15]

- **RF3**

Is set of protocols between ASN and CSN which support AAA, enforcement of policy and mobility features. Does tunneling to send and receive user data between ASN and CSN.[15]

- **RF4**

Is a link between two ASNs.[15]

- **RF5**

Reference point 5 consists of protocols for internetworking, communication between visited and home CSN.[15]

- **RF6**

Protocol link between BS and ASN-GW.[15]

- **RF7**

Situated in ASN-GW, represents inter gateway communication.

- **RF8**

Link between two base stations. Supporting the criterion of the fast handover.

2.2.2 Access Service Network (ASN)

ASN determines the analytical boundary and it represents the suitable way to the collection of functional entities and congenial flow of messages with the ASN. It also depicts the limit for interoperability for WiMax clients. The connectivity functions and aggregation of functions are comprised by various vendors. ASN has at least one BS (Base Station) and a ANS-GW (Access Service Network Gateway). ASN and MS uses R1 where BS to BS communication is via R8. R3 is shared between ASN and CSN. Between number of ASN-GW, R4 logical reference point is used. One BS can be connected with more then one ASN-GW using R6.

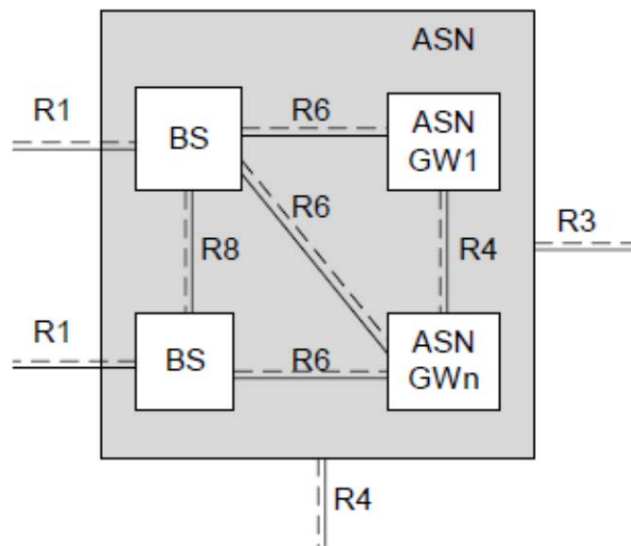


Figure 2.2: ASN reference Model [16]

The functional decomposition of ASN in various profiles is shown in Table 2.1

Functional Category	Function	ASN Entity Name		
		Profile A	Profile B	Profile C
Security	Authenticator	ASN-GW	ASN	ASN-GW
	Authentication relay	BS	ASN	BS
	Key distributor	ASN-GW	ASN	ASN-GW
	Key receiver	BS	ASN	BS
Mobility	Data path function	ASN-GW and BS	ASN	ASN-GW and BS
	Handover control	ASN-GW	ASN	BS
	Context server and client	ASN-GW and BS	ASN	ASN-GW and BS
	MIP foreign agent	ASN-GW	ASN	ASN-GW
Radio resource management	Radio resource controller	ASN-GW	ASN	BS
	Radio resource agent	BS	ASN	BS
Paging	Paging agent	BS	ASN	BS
	Paging controller	ASN-GW	ASN	ASN-GW
QoS	Service flow authorization	ASN-GW	ASN	ASN-GW
	Service flow manager	BS	ASN	BS

Table 2.1 Functional decomposition of ASN. [17]

2.2.2-a BS (Base Station)

BS is a sector which allocates one frequency to the MS while implementing the WiMax interface. With the frequency assignment it also performs other functions which include scheduling for both uplink and downlink, classification of traffic, management of service flow, enforcement of QoS, support for tunneling protocol, passing authentication messages between ASN-GW and MS, receive and deliver TEK and KEK, and loads of other functions. For load balance management a BS can be connected with more than one ASN-GW.

2.2.2-b ASN-GW(Access Service Network Gateway)

ASN-GW is an analytical entity which depicts the collection of control plane functional entities, which can be paired with accordant functions in ASN. Routing and bridging can be performed by ASN-GW.

ASN-GW can be further disintegrated into two functional groups which are DP (Decision Point) and EP (Enforcement Point).

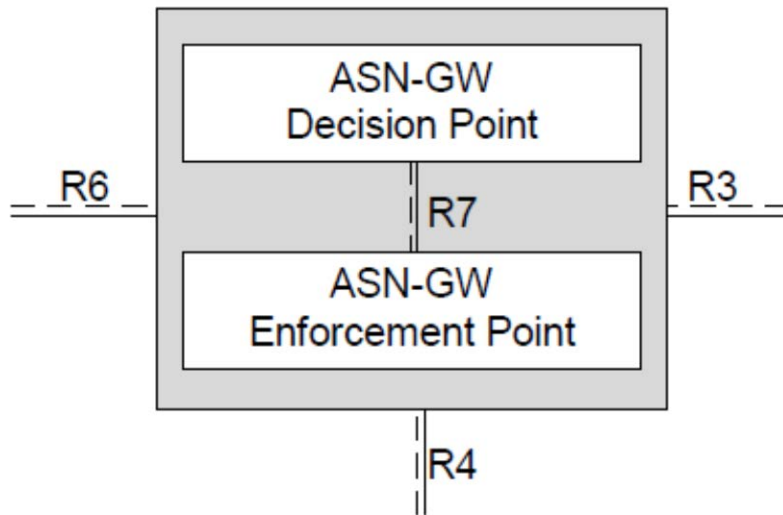


Figure 2.3 Decomposition of ASN-GW [16]

2.2.3 Connectivity Service Network (CSN)

The main purpose of CSN is to deliver IP connectivity to WiMax users. CSN has number of network entities which include AAA server, user database, gateway devices, routers. Figure 2.4 gives the detailed preview of network elements with in. The functions provided by CSN are as follow

- Allocates IP address to MS

- It provides authentication, authorization, and accounting.
- According to the user profile it does admission control.
- Settlement of user billing.
- Tunneling for roaming with in CSN.
- Mobility with in ASN.
- Provides connectivity to WiMax services.

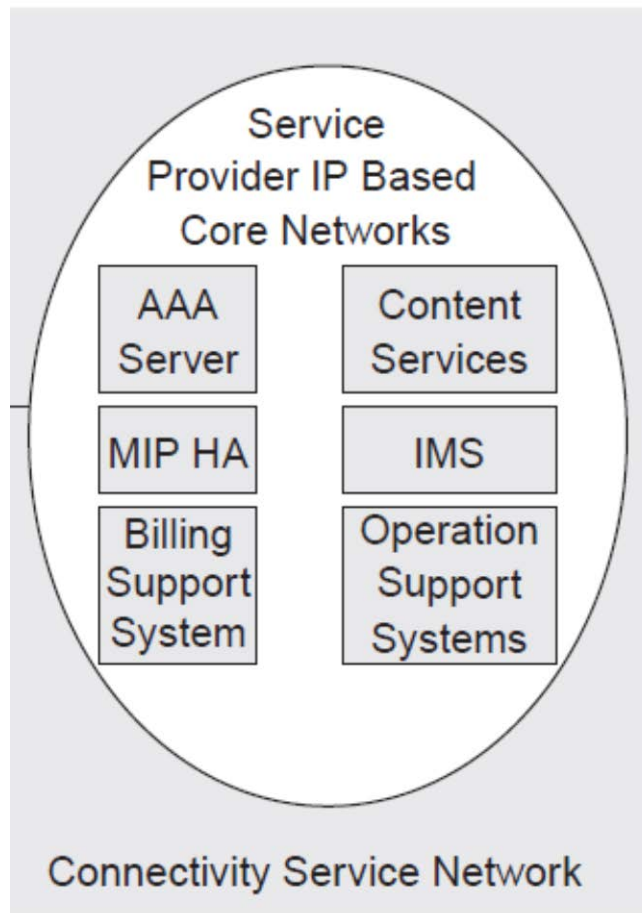


Figure 2.4 : CSN (Connectivity Service Network) [18]

2.3 Protocol Layering

The Wimax architecture has resemblance to the other IP based networks, for the access to IP based service to end user features of link layer are used. ASN is situated in link layer and it provides the link concentration where as CSN gives access to IP based applications and also provides IP address. Through the IP network, links are sent from ASN-GW to CSN. Figure 2.5 gives the logical view of network architecture.

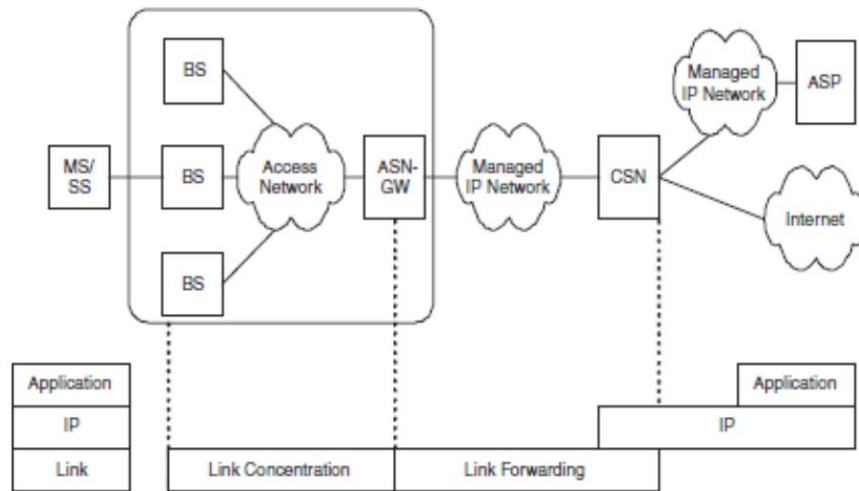


Figure 2.5: Analytical view of WiMax architecture[17]

Now analyzing the Wimax protocol layering as packets are sent from MS to CSN. IP packets are sent by using IP-CS (IP convergence sub layer) or ETH-CS (Ethernet convergence sub layer) on the WiMax network. So now we know that Wimax architecture supports both IP packets and Ethernet packets. IP in IP which are encapsulation protocols can be used routing over ASN.

For better understanding of wimax architecture protocol layering, it is shown in figures. Figure 2.6 shows when using Ethernet convergence sub layer to send IP packets over ASN. Where as when using IP convergence sub layer to send IP packets it is shown in figure 2.7.

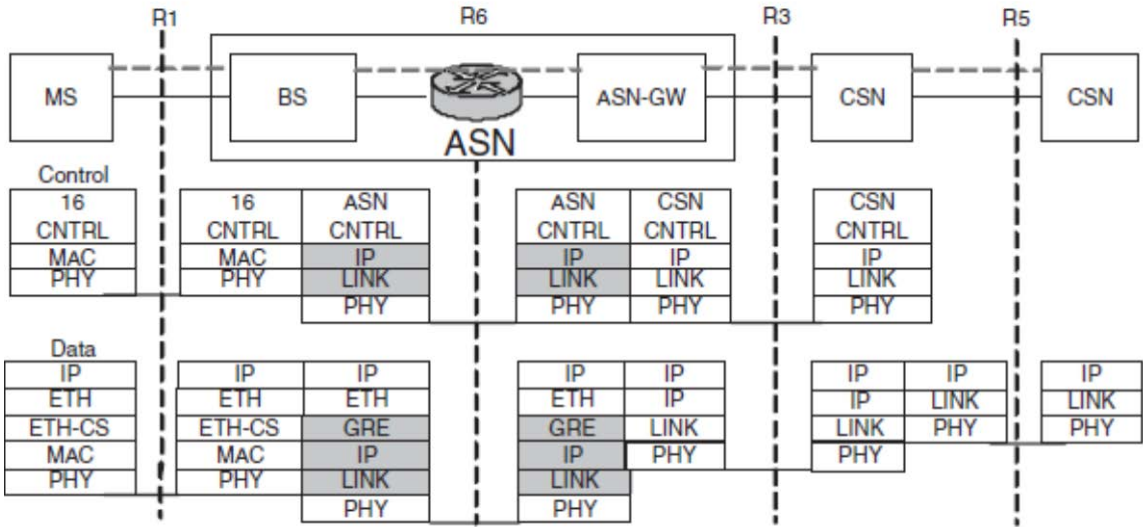


Figure 2.6 Using ET-CS[16]

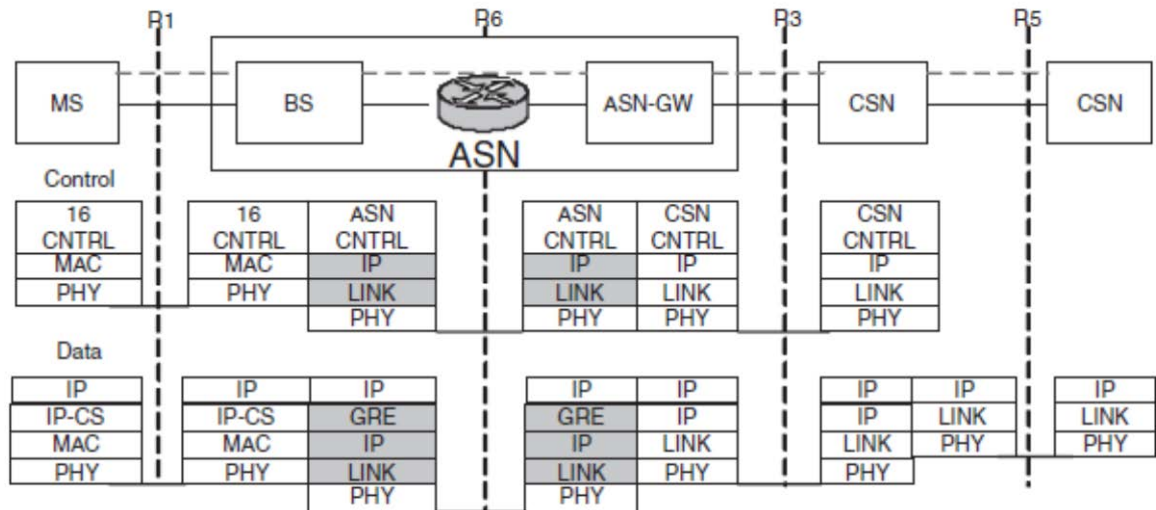


Figure 2.7 Using IP-CS[16]

2.4 Discovery And Selection of Network

Wimax has support for both the manual and automatic network selection for the users choice. In the scenario when number of networks are available in the environment where MS is operating and there are various service providers over the available wimax network. There is a solution given in Wimax standard for network discovery and selection which is comprised of following procedures.

2.4.1 NAP Discovery

The process of Network Access Point discovery makes MS able to find NAP in its coverage area. On the distinguished channel MS scans and decodes the ASN's DL MAP. NAP identifier is of 24 bits value.

2.4.2 NSP Discovery

ASN broadcasts information identity message through which MS finds the available NSP in the list. NSP ID is of 24 bits. Also by using SBC request message, MS can request to BS for NSP ID.

2.4.3 NSP Enumeration And Selection

The selection of NSP can be done automatically or manually. MS makes selection of NSP by using algorithm.

2.4.4 NSP Attachment

When a selection of NSP and ASN affiliated to that NSP is done then MS sends Network Access Identifier (NAI) to specify NSP selection. AAA hop is determined by ASN by using realm part of NAI Message sent by MS.

2.5 IP Addressing

In this section IP addressing is defined for both versions of IP, IP v 4 and IP v 6. To assign IP address PoA to MS, DHCP is used or in other case CSN can assign IP address to ASN which is sent via DHCP to MS. PoA should be assigned to MS when MS itself is an IP gateway. On the other hand IP ETH-CS. [16]

In case of IP v6, MS gets CoA and HoA respectively from ASN and CSN, AR (Access Router) functionality is included in ASN for IP v6 support and MS gets global routing IP address from AR. MS can utilize either CoA or HoA based on its packet routing through CN (Connectivity Node) or HA (Home Agent).[19]

To have an interoperable wireless network, simply MAC and PHY alone are not enough. The purpose is to deal with the aspects like IP connectivity, Qos, security and mobility management.

End to end network aspects are developed and standardized by Network Working Group (NWG) of WiMax forum.

Three stage development process has been adopted by WiMax NWG for the development of end to end network architecture.

The intention of the NWG was to have an architecture aligned with wired access networks but also with the high speed mobility support.

The NRM is decomposed into four logical parts: Mobile Station (MS), Network Access Provide (NAP), Network Service Provider (NSP), and Internet.

Reference points are actually conceptual and they represent huge number of protocols same as in IP network interface.

Reference point are conceptual links, which are number of protocols between functional entities.

ASN determines the analytical boundary and it represents the suitable way to the collection of functional entities and congenial flow of messages with the ASN.

ASN has at least one BS (Base Station) and a ANS-GW (Access Service Network Gateway).

BS is a sector which allocates one frequency to the MS while implementing the WiMax interface.

With the frequency assignment it also performs other functions which include scheduling for both uplink and downlink, classification of traffic, management of service flow, enforcement of Qos, support for tunneling protocol, passing authentication messages between ASN-GW and MS, receive and deliver TEK and KEK, and loads of other functions.

For load balance management a BS can be connected with more then one ASN-GW.

ASN-GW is an analytical entity which depicts the collection of control plane functional entities, which can be paired with accordant functions in ASN.IP packets are sent by using IP-CS or ETH-CS on the WiMax network. IP in IP which are encapsulation protocols can be used routing over ASN. Wimax has support for both the manual and automatic network selection for the users choice.

CHAPTER 3

MOBILITY MANAGEMENT

Mobility Management

As compared to traditional wired technologies use of mobile devices is increased in communication today, due to sufficient data rate provided by new technologies user wants to access the same services as in wired connection i-e web browsing, emails, instant messaging, audio , video streaming no matter where they are. That's why now these services are available on mobile devices like mobile phones, PDA's , Laptops etc. In areas where there is no network architecture mobile network is the quick solution.

There are several requirements for the development of network which supports mobility. The most important requirement is that the device to be used should be able to switch from serving BS when its on the go , which means handoff and communication support even if the user is traveling at high speed.

Limited power resources are another issue for mobile devices, they can carry small amount of charge and has to be charged regularly.

Wimax is a new emerging technology, based on IEEE 802.16 family of standards in access systems, which allows high speed broadband wireless access. This chapter presents types of handover and procedures used during user mobility.

Continuous development for the new standards led to the development of IEEE 802.16 mobile WiMAX. This version is based on amendment 802.16e and provides support for handoff and roaming [1]. The goal of this amendment is to keep the mobile portable devices connected to the MAN. 5, 7, 8.75 and 10 MHz channel bandwidths are covered by mobile WIMAX profile for worldwide licensed spectrum of frequency bands which includes 2.3, 2.5, 3.3 and 3.5 GHz[20].

In WiMAX, mobility management is further classified into following categories. The “macromobility ” refers to the movement of MS between two networks whereas in “micromobility” movement of MS is between two subnets within the same network[21].

3.1 Power Management

Sleep and Awake are two modes defined by IEEE802.16e for MS when registering with the currently serving BS [24]. MS can send and receive data while in awake mode where as in sleep mode MS is unavailable to the BS. For efficient use of power IEEE802.16e defines idle mode[23].

3.1.1 Awake mode

To exchange traffic between MS and BS during awake mode MS and BS performs normal operations. MS can keep connected with serving BS without going through access state. When power is not an issue awake mode is best for the performance.

3.1.2 Sleep mode

Initially MS sleeps for a fixed interval which is also called sleep window and is negotiated between both MS and BS. Sleep window is exponentially increased subsequent sleep periods. MS wakes up and if does not find DL traffic from BS it doubles the sleep window size up to maximum. To maintain connectivity during sleep mode MS listen occasionally to the channel.

Sleep mode was proposed for the reduction of power consumption in MS for improved battery life. According to the (*Four Interrupted Poisson Process*) 4IPP the nature of MS traffic profile is bursty. There are *On* and *Off* periods, during *On* period 4IPP generates packets but not in *Off* period. 4IPP traffic model is shown in figure (3.1) [25]

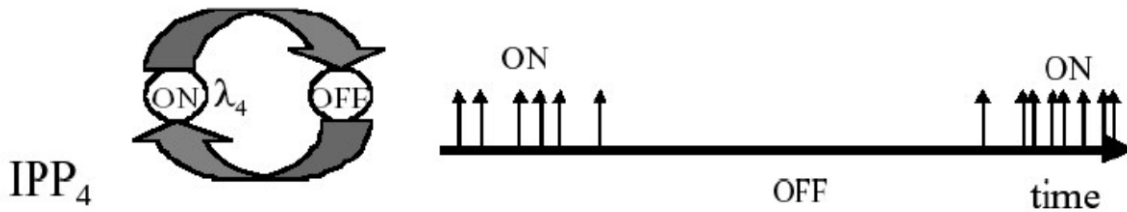


Figure 3.1 : 4IPP Model [25]

The motivation of using sleep mode is given by long idle periods in 4IPP traffic model where MS does not generate traffic, by switching off MS's air interface in idle intervals power can be saved.

The point when MS enters sleep mode until it wakes up is known as *sleep interval*, when MS wakes up it synchronize with the DL transmission and decide whether to stay in awake mode or go back to sleep mode. BS sends signal message when it wants to wakeup MS, This signal message to wakeup the MS is called *paging signal*.

A request message (MOB-SLP-REQ) from MS is sent to BS which actually is permission to enter sleep mode, after the request is received from MS, BS responds with (MOB-SLP-RES) response message. In response message from BS, minimum sleep window (T_{min}), maximum sleep window (T_{max}) and listening window (L) are defined.

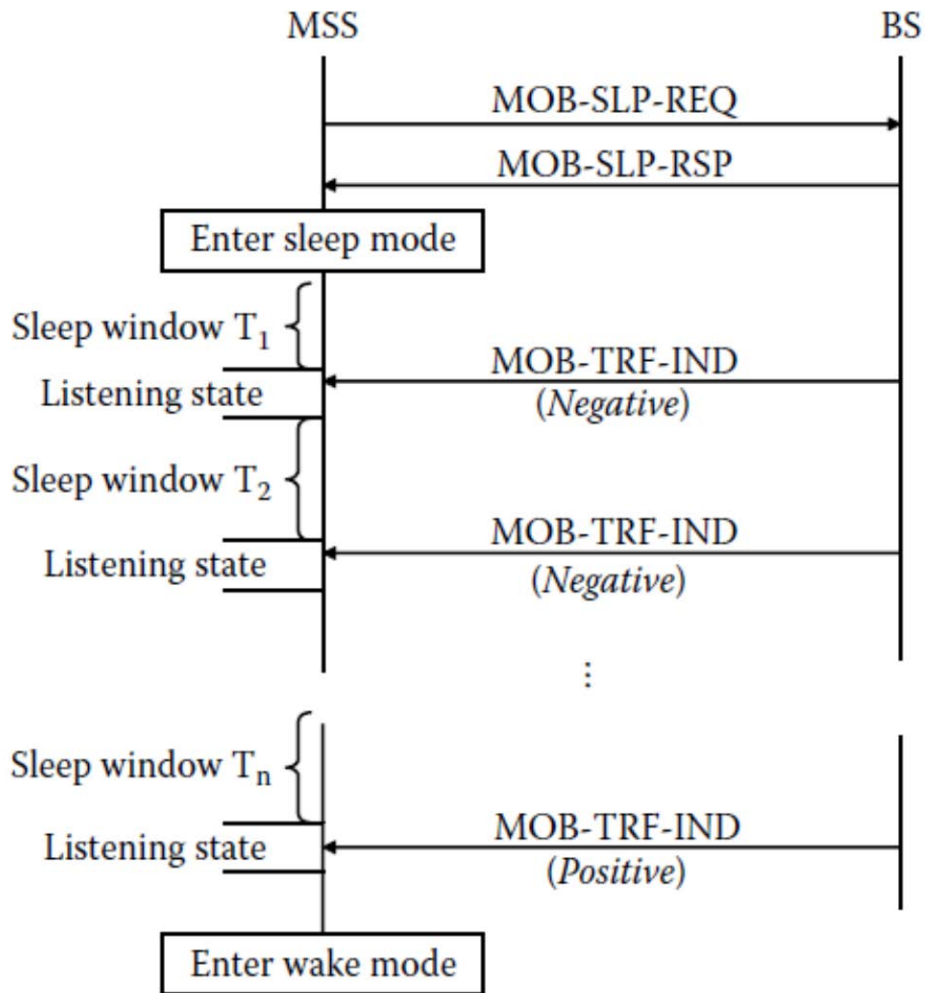


Figure 3.2 : Sleep mode operation sequence
In WiMAX[26]

The time of first sleep interval (T_1) of MS is minimum sleep window (T_{min}). When the time of minimum sleep window is complete MS changes its state and enters listening state (L), if there is traffic indication message (MOB-TRF-IND) which fixed and is equal to the L parameter and was already defined in the (MOB-SLP-RSP) message. If there is no traffic directed to the MS while it was in its first sleep interval (T_1) then MS goes

back to its sleep mode which is exponentially increased, till sleep interval reaches the size of maximum sleep window (T_{max}) . sleep interval in n th cycle is given by:

$$T_n = \begin{cases} T_{min}, & n = 1 \\ \min(2^{n-1} T_{min}, T_{max}), & n > 1. \end{cases}$$

MS during its lifetime stays either in sleep and awake mode, when sleep mode reaches to its time limit it starts listen if there is any traffic addressed to MS while it was in its sleep mode, packets are buffered in BS and are delivered when it wakes up, listen window is settled between MS and BS. In figure 3.3 sleep and awake modes of MS are shown.

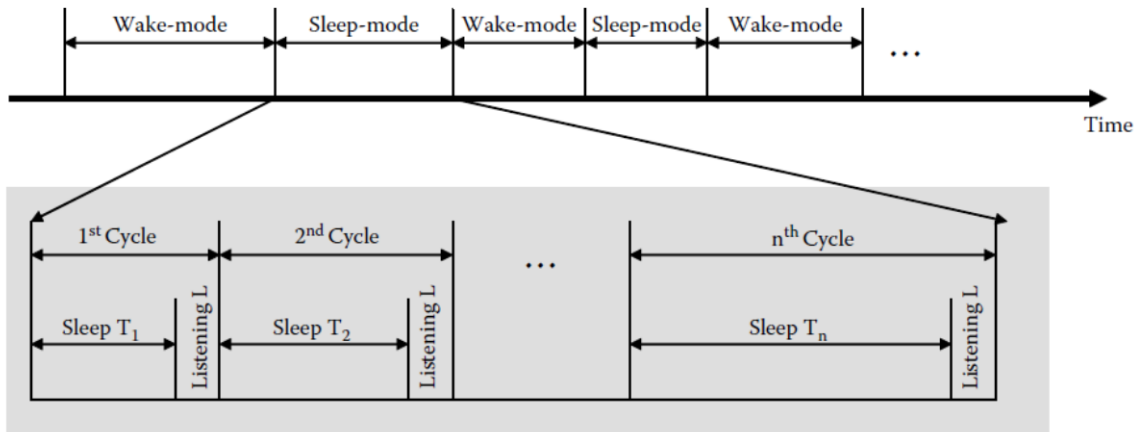


Figure 3.3 WiMAX wake & sleep mode transition [26]

There are three power saving classes and sleep mode operation occurs in one of them.

Sleep mode surely is a solution for power management but on the other hand BS does not transmit to MS when it is entered sleep mode and obviously has a packet delay and has other disadvantage, it may power down those operations which do not need connection with BS.

3.1.3 Idle mode

IEEE 802.16e standard defines idle mode for usage of power in more efficient way. During idle mode MS is available time to time, to receive DL broadcast traffic while it is

not necessary for MS to register with some specific BS. In idle mode MS does not scan at discrete time intervals due to which power and other recourses are saved. In idle mode there is no need for handovers but MS makes itself available time to time for downlink traffic. Since handover is not needed and MS is not registered to some specified BS, before MS goes to idle state it is assigned to a paging group by BS which is formed by group of BS.

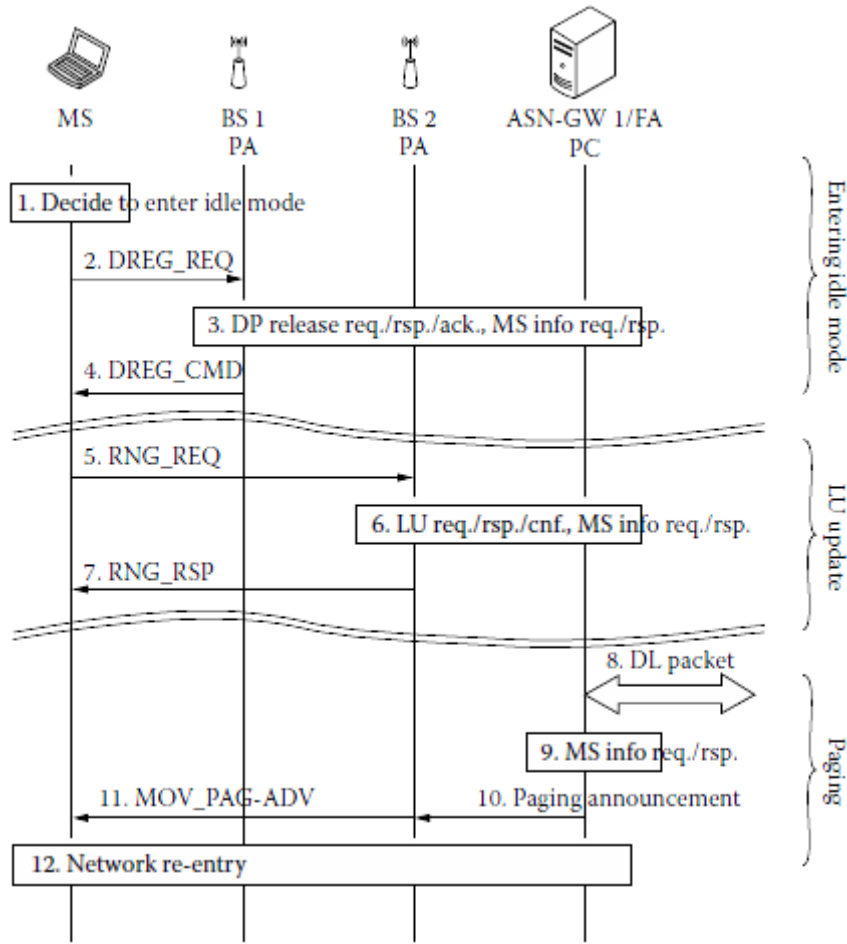


Figure 3.4: Management of idle mode & paging [26]

Like other mobile communication systems WiMAX also has its own paging network architecture. PC paging controller is conjunct with PG paging group.

PG is comprised of one or more (PAs) paging agents in the similar NAP. PG manages the MS in idle mode where PG is managed by PC and is responsible for paging and idle mode management.

From MS deregistration request (DREG-REQ) is sent to ASN-GW before going to idle state then the resources of MS are released by ASN-GW and the location is updated in

LR. Parameters such as paging cycle, paging offset, paging interval, paging group identifier, PC identifier are settled for MS by PC and PA. from these parameters MS determines paging listening interval. In paging cycle, paging listening interval of BS starts from paging offset frame. To receive broadcast messages (MOV-PAG-ADV) from BS, MS has to stay awake for entire paging listening interval.[26]

3.2 Handover

When the term handover is used the basic concept which comes to mind is, to provide the continuous connectivity to the MS when it shifts from coverage area of one BS to other BS. Whereas handover can occur between different channels under same BS which is called intra-cell handover, handover from one BS to other is called inter-cell handover. With in same technology network horizontal handover occurs and handover between different networks is vertical handover.

In 802.16e simple mobility and full mobility is specified where in 802.16-2004 there were no standards defined to support mobility, in the following table the details of comparison between 802.16-2004 and 802.16e are summarized which shows the maximum allowed speed and handovers in both 802.16-2004 and 802.16e versions.

Access	Speed	Handover	802.16 2004	802.16e
Fixed access	stationary	no	yes	Yes
Nomadic access	stationary	no	yes	Yes
Portability	walking speed	hard	no	Yes
Simple mobility	low vehicular speed	hard	no	Yes
Full mobility	high vehicular speed	soft	no	Yes

Table3.1: comparison detail for 802.16e & 802.16-2004

common types of handover are hard handover and soft handover, full mobility falls in the group of soft handover and portability & simple mobility comes in hard handover group.

In mobile wimax 802.16e MAC layer handover procedure is specified , Handover occurs in the situation when A MS moves for the better signal from one BS to another BS or MS

can have better service at other BS. Before handover occurs following steps takes place to achieve the network topology acquisition.

1 Advertisement :An information about the network topology is broadcast by BS which is acquired from backbone. MOB-NBR-ADV advertisement message is sent by serving BS time to time, from this advertisement message MS gets information about the characteristics of the surrounding BS.

2 Scanning :To seek and monitor the surrounding BS which can be the host for handover. The duration of scanning process is called scanning interval, (MOB-SCN-REQ) mobile scan request is send by MS and serving BS sends back (MOB-SCN-RSP) mobile scan response message in the reply to scan request message which consists information about the neighboring BS which can be candidate for handover. By the recommendation of serving BS the MS choose suitable BS for handover

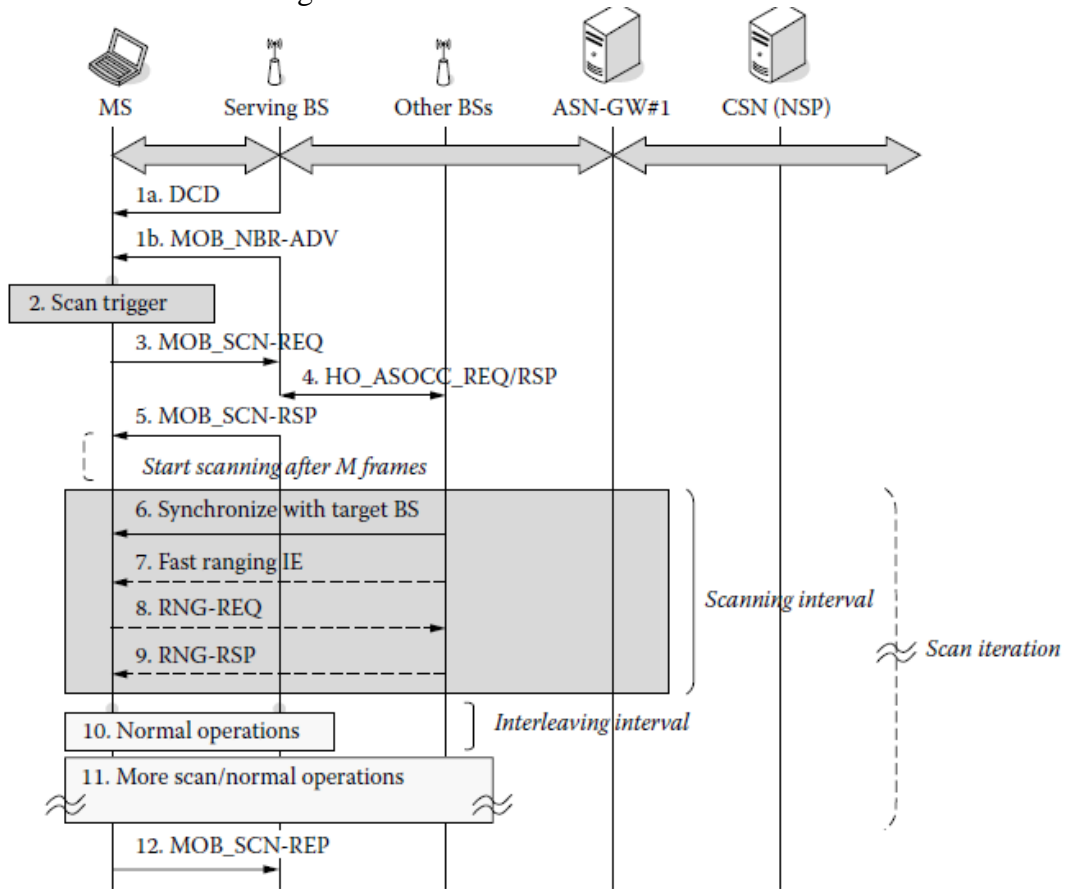


Figure 3.5 procedure of scanning and association[26]

3 Association :For the purpose of the selection of suitable target BS for handover, Association function is makes MS to be able to get and keep the information about the availability of service and ranging parameters, since association is optional but when its done before handover it reduces the synchronization and registration time of MS with the target BS. Association and its type is decided by the recommendation of serving BS in scan response message (MOB-SCN-RSP).

Roughly two types of handovers are supported in 802.16e which are hard handover (HHO) and soft handover. Hard handover is required and soft handover is optional[8].

In the process of hard handover brake-before-make may occur while association and establishment of connection with the target BS therefore it is a need for optimization, on the other hand (MDHO) macro diversity handover and (FBSS) fast base station switching are two schemes in soft handover[27] .

3.2.1 Hard handover (HHO)

Hard handover takes place when the signal strength of neighboring BS becomes stronger than the serving BS. MS communicates with only one BS at the same time so there may be brake-before-make.

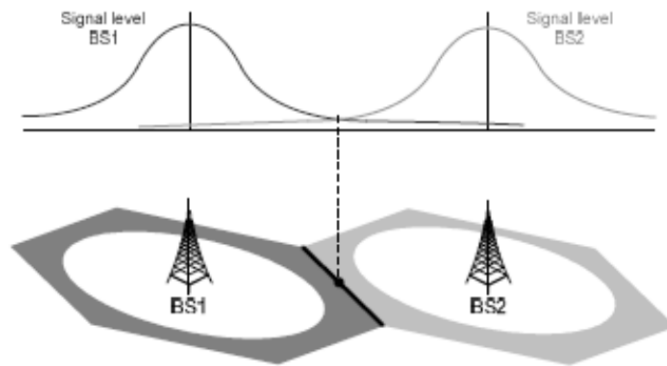


Figure 3.6 : realization of hard handover[29]

BS broadcast advertisement messages (MOB-NBR-ADV) when decision is made for handover it is done in following steps,

Handover preparation : Handover can be initiated by both the MS or BS by using (MOB-MSHO-REQ) or (MOB-BSHO-REQ), if request is sent by MS then BS replies with (MOB-MSHO-REP) reply message which contains recommended BS for handover.

Handover execution : After getting handover reply from BS with recommended target BS then MS send (MOB-HO-IND) message to serving BS and stop communication with the serving BS . MS negotiates with the target BS and performs authentication and registration.

Description of handover preparation and execution is given in the figure below:

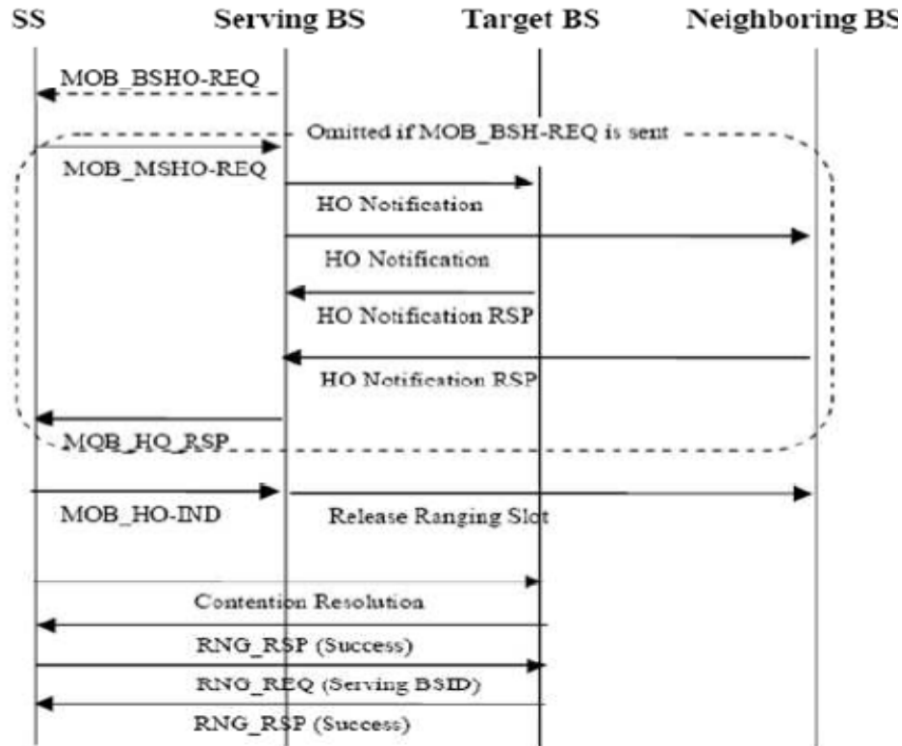


Figure 3.7 : handover preparation & execution[28]

3.2.2 Macro diversity Handover (MDHO)

The situation where number of receivers and transmitters are used for transferring the same signal is called diversity. Macro diversity handover (MDHO) is an optional scheme to reduce the delay and packet loss during handover, since MS communicates with several BS all the BS involved are known as diversity set. Among number of BS in diversity set one BS which controls DL and UL allocations is referred as anchor BS.

There might be some BS which are reachable by the MS but the signal is weak for traffic such BS are not included in the diversity set and falls under the category of neighbor BS. At some point neighbor BS can be included in diversity set when MS gets close to neighbor BS.

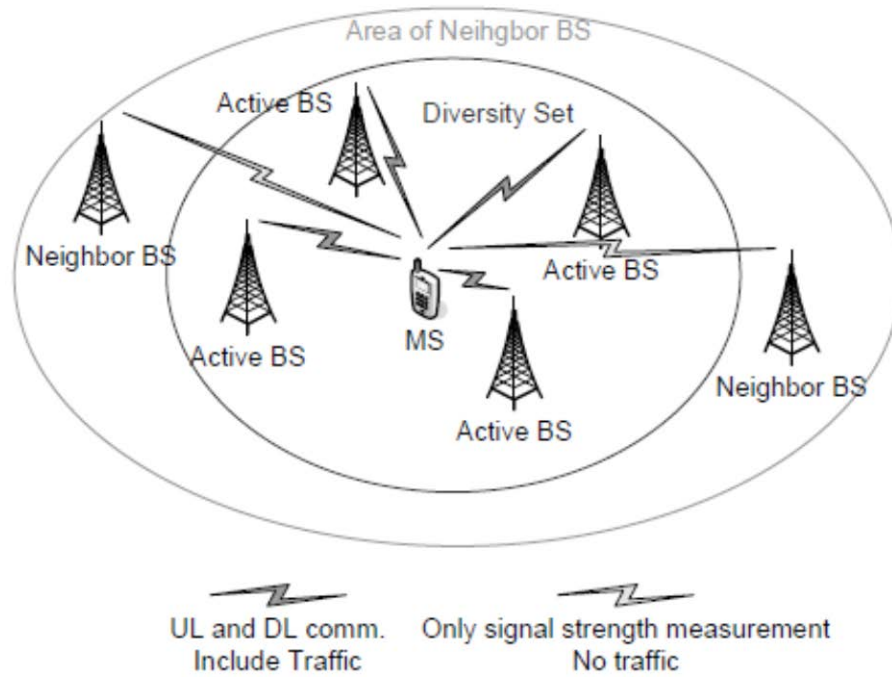


Figure 3.8: MDHO (macro diversity handover)[29]

There is special case when MDHO has only one BS in diversity set. Diversity set is updated when in diversity set the CINR of serving BS is less than the threshold, MS sends MOB-MSHO-REQ message to delete the BS from diversity set.

There are two ways by which MS monitors its DL and UL allocations. In first scheme MS proctor just DL MAP and UL MAP of anchor BS which gives information about the DL and UL allocation of MS for the anchor BS and all other BS in diversity set. In the second method, the DL MAP and UL MAP of all the BS in diversity set are proctored by MS for DL and UL allocations. First the DL signal is combined from all the BS in diversity set before decoding [30].

The best way to combine the signals from BS in diversity set is to combine at RF level. Which means at the all the BS should be synchronized i-e in time, frequency, encryption mask, format of modulation, H-ARQ, and also use the same CID.

3.2.3 Fast Base Station Switching (FBSS)

Same as MDHO , FBSS is also optional and maintains diversity set and anchor BS the purpose is same, to reduce the handover delay and packet loss. Serving BS which

transmits and receives data from MS is anchor BS. In diversity set all incoming traffic is multicast to all the BS, but in this case MS just send and receive traffic to and from only anchor BS where anchor BS can be changed for every frame. Updating of diversity set is similar as in MDHO.

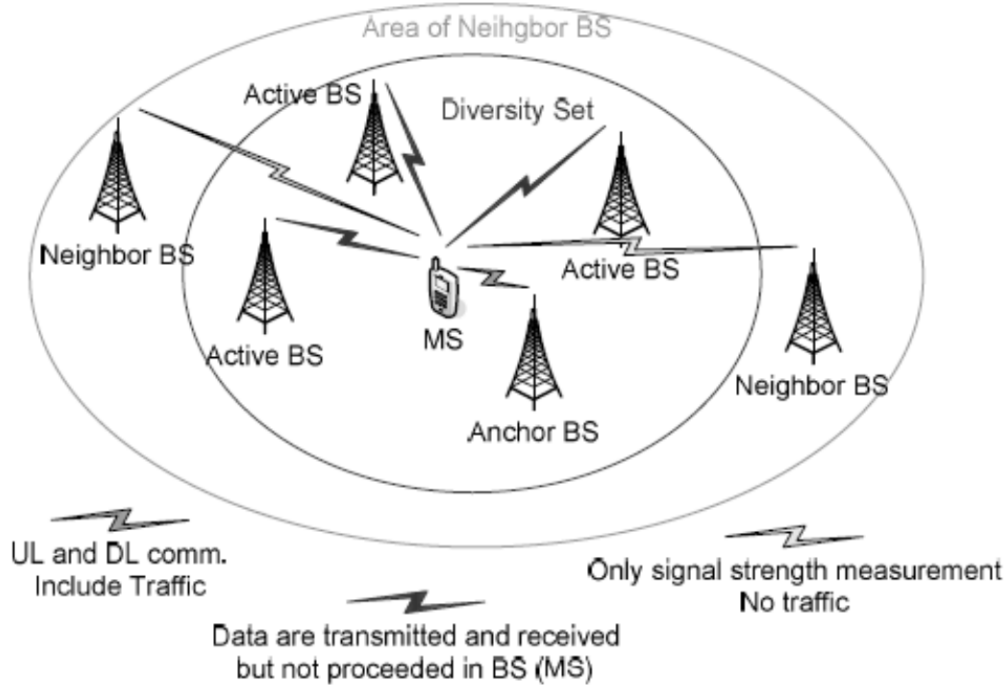


Figure 3.9 :FBSS, Fast Base Station Switching[29]

In FBSS active set is maintained , which consists of all involved BS. MS , on the continuous basis checks the active set and manage the CID and does ranging with each and every BS in active set. Obviously as it is discussed before MS communicates only with anchor BS where anchor BS can be changed by switching the connection from one BS to another BS in the active set. MS updates CQICH about the change in anchor BS.

Though both the soft handover schemes macro diversity handover (MDHO) and fast base station switching (FBSS) offer better performance to the hard handover (HHO), they are not included in Wimax forum release 1 and are not completely developed yet. All they require is that the BS in diversity or active set are fully synchronized.

3.3 Process of Handover

Some details of handover process in 802.16e Wimax are already discussed. Further involved steps in handover process are discussed in following section for the better understanding.

When network acquisition is done which includes Advertisement, Scanning and Association procedures, Now we r going to discuss the rest of the process which are : handover decision, Initiation, and ranging, Authorization and Registration procedures.

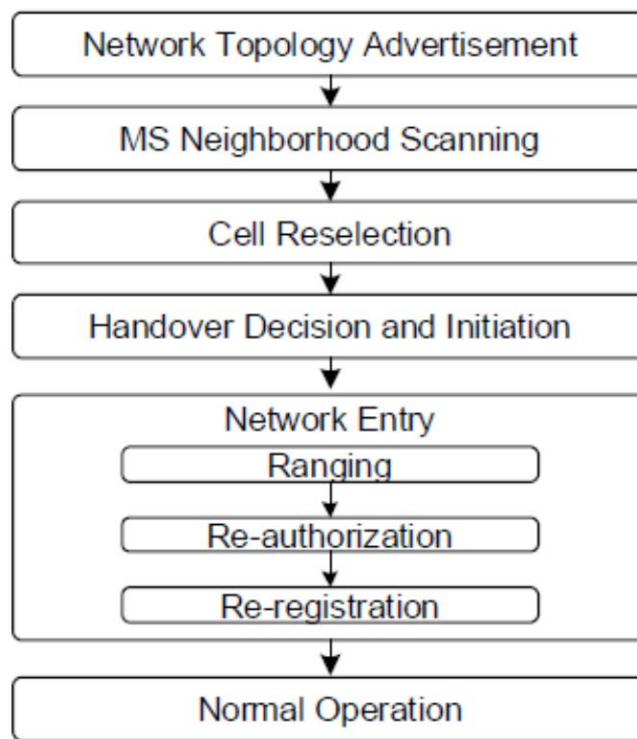


Figure 3.10: Handover Process

3.3.1 Cell Re-selection

Cell reselection is the first process in handover process in which MS gets information of surrounding BS by the advertisement message and it selects BS as a target for handover. To conduct the cell reselection the currently serving BS schedule sleep / scan intervals.

3.3.2 Handover Decision and Initiation

Actually the process of handover begins with the decision which can be made by both the MS and BS, when the decision is made by MS it sends MOB-MSHO-REQ to the serving BS, this message contains list of target BS for handover in reply to message BS sends back MOB-BSHO-REP suggesting the target BS. The MS sends indication message MOB-MSHO-IND to the serving BS, [30]

In case the decision is taken by BS, BS sends request to the MS MOB_BSHO-REQ suggesting the target BS for handover. The MS sends back the indication message MOB-MSHO-IND informing about the choice of target BS for handover process. The process is shown in the following figure.[30]

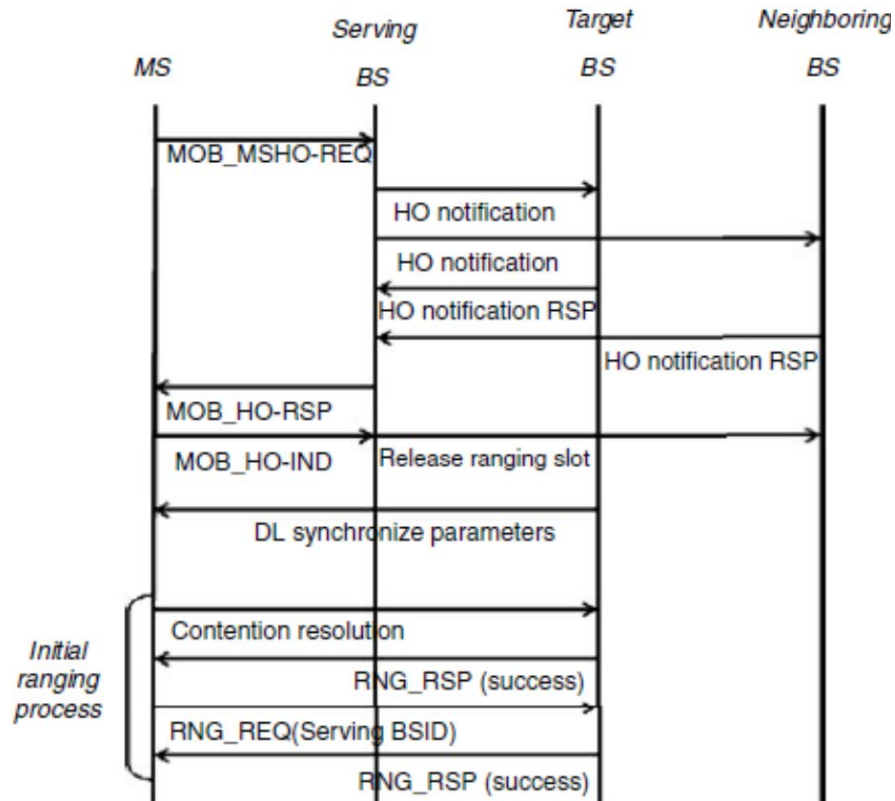


Figure 3.11: Handover decision & Initiation [27]

3.3.3 Synchronization with the target BS

After determining the target BS, MS synchronizes with DL traffic. From DL frames, MS collects information like time and frequency synchronization with the BS. From DL-MAP, UL-MAP, DCD and UCD messages MS gets information about ranging.

3.3.4 Ranging

In this process target BS gets information from serving BS. To setup the communication parameters, MS and target BS conduct initial ranging or handover ranging. The ranging done from MS to the BS is connection based, on the other hand if serving BS sets the ranging with the target BS it sends CDMA code to the MS in MOB-BSHO-RSP message.

3.3.5 Re authorization

After achieving the authorization, MS time to time seek reauthorization with the serving BS. To keep the FK MS has to maintain its state of reauthorization. Reauthorization process is same as authorization but in this case authentication message is not issued by MS. If static SAID change while reauthorization, TEK state machines can be started or stopped[27]. Through the authorization state machine also reauthorization is achieved. The figure 3.12 illustrates the process of authorization and authentication.

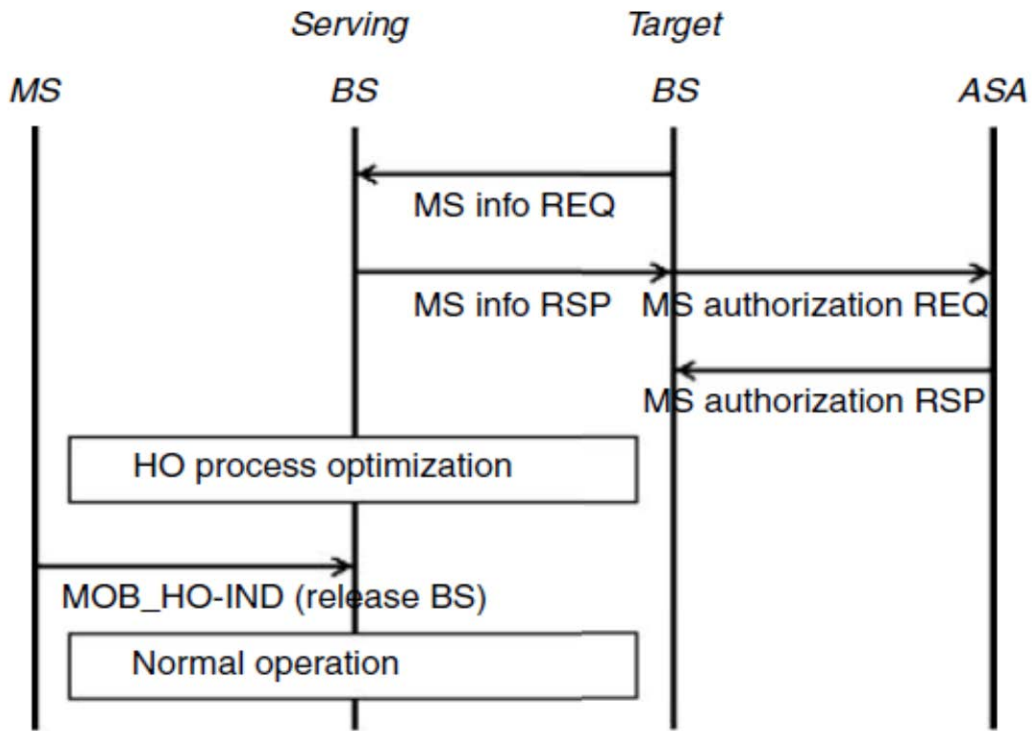


Figure 3.12 : authorization & authentication[27]

3.3.6 Re registration

During network initialization and re-registration initial ranging is performed to allocate CDMA codes. After that MS is permitted to join network to get the parameters (TX parameters (timing off set and TX power level). When transmission is taking place on periodic basis, periodic ranging is done which uses UL burst to permit MS to set TX parameters so it can maintain UL communication with BS[26].

3.3.7 Termination of MS context with previous BS

The last step in wimax handover . when a successful handover is done now its time to terminate the connection with serving BS. When the connection with the target BS is established the MS decides to terminate the connection with BS by sending an indication message MOB_HO-IND to the BS then BS starts the *resource retain timer* and keeps all the associated MAC state machines and buffered MAC PDUs unless the timer expires, then BS deletes all the associated MAC state machines and MAC PDU to the MS.

CHAPTER 4

SOLUTION FOR HANDOVER PROBLEM

Fast Handover Schemes and Solutions of Problems causing Handover delay

We can categorize WiMax Handover in three main categories which are Hard handover, Fast Base Station Switching (FBSS) and Macro Diversity Handover (MDHO)[31]. Except from hard handover the remaining two types are optional whereas hard handover is mandatory.

In all three handover schemes HHO is the most simple one contrary to other two. From this point onward in the document the handover will refer to hard handover.

Below are the phases involved in MAC layer at time of handover:

- acquiring network topology before handover including topology advertisement as well as MS scanning of the BS's.
- Execution of handover includes reselection of cells, initialization of process and handshake. Apart from this other actions involved are connection release and the re-entry of the target network.

4.1 Handover Topology

As explained already in the chapters before that in 802.16e the reasons for handover in detail. In network

topology in 802.16e MS is served whereas base stations BS1~BSn regionally manage and control the MS. On moving out of MS from any BS like BS1 the handover becomes mandatory. The figure below shows the dissection of handover process [32].

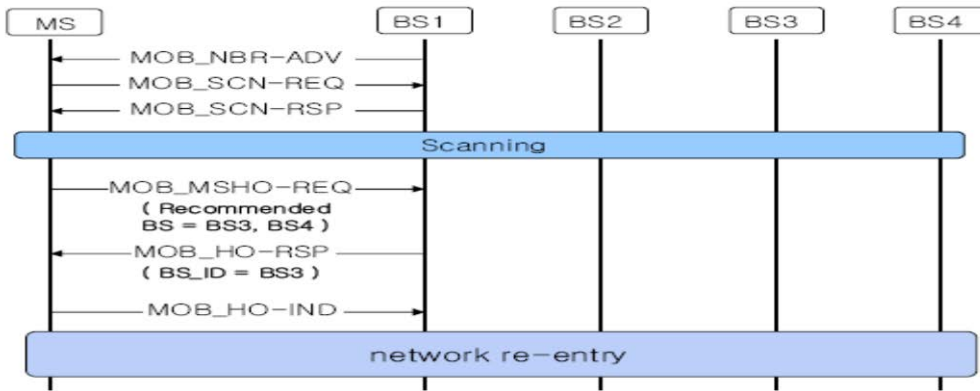


Figure4.1 Handover Topology [32]

The serving BS on set intervals send messages to MS regarding channel information about the neighbour BS's using `MOB_NBR-ADV`. When the strength of the signal goes down `MOB_SCN-REQ` is sent by MS to the serving BS whereas it receive `MOB_SCN-RSP` message as a result in order to get the scanning time interval. At the end of above processes the target BS's are selected by MS depending on the signal strength as well as response time calculated during scanning. MS sends `MOB_MSHO-REQ` message to the serving BS. `MOB_MSHO-RSP` message is received as a result of final selection of the target BS lets assume BS3.

When the `MOB_HO-IND` message is issues by MS the actual handover occurs in a result making network re-entry.

The figure below shows the scanning process in the example context in detail as explained above [32]

As a result of `MOB_SCN-REQ` and `MOB_SCN-RSP` messages MS receive time interval regarding scanning. After that MS scan the adjacent BSs using the process of synchronization as well as association. After the above processes CINR (carrier-to-interference-and-noise ratio) is calculated [33] also the relative delay for adjacent BS. Incoming data is buffered while termination of transmission towards MS in the scanning process. Also the scnning of neighbouring BSs is done sequentially in contrast to simultaneous scanning. As a result of sequential scanning the process is stretched which

further pauses the transmission of data towards MS making the system's performance down.

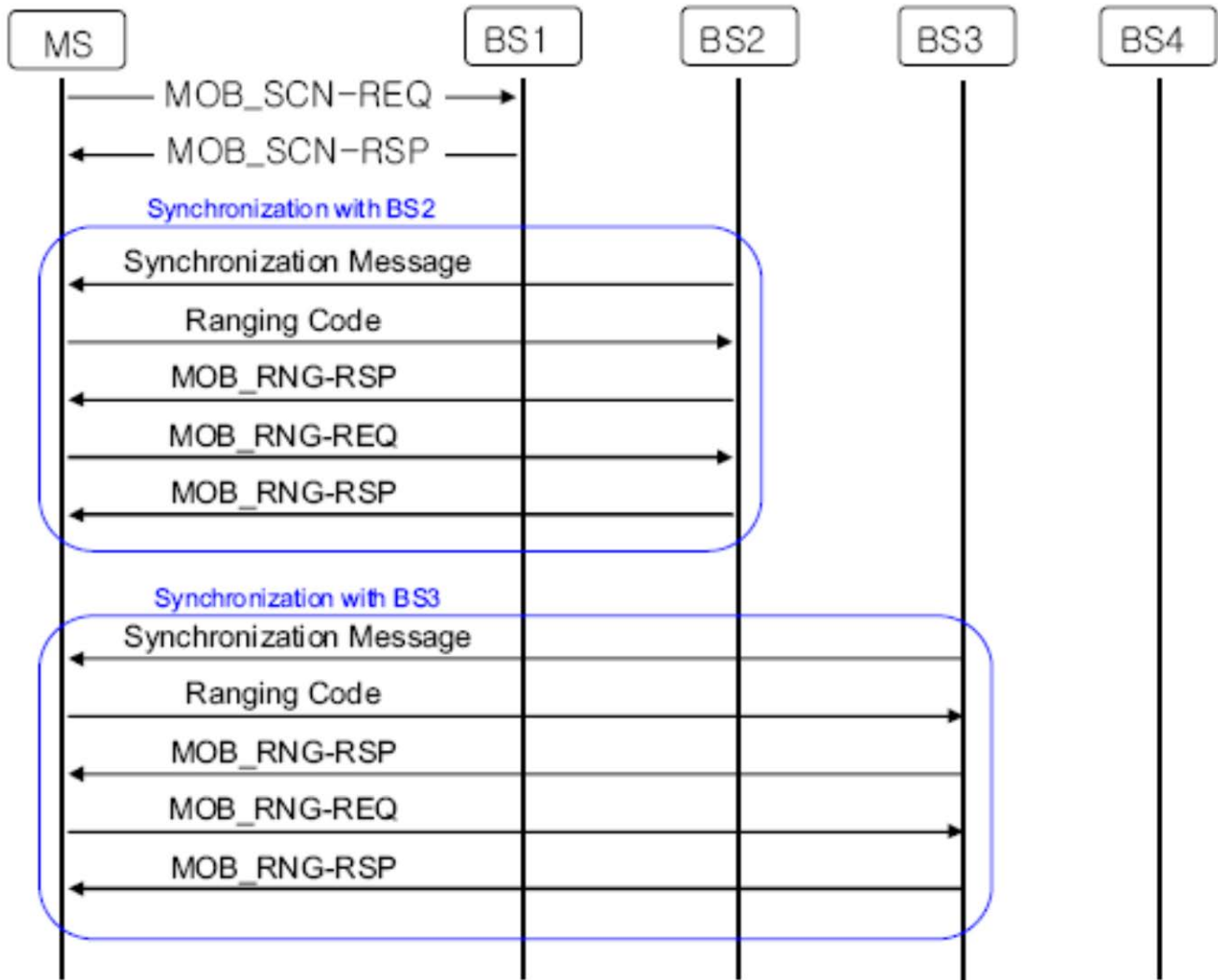


Figure4.2 [32]

- **Negotiation:** On completion of scanning MOB_MSHO-REQ message is sent by MS and utilizing list of target BSs serving BS starts HO pre_notification procedure including the MS identification, bandwidth as well as QoS needed by MS in context of

backbone network. Validation of MS performance expectation is carried out on reception of HO pre_notification response by serving BS. These sets of activities are known as negotiation and are critical for selection of target BS finally. Following figure shows the negotiation process [34]

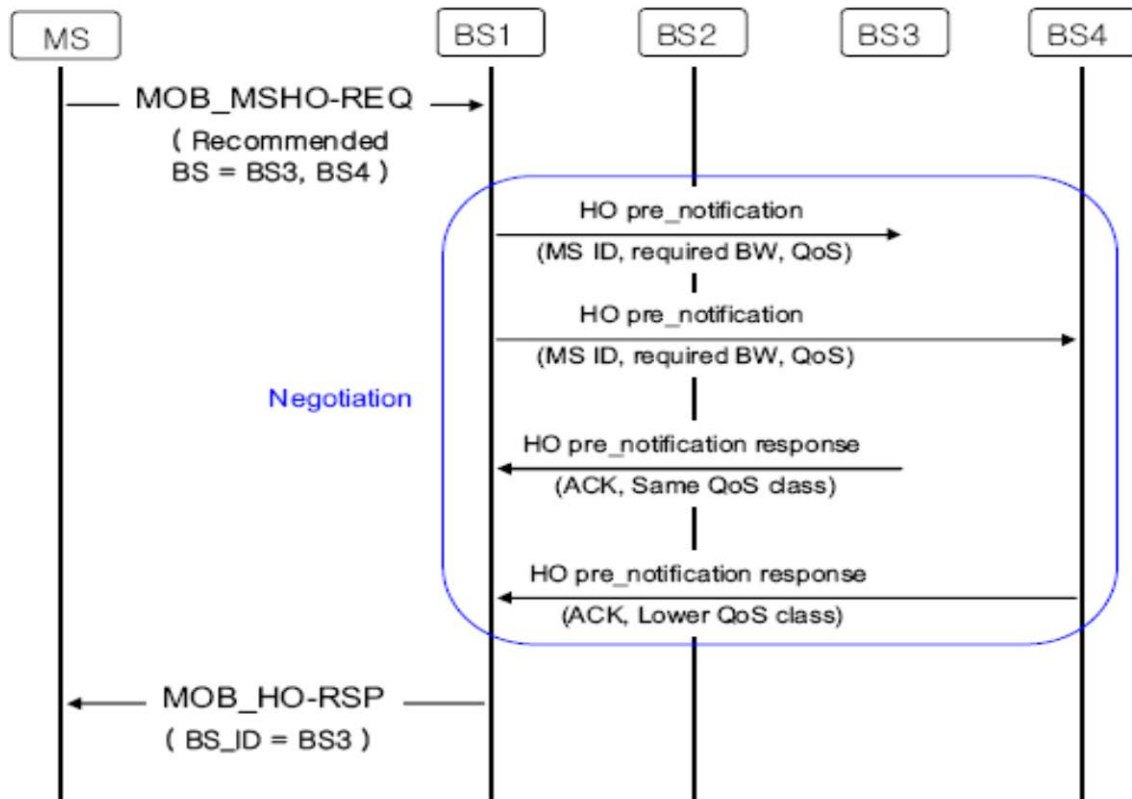


Figure 4.3 negotiation process [34]

In the above figure BS is being served by BS1 whereas BS3 and BS4 constitute target list for BS. It also displays the procedure of target BS selection which in this case is BS3 in result of negotiation done using backbone network. In the above figure BS3 is selected as a result of its capability of QoS required by MS.

The point focused in proposed scheme is that target BS selection during handover process is done in two portions. That is scanning of neighbour BSs is achieved in IEEE

802.16e before selection of any BS as target also after negotiating target BS is selected by serving BS. Contrary to that in conventional algorithm selection of target BS takes place using the 'scanning negotiation' way. Whereas it is opposite in case of proposed scheme where the sequence of negotiation scanning is reversed which in turn lessens the BSs scanning. On issuance of MOB_SCN-REQ message for time interval, all the neighbouring BSs are negotiated through the backbone network by the serving BS.

The neighbouring BSs notify back using HO pre_notification response which provides the MS information regarding performance, after each of them get notification from serving BS about information regarding MS identification as well as required bandwidth along with QoS.

The BSs unable to provide QoS as per MS requirement are eliminated and MOB_SCN-RSP message is sent by the serving BS. As a result only the BSs satisfying the conditions are scanned by MS and at the end of scanning the target BS is already selected. CINR checking for neighbouring BS is done for single target BS estimation based on the list of QoS satisfying BSs. In other words then neighboring BS with most suitable CINR is processes only.

4.2 Redundancies in MAC Layer Handover Process

Real handover process is done after network topology phase in IEEE 802.16e MAC layer handover procedure[35]. In the process of network topology mere one BS selection is done, making potential redundancy in scanning provided many BSs are selected for scanning process for target BS. Also as the data transmission is stoped during the scanning process the throughput becomes little in case scanning processes take too much of the available resources. In case of change in the neighbouring BSs channel quality the calculations may be of no use and a considerable amount of system resources may be utilized without any purpose.

In the three way handshake as well as the resellection of cell's process the downlink data may be received by MS from the serving BS and there is also possibility of sending uplink data. The link between serving BS and MS can be finished on reception of HO-IND message by the serving BS, which carries information regarding connection release as well as handover start. The paused or in other words in buffer data transmission is normalized after re-entering target BS procedure.

4.3 Cost-Effective Target BS Selection Scheme

The serving BS provides the channel information depending on which MS do the scanning of the neighbouring BSs, this process is done before making the handover decision. On the completion of the scan process negotiation is done between serving BS and the target BSs using backbone network message, as a result one target BS is filtered out which fulfils the requirements I.e bandwidth as well as QoS as per request of MS. As discussed earlier during the scanning process by MS data transmission is halted by buffering that in the allocated buffers which somehow decrease system pformance. In parallel with this mobility factor also needs consideration therefore consideration of adaptive channel scanning technique [36] is beneficial to be considered.

In the proposed scheme by negotiating the neighbouring BSs unwanted BSs are eliminated before scan process. Information regarding bandwidth and QoS is sent to neighbouring BSs using backbone network message before MS starts scanning [37].

The protocol calculates the MS' required performance by the response given by neighbouring BSs provided the service is given by the respective BS. In this way only the BSs satisfying the demands are scanned by the MS. As a result the list of BSs to be scanned is reduced as well as the time in turn minimizing system interruptions.

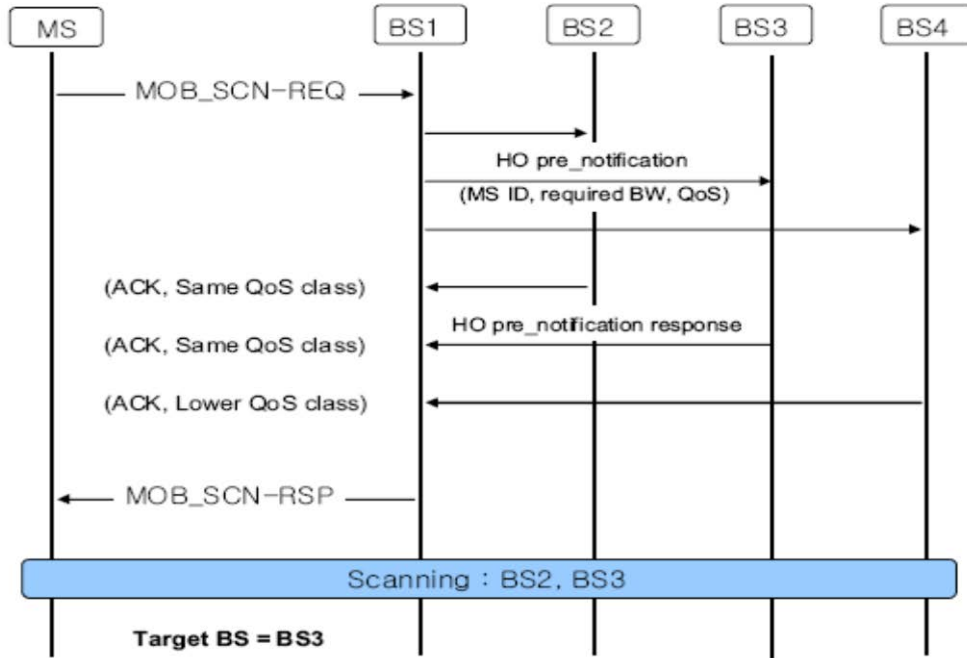


Figure 4.4 CTBS [38]

In the context of above figure (BS2 to BS4) belong to neighbouring BSs group whereas BS1 is the serving BS,. Also from the list of neighbouring BSs BS4 is unable to meet the QoS requirements contrary to BS2 and BS3. Therefore while negotiation process BS4 is excluded and is out of scanning process. In short only BS2 and BS3 are included in scanning process. After receiving the MOB_SCN-REQ message HO pre,_notification is transmitted by BS1 to BS2, BS3 and BS4 in order to inform them about MS ID and other information like bandwidth and QoS requirements.

BS1 is informed by HO pre_notification response about BS2and BS3 adequacy about MS demanded QoS requirements and also inadequacy of BS4 in this regard. This information is received by MS through MOB_SCN-RSPmessage making it scan the filtered list containing BS2 and BS3 only. After the calculations using information provided by scanning process BS3 is taken as target BS. On contrary to this in the normal process all neighbouring BSs are scanned taking down system performance because of more

transmission suspensions in scan procedure. In parallel to this the procedure of negotiation is done using backbone network which in turns doesnt halt transmission. Thats the reason that before the scan process negotiation is done to figure out the MS demand fulfilling BSs. And in this way the selected list of BSs is scanned making amount of scans lesser and in result taking down halts in transmissions.

4.4 Fast Ranging and Pre-registration

Handover delay in IEEE 802.16e is done most in target network re-entering process. Its also logical to say that lower the handover delay more are the chances of successful handovers. So we can safely say that optimization of network re-entering process in context of reducing handover delay can surely make the system performance better. Target BS is told in fast ranging [39] about provision of dedicated ranging for MS. For broadcasting UL-MAP message by MS Fast_Ranging_IE is used to give uplink possibility to MS. There remains no need for contention based ranging by MS after the target BS gives possibility of dedicated ranging. In result reducing the time for ranging.

Before handover target BS gets the information about authentication as well as service flow of MS using backbone network in the process of pre-registration [40]. Therefore there remains no need of information from authorization server by target BS through backbone, in result reducing the time period of handover process. But its also fact that target BS still needs to give CID using REQ-RSP message updation to MS though it know about the information regarding service flow and authentication. This in turn makes the pre-registration time to almost half of the overall registration process time period. Utilizing Fast_Ranging_IE there is provided opportunity to MS for a dedicated ranging, whereas using pre-registration service flow as well as authentication information is got by target BS. Hence making the re-entering process faster and in simple words handover delay is decreased making more chances of successful handover.

4.5 Security Issues in WiMax

We are going to discuss the security provision managed in Wimax. To understand the security provision in WiMax we can divide that in layers. We can safely divide the architecture in two main layers, which are MAC and Physical.

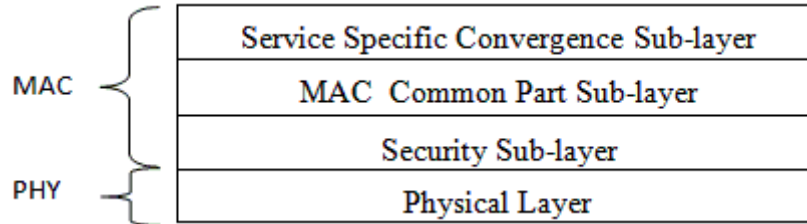


Figure 4.5 IEEE 802.16 Protocol structure [41]

Also we can subdivide MAC layer into three sub-layers, which are, the Service Specific Convergence Sub-layer (CS) which is responsible for integrating higher level data services, to the service flows and connections of MAC layer [41]. Whereas second is known as CPS, that is Common Part Sub-layer considered as the core and have close connection with the third layer, that is security sub layer. The security sub layer is present between MAC and PHY layers. This layer deals with the establishment of key, authentication process as well as encryption and decryption of the data between the other two sub layers.

4.6 Loop holes in WiMAX security and Their Solutions

PHY layer problem

As we have idea that security sub layer is over PHY layer which makes PHY layer insecure [42], in turn making it potentially open to problems of wireless security like jamming, water torture attacks and scrambling. It is also a fact that because of mobility support in WiMax, it is even more open to these threats as the attacker have no need to be in a fixed place. We are going to synthesize these attacks in a little more explanation here.

Jamming attack is used to reduce the channel capacity to a big extent by giving a strong noise source [42] . Jamming can be both intentional or unintentional. Its also really easy to make jamming attack as the information and equipment are easily available.

Jamming can be avoided by increase in signal strength or by increase in the bandwidth using spectrum techniques like frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS) [42]. Also law enforcement institutions can also be informed as its not a difficult task to detect jamming source using radio direction finding equipment.

Scrambling is also a kind of jamming but its done for short time period targeting specific frames in WiMax or parts of frames in PHY layer. Control or management information can be scrambled by attackers in order to sabotage the normal working of the network. Chunks of the traffic owned by the targeted SSs can be scrambled making them to retransmit the data again. Scrambling attack is a lot more difficult than jamming as the attacker have to know about the control information and to introduce the noise data during specific interval [42].

It is much more harder to detect scrambling as compared to jamming but we can utilize anomalies monitoring beyond performance norm (or criteria) for the detection of scramblers [42].

, In water torture attack SS is forced to drain battery or to utilize resources for computing by sending fake frames [43]. This attack is much more devastating than standard DoS attack because of the fact that SS because of portability have limited resources.

In order to avoid this water torture attack a refined mechanism is needed to differentiate fake frames.

Other than jamming, scrambling and water torture attacks WiMax is potentially vulnerable to attacks such as forgery attacks using which wireless channels can be written using proper radio transmitters [43].

However in WiMAX security problem of 802.16 is fixed using mutual authentication.

Threats to the MAC layers

There are a lot of security issues in WiMax MAC layer. Following are some problems regarding security in MAC layer of WiMax.

The Ranging Request-Response (RNG-REQ, RNG-RSP) message is utilized in the initial ranging process. There are many potential threats for these messages. For example after interception of RNG-REQ message the attacker can make the priority of burst profile of SS from preferred to least priority in turn downgrading the service [44] [45] Also spoofing of ranging message can be done to interfere in the normal activities of the network This problem in security can be used for DoS attack.

In the WiMax authentication masquerading attack can be done on the authentication protocol of PKM . By reprogramming a device with different address attackers can by interfering the management message An attacker can reprogram a device with the hardware address of another device, whereas the address can be taken by interference of the messages regarding management. Also by using a fake BS which presents itself as a legitimate BS can compromise SS by making SSs believe that they are in connection with the original BS. Because of which complete information of SSs can be taken.

Conclusion

In the thesis we have analyzed and studied IEEE802.16e architecture and handover mechanism indepth. During the process of handover there are present some problems which make it delayed. It is also a fact that WiMax is still in the phase of improvement and needs special attention on the process of handover optimization. The handover delay causes some problems in the overall quality and at the application layer the effect is most critical, which may cause some time critical and real time applications to suffer or potentially disturb the actually wanted results.

In the analysis we have figured out some of the factors making the handover process delay hence making QoS down. We have also proposed some schemes like CTBS, Fast ranging and pre-registration mechanism for the optimization of handover process. The CTBS is used to for the negotiating process before the scan process and is able to lessen the scanning time in the procedure of acquiring the topology whereas the delay can be reduced by fast ranging and pre registration.

In short these schemes can improve the use of resources and hence increase efficiency and reduce handover delay. We have also discussed the security threats and some of their solutions briefly. The security threats in this document are divided on the basis of physical and MAC layer. Although there is a security layer between these two layers but still there are many deficiencies in WiMax because of the wireless and mobility communication in general. However these deficiencies can be taken care of by implementing some new solutions, some of which are already discussed in this document.

Future Work

In the future work the proposed schemes can be simulated and verified. Also there are other schemes in research stages which can be analysed and simulated to cope up with handover delay and making the whole handover process optimized.

References

- [1] WiMAX: Technology for Broadband Wireless Access Loutfi Nuaymi © 2007 John Wiley & Sons, Ltd. ISBN: 0-470-02808-4
- [2] The wimax forum , internet home page www.wimaxforum.org , april 2009.
- [3] WiMAX: The Innovative Broadband Wireless Access Technology, JOURNAL OF COMMUNICATIONS, VOL. 3, NO. 2, APRIL 2008
- [4] Wireless overview, internet homepage www.wirelessoverview.net/index.php/wimax/tutorial
- [5] MobileWiMAX: Edited by Kwang-Cheng Chen, J. Roberto B. de Marca, April 2008
- [6] Prentice Hall: “ Fundamentals of WiMAX “ , Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed .Feb 2007.
- [7] Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks , by Senza Fili Consulting on behalf of the WIMAX Forum ,Nov 2005.
- [8] Auerbach publications: Mobile WiMAX : toward broadband wireless metropolitan area networks / editors, Yan Zhang and Hsiao, Hwa Chen. Dec 2007.
- [9] Auerbach publications: WiMAX MobileFi Advanced Research and Technology / editors, Yang Xiao Dec.2007
- [10] C. Eklund, R.B. Marks, and K.L. Stanwood, IEEE Standard 802.16: A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, IEEE Commun. Mag.,40(6), 98, 2002.

- [11]. K. Wongthavarawat and A. Ganz, Packet Scheduling for QoS Support in IEEE 802.16 Broadband Wireless Access Systems, *Int. J. Commun. Sys.*, 16, 81, 2003.
- [12]. J. Chen, W. Jiao, and H. Wang, A Service Flow Management Strategy for the IEEE 802.16 Broadband Wireless Access Systems in TDD Mode, White paper, IEEE, Washington, DC, 2005.
- [13]. H.Wang,W. Li, and D.P. Agrawal, Dynamic Admission Control and QoS for 802.16Wireless MAN, *Wireless Telecommunications Symposium*, p. 60, IEEE, Washington, DC, 2005.
- [14] Wimax RF frequencies : web page <http://www.wimax.com/education/faq/faq47> , April 2009.
- [15] Network Reference Model , Internet home page : http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/WiMAX_Overview3.html , May 2009.
- [16] WiMAX Forum® Network Architecture, (Stage 2: Architecture Tenets, Reference Model and Reference Points) [Part 1] , Release 1.0 Version 4, WiMAX Forum APPROVED ,WiMAX Forum Document Number, WMF - T32-002-R010v04 February 03, 2009
- [17] Prentice Hall: “ Fundamentals of WiMAX “ , Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed .Feb 2007.
- [18] Mobile WiMAX, edited by Kwang-Cheng Chen, J. Roberto B. de Marca, JohnWiley & Sons, Ltd, APR 2008

- [19] WiMAX Forum® Network Architecture, (Stage 2: Architecture Tenets, Reference Model and Reference Points) [Part 3 – Informative Annex], Release 1.0 Version 4, WiMAX Forum APPROVED ,WiMAX Forum Document Number WMF - T32-004-R010v04, February 03, 2009
- [20] IEEE P802.16e/D11: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, September 2005
- [21] WiMAX Forum, Mobile WiMAX—Part 1: A Technical Overview and Performance Evaluation, WiMAX Forum, Beaverton, OR, 2006.
- [22] J.-Y. Hu and C.-C. Yang, On the Design of Mobility Management Scheme for 802.16-Based Network Environment, IEEE 62nd Vehicular Technology Conference (VTC-2005-Fall), vol. 2, pp. 720, IEEE, Washington, DC, 2005
- [23] IEEE, IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, Standard 802.16e-2005, IEEE, Washington, DC, 2006.
- [24] K. Han and S. Choi, Performance Analysis of Sleep Mode Operation in IEEE 802.16e Mobile Broadband Wireless Access Systems, IEEE 63rd Vehicular Technology Conference (VTC-2006-Spring), vol. 3, p. 1141, IEEE, Washington, DC, 2006
- [25] Itzik Kitroser, Yossi Segal, Yigal Leiba, Zion Hadad ,IEEE 802.16 Broadband Wireless Access Working Group, IEEE 802.16e Sleep Mode, 2003-03-11
- [26] Auerbach publications: Mobile WiMAX : toward broadband wireless metropolitan area networks / editors, Yan Zhang and Hsiao, Hwa Chen. Dec 2007.

[27] Auerbach publications: WiMAX MobileFi Advanced Research and Technology / editors, Yang Xiao Dec.2007

[28] Vinh Dien HOANG¹, Maode MA², Ryu MIURA¹ and Masayuki FUJISE¹,
A Novel way for Handover in Maritime WiMAX Mesh Network. June 2007

[29] Zdenek Becvar, Jan Zelenka : “Handover In Mobile Wimax” , Czech Technical University, Department of Telecommunication Engineering.

[30] Prentice Hall: “ Fundamentals of WiMAX “ , Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed .Feb 2007.

[31] WiMAX Forum: Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation, February 2006

[32] Sik Choi, Gyung-Ho Hwang, Taesoo Kwon, Ae-Ri Lim, and Dong-Ho Cho, “Fast handover scheme for real-time downlink services in IEEE 802.16e BWA system,” Vehicular Technology Conference, pp 2028- 2032 Vol 3, May 2005.

[33] IEEE 802.16 Broadband Wireless Access Working Group <<http://ieee802.org/16>> Calculating CINR for Handoff.

[34] A Cross-layer Fast Handover Scheme For Mobile WiMAX by Ling Chen , Xuejun Cai, Rute Sofia, Zhen Huang

[35] Doo Hwan Lee, Kyandoghene Kyamakya, and Jean Paul Umondi, “Fast handover algorithm for IEEE 802.16e broadband wireless access system,” Wireless Pervasive Computing, January 2006.

[36] R. Rouil and N. Golmie, “Adaptive Channel Scanning for IEEE 802.16e,” Proceedings of 25th Annual Military Communications Conference (MILCOM 2006),

Washington, D.C., October 23-25, 2006.

[37] Kyung-ah K, Chong-Kwon K, Tongsok K, A seamless handover Mechanism for IEEE 802.16e Broadband Wireless Access[C]. ISPC 2004, August 2004

[38] Hoon-gyu Choi, Jongpil Jeong, and Hyunseung Choo, "CTBS: Cost-Effective Target BS Selection Scheme in IEEE 802.16e Networks.

[39] Pre-Coordination Mechanism for Fast Handover in WiMAX Networks by Jenhui Chen and Chih-Chieh Wang and Jiann-Der Lee.

[40] H. Jang, J. Jee, Y-H. Han, S.D. Park, J.Cha, "Mobile IPV6 Fast Handovers over IEEE 802.16e Networks," MIPS SHOP Working Group, Internet Draft.

[41] Abdelrahman Elleithy, Alaa Abuzagheh, Abdelshakour Abuzneid, "A new mechanism to solve IEEE 802.16 authentication vulnerabilities", Computer Science and Engineering Department University of Bridgeport, Bridgeport, CT.

[42] Michel Barbeau, "WiMax/802.16 Threat Analysis", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Quebec, Canada 2005.

<http://portal.acm.org/citation.cfm?id=1089761.1089764>

[43] David Johnson and Jesse Walker, "Overview of IEEE 802.16 Security", Intel Corp, IEEE Security and Privacy, 2004

<http://portal.acm.org/citation.cfm?id=1009288>

[44] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", International Journal of Computer

Science and Network Security, VOL.7 No.11, November 2007.

http://paper.ijcsns.org/07_book/200711/20071102.pdf

[45] Sheraz Naseer, Dr. Muhammad Younus, Attiq Ahmed, "Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks: A Survey", Proceedings of the 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4617395