Analysis of Handover Schemes in

IEEE 802.16 (WiMAX)

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Computer Science and Engineering

Thapar University, Patiala

By:

Mohit Saini

(80632014)

Under the supervision of

Dr. Anil K. Verma

Lecturer

JUNE - 2008

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Analysis of Handover Schemes in IEEE 802.16 (WiMAX)"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted to Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Anil K. Verma* and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(Mohit Saini)
Roll No. 80632014

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Anil K. Verma)
Supervisor
Computer Science and Engineering Department
Thapar University
Patiala

Countersigned by

(Dr. (Mrs.) Seema Bawa)
Professor & Head
Computer Science & Engineering Department
Thapar University
Patiala

(Dr. R.K. Sharma)
Dean, Academic Affairs
Thapar University
Patiala

ACKNOWLEDGEMENT

"The need to be right all the time is the biggest bar to new ideas. It is better to have enough ideas for some of them to be wrong than to be always right by having no ideas at all."

- Edward de Bono

I am highly thankful to my guide Dr. Anil K. Verma, Lecturer, Computer Science & Engineering Department, Thapar University, Patiala, for his advice, motivation, guidance, moral support, efforts and the attitude with which he solved all of my queries in making this thesis possible. It has been a great honor to work under him.

I am also thankful to Dr. (Mrs.) Seema Bawa, Professor and Head**,** Computer Science and Engineering Department, Thapar University, Patiala, for providing us with adequate infrastructure in carrying the research work.

I am also thankful to Ms. Damandeep Kaur (PG Coordinator) and other faculty members for their contribution in making this thesis possible. Besides the above dignitaries, I am also thankful to my friends Ashish Jain, Neeraj Rathore, Rajeev Rathor, Arun Arora, Anranya Yadav and Nikhil Gautam for their kind and noble support.

I am forever indebted to my parents for their constant support and encouragement throughout the past years. This thesis is devoted to them.

Mohit Saini

ABSTRACT

Enterprises, Internet Service Providers, and Mobile Network Operators are all looking for cost-effective ways to move data ,voice and video amongst multiple, separate locations at broadband speeds. Copper and fiber optics solutions often fall short due to up-front costs, recurring leases from telecommunications companies, and a lack of flexibility to scale with the operating organization. Broadband Wireless has emerged as a means to fill these gaps and to provide a lower total cost of ownership than wired solutions, while maintaining or exceeding the reliability and performance of those technologies. The IEEE 802.16 family of standards and its associated industry consortium, WiMAX, promises to deliver high data rates over large areas to a large number of users in the near future. This exciting addition to current broadband options such as DSL, Cable, and WiFi promises to rapidly provide broadband access to locations in the world's rural and developing areas where broadband is currently unavailable.

It is also necessary to provide Quality of Service (QOS) guaranteed with different characteristics for Broadband Wireless Access (BWA) networks. Major issue concerning implementation of WiMAX is to provide effective handover. Considering QOS parameters it becomes necessary to provide handover process to be as fast as possible. Various fast handover techniques have been suggested in literature to meet QOS requirements.

This thesis explains handover process in WiMAX along with different handover techniques. Various Fast handover techniques explained include Cost effective Target Base Station Selection, Fast Ranging and Pre-registration. Effect of these Handover Techniques on the WiMAX parameters like Scanning Time and Handover Latency have been studied taking assumptions into consideration. By extensive simulation it has been shown that these fast handover schemes when combined reduce the scan time and handover latency during handover process and increase the overall performance of WiMAX handover process.

KeyWords: Handover, Cost Effective Target BS Selection (CTBS), IEEE 802.16, WiMAX

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAA: Authentication, Authorization and Accounting

AMC: Adaptive modulation and Coding

AES: Advanced Encryption Standard

ASN: Access Service Network

BS: Base Station

CBR: Constant Bit Rate

CINR: Carrier Interference Noise Ratio

CSN: Connectivity Service Network

CTBS: Cost Effective Target BS selection Scheme

DL-MAP: Downlink Map Message

DSL: Digital Subscriber Line

DCD: Downlink Channel Descriptor

FDD: Frequency Division Duplex

FDMA: Frequency Division Multiple Access

FFT: fast Fourier transforms

FTP: File Transfer Protocol

FEC: Forward Error Correction

FBSS: Fast BS Switching

HO: Handover

HHO: Hard Handover

ISI: Inter Symbol Interference

IE: Information Element

LOS: Line Of Sight

MAC: Medium Access Control

MPDU: MAC Protocol Data Units

MSDU: MAC Sevice Data Units

MPEG: moving pictures experts group

MS: Mobile Station

MDHO: Macro Diversity Handover

NLOS: Non-Line Of Sight

nrtPS: non-real-time Polling Service

NWG: Network Working Group

OFDM: Orthogonal Frequency Division Multiplexing

OFDMA: Orthogonal Frequency Division Multiple Access

PDA: Personal Digital Assistant

PER: Packet Error Rate

PHY: Physical Layer

PMP: Point to Multi-Point

QAM: Quarter Amplitude Modulation

QoS: Quality of Service

rtPS: real time Polling Service

SDU: Service Data Units

SNR: Signal to Noise Ratio

SS: Subscriber Station

TDD: Time Division Duplex

TDM: Time Division Multiplexing

TDMA: Time Division Multiple Access

UCD: Uplink Channel Descriptor

UGS: Unsolicited Grant Service

UL-MAP: Uplink Map Message

VBR: Variable Bit-Rate

VoIP: Voice over IP

WLAN: Wireless Local Area Networks

WMAN: Wireless Metropolitan Area Network

WiBro: Wireless Broadband

WiMAX: Worldwide interoperability for Microwave Access

CHAPTER 1
INTRODUCTION

WiMAX is an acronym meaning Worldwide Interoperability for Microwave Access (WiMAX). WiMAX is based on Wireless Metropolitan Area Networking (WMAN) standards [1] developed by the IEEE 802.16 group. WiMAX enables the delivery of broadband wireless services anytime, anywhere. The IEEE 802.16 standard was developed to deliver Non-Line-Of-Sight (NLOS) connectivity between a subscriber station and base station with typical cell radius of three to ten kilometers. WiMAX systems can be expected to deliver capacity of up to 40 Mbps per channel. This is enough bandwidth to simultaneously support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL (Digital Subscriber Line) speed connectivity. A broad industry consortium, the WiMAX Forum [2] has begun certifying broadband wireless products for interoperability and compliance with a standard. The WiMAX mobile network deployments are to provide up to 15 Mbps of capacity within a typical cell radius of up to three kilometers. WiMAX technology already has been incorporated in notebook computers and PDAs (Personal Digital Assistant) to deliver high speed mobile Internet services anytime, anywhere.

1.1 IEEE 802.16 and WiMAX

The IEEE 802.16 Working Group is the IEEE group for Wireless Metropolitan Area Networks (WMANs) air interface for Fixed Broadband Wireless Access Systems. IEEE 802.16 group [3] was formed in 1998 to develop standards and recommended practices to support the development and deployment of fixed broadband wireless access systems. The first 802.16 standard was approved in December 2001. IEEE-802.16a was an amendment to 802.16 . 802.16a was ratified in January 2003 and was intended to provide last mile fixed broadband access 802.16c.

In September 2003, a revision project called 802.16d commenced. This project concluded in 2004 with the release of 802.16-2004 which replaced all prior versions including the a/b/c amendments and formed the basis for the first WiMAX solution. These early WiMAX solutions based on IEEE 802.16-2004 targeted fixed applications, and are referred to as Fixed WiMAX [4].

An amendment to 802.16-2004, IEEE 802.16e-2005 (formerly known as IEEE 802.16e), addressing mobility, was concluded in December 2005. The IEEE 802.16e-2005 forms the basis for the WiMAX solution for nomadic and mobile applications and is often referred to Mobile WiMAX [5].

The basic characteristics of the various IEEE 802.16 standards are summarized in Table 1.1.

Table 1.1 Basic Data on IEEE 802.16 Standards [6]

Parameters	**802.16**	**802.16-2004**	**802.16e-2005**
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM

Parameters	**802.16**	**802.16-2004**	**802.16e-2005**
Gross data rate	32–134.4Mbps	1–75Mbps	1–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/OFDMA	Burst TDM/TDMA/OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

1.2 WiMAX Architectural Issues

Various architectural issues involved with WiMAX like point to point Vs point to multipoint, Los Vs NLOS are discussed in following subtopics:

1.2.1 P2P Vs PMP

There are two scenarios for wireless deployment: point-to-point and point-to-multipoint.

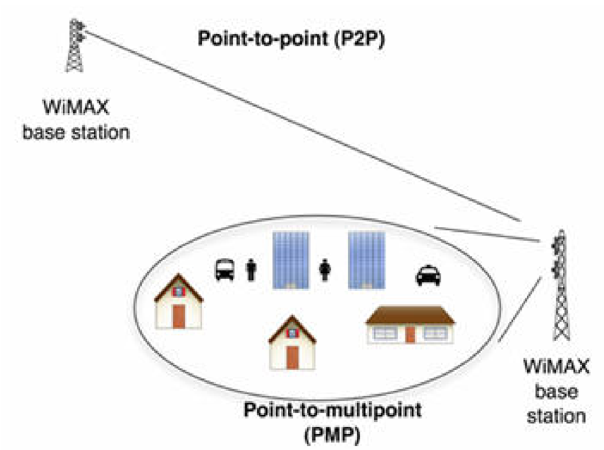

Figure 1.1: Point-to point and point-to-multipoint configurations[7]

Point-to-Point (P2P)

Point to point is used where there are two points of interest: one sender and one receiver. This is also a scenario for backhaul or the transport from the data source (data center, co-lo facility, fiber POP, Central Office, etc) to the subscriber or for a point for distribution using point to multipoint architecture. Backhaul radios comprise an industry of their own within the wireless industry. As the architecture calls for a highly focused beam between two points range and throughput of point-to point radios will be higher than that of point-to-multipoint products.

Point-to-Multipoint (PMP)

As seen in the figure above, point-to-multipoint is synonymous with distribution. One base station can service hundreds of dissimilar subscribers in terms of bandwidth and services offered.

1.2.2 LOS Vs NLOS

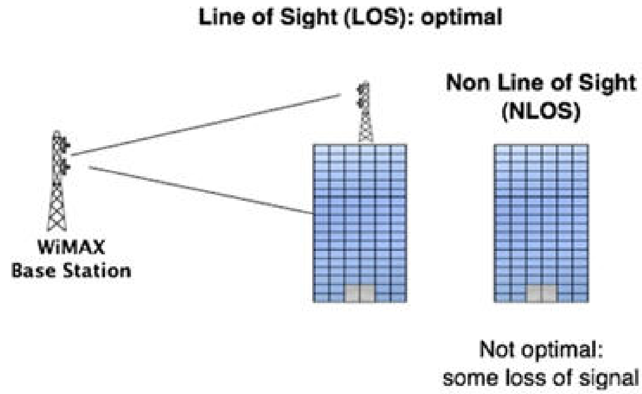

Figure 1.2: The difference between line of sight and non-line of sight [7]

Earlier wireless technologies were unsuccessful in the mass market as they could not deliver services in non-line-of-sight scenarios. This limited the number of subscribers they could reach. WiMAX functions best in line of sight situations and, unlike those earlier technologies, offers acceptable range and throughput to subscribers who are not line of sight to the base station. Given WiMAX's ability to deliver services non-line-of-sight, the WiMAX service provider can reach many customers in high-rise office buildings to achieve a low cost per subscriber because so many subscribers can be reached from one base station.

1.3 WIMAX TYPES

Various WiMAX types like Fixed WiMAX and Mobile WiMAX are discussed in following subtopics:

1.3.1 Fixed WiMAX

WiMAX provides fixed, portable or mobile non-line-of sight service from a base station to a subscriber station, also known as customer premise equipment (CPE). Some goals for WiMAX include a radius of service coverage of 6 miles from a WiMAX base station for point-to-multipoint, non-line-of-sight (see following pages for illustrations and definitions) service. This service should deliver approximately 40 megabits per second (Mbps) for fixed and portable access applications. That WiMAX cell site should offer enough bandwidth to support hundreds of businesses with T1 speeds and thousands of residential customers with the equivalent of DSL services from one base station.

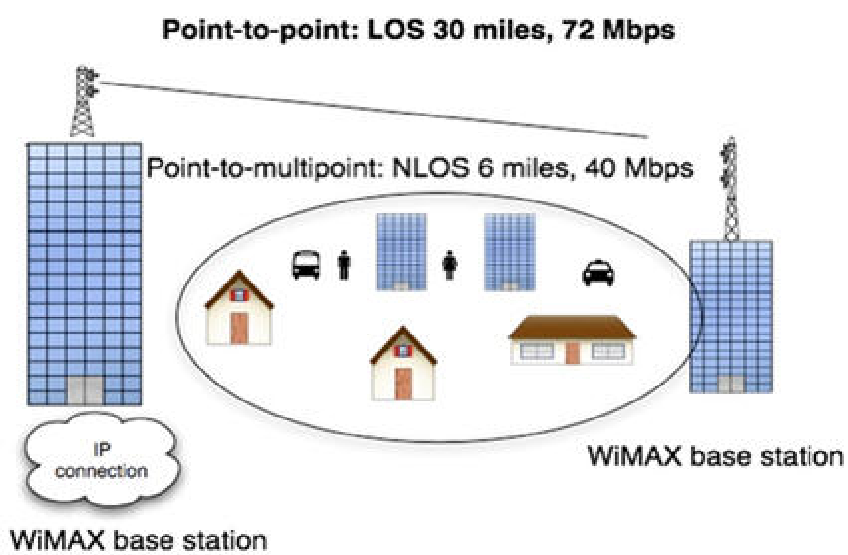

Figure 1.3 Fixed WiMAX [7]

1.3.2 Mobile WiMAX

Mobile WiMAX takes the fixed wireless application a step further and enables cell phone-like applications on a much larger scale. For example, mobile WiMAX enables streaming video to be broadcast from a speeding police or other emergency vehicle at over 70 MPH. It potentially replaces cell phones and mobile data offerings from cell phone operators such as EvDo and HSDPA. In addition to being the final leg in a quadruple play, it offers superior building penetration and improved security measures over fixed WiMAX. Mobile WiMAX will be very valuable for emerging services such as mobile TV and gaming.

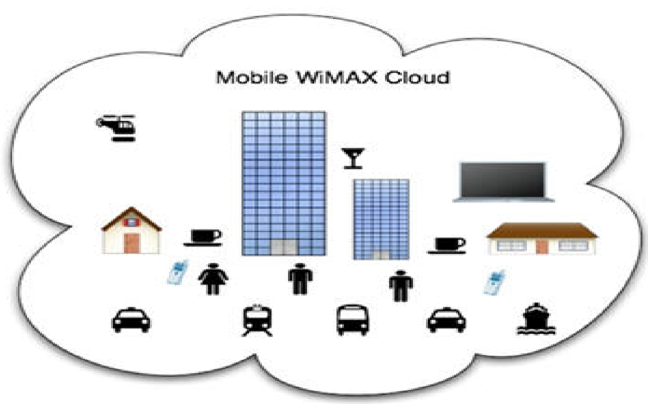

Figure 1.4 Mobile WiMAX [7]

1.4 WiMAX Reference Network Architecture

The IEEE 802.16e-2005 standard provides the air interface for WiMAX but does not define the full end-to-end WiMAX network. The WiMAX Forum's [8] Network Working Group (NWG), is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface. The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators. The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. The overall network may be logically divided into three parts:

(1) mobile stations used by the end user to access the network

(2) the access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.

(3) the connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

Base station (BS): The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP proxy, key management, session management, and multicast group management.

Access service network gateway (ASN-GW): The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys, AAA client functionality, establishment and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.

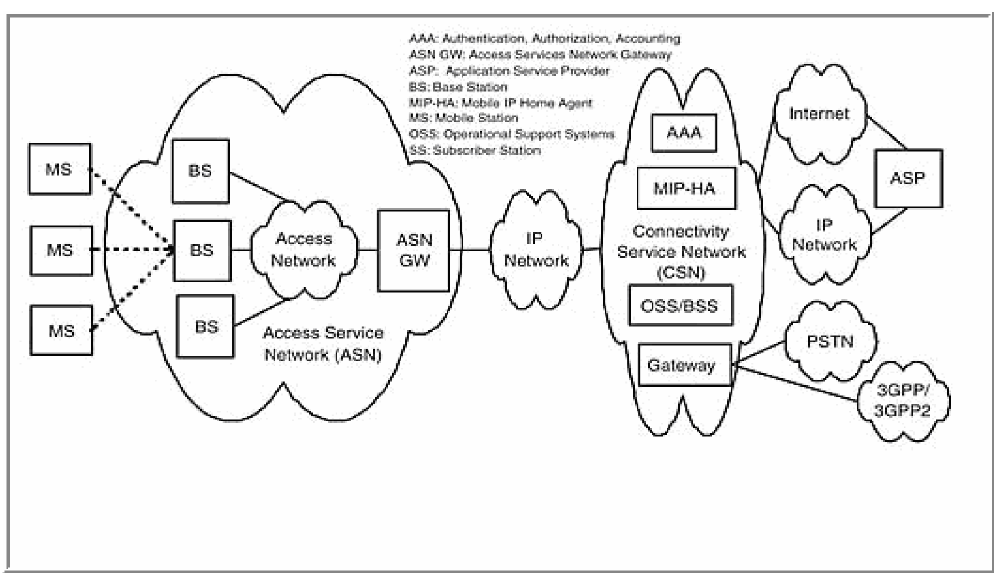

Figure 1.5: IP-Based WiMAX Network Architecture[9]

Connectivity service network (CSN): The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2.

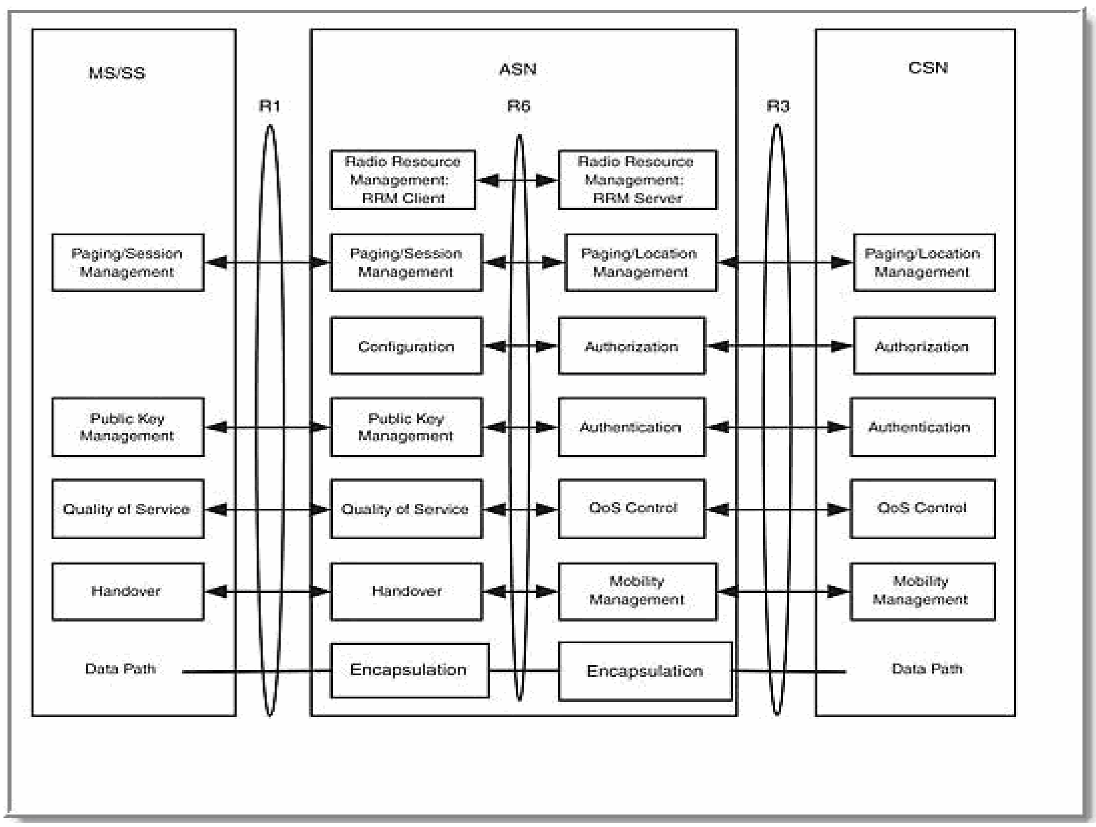

Figure 1.6 Functions performed across reference points [9]

In addition to functional entities, the reference architecture defines interfaces, called reference points, between function entities. The interfaces carry control and management protocols mostly transport-layer protocols—in support of several functions, such as mobility, security, and QoS, in addition to bearer data. The WiMAX network reference model defines reference points between:

(1) MS and the ASN, called R1, which in addition to the air interface includes protocols in the management plane

(2) MS and CSN, called R2, which provides authentication, service authorization,IP configuration, and mobility management,

(3) ASN and CSN, called R3, to support policy enforcement and mobility management

(4) ASN and ASN, called R4, to support inter-ASN mobility,

(5) CSN and CSN, called R5, to support roaming across multiple NSPs,

(6) BS and ASN-GW, called R6, which consists of intra-ASN bearer paths and IP tunnels for mobility events.

(7) BS to BS, called R7, to facilitate fast, seamless handover.

1.5 Features of 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. Some of the more salient features [9] that deserve highlighting are as follows:

Very high peak data rates: WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum. More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively..

OFDM-based physical layer: The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions. OFDM is now widely recognized as the method of choice for mitigating multipath for broadband wireless.

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.

Adaptive modulation and coding (AMC): WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed on a per user and per frame basis, based on channel conditions. The adaptation algorithm typically calls for the use of the highest modulation and coding scheme that can be supported by the signal-to-noise and interference ratio at the receiver such that each user is provided with the highest possible data rate.

Support for advanced antenna techniques: The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques[10], such as beamforming, space-time coding, and spatial multiplexing. These schemes can be used to improve the overall system capacity and spectral efficiency by deploying multiple antennas at the transmitter and/or the receiver.

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 QoS parameters [11] such as constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic. WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

Link-layer retransmissions: For connections that require enhanced reliability, WiMAX supports automatic retransmission requests (ARQ) at the link layer. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted. WiMAX also optionally supports hybrid-ARQ, which is an effective hybrid between FEC and ARQ.

IP-based architecture: The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture [12] relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility. Reliance on IP allows WiMAX to ride the declining costcurves of IP processing, facilitate easy convergence with other networks, and exploit the rich ecosystem for application development that exists for IP.

Robust security: WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol. The system also offers a very flexible authentication architecture based on Extensible Authentication Protocol (EAP), which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

1.6 Applications of WiMAX

WiMAX has the potential to replace a number of existing telecommunications infrastructures. In a fixed wireless configuration it can replace the telephone company's copper wire networks, the cable TV's coaxial cable infrastructure while offering Internet Service Provider (ISP) services. In its mobile variant, WiMAX has the potential to replace cellular networks.

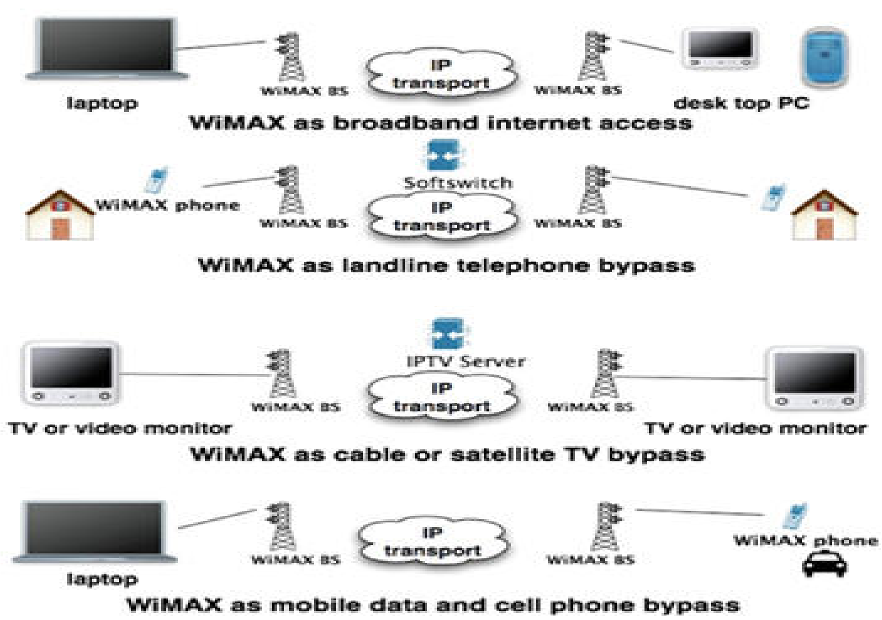

Figure 1.7: WiMAX Applications [12]

1.6.1 WiMAX VoIP

A fixed wireless solution not only offers competitive internet access, it can do the same for telephone service bypassing the telephone company's copper wire network. Voice over Internet Protocol (VoIP) offers a wider range of voice services at reduced cost to subscribers. The figure 1.8 illustrates a typical solution where a WiMAX service provider can obtain wholesale VoIP services (no need for WiMAX service provider to install VoIP softswitch) at $5/number/month and resell to enterprise customers at $50.

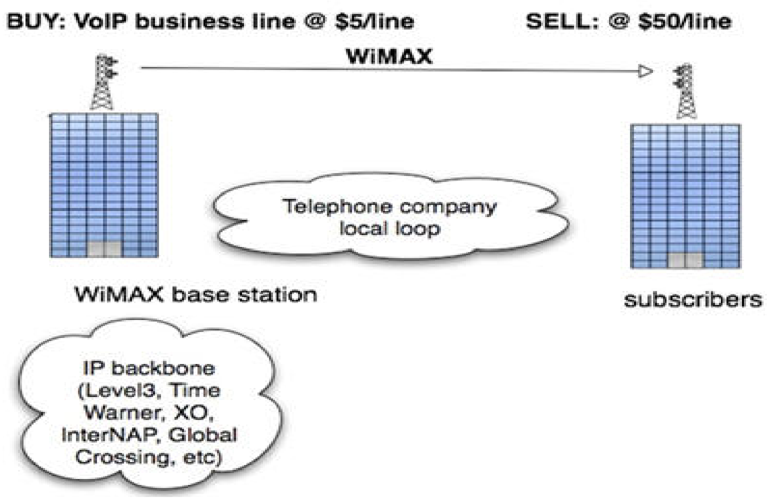

Figure 1.8: VoIP over WiMAX

1.6.2 Mobile TV

Cell phone service providers now offer some limited mobile TV. Ultimately, the cell phone networks of today will not be able to handle the bandwidth demands posed by mobile TV. The video iPod from Apple has launched a revolution in TV viewing. Initially, TV viewers had to watch what programming was available when TV executives made it available. Mobile TV devices allow viewers to watch "what" they want, "when" they want and here comes the new part: "where" they want. WiMAX drives demand for residential broad-band so that the consumer can download the video they want to watch and facilitates live video streamed over a WiMAX connection while the viewer is mobile.

1.6.3 WiMAX & IPTV

The third leg of the triple play is Internet Protocol Television (IPTV). IPTV enables a WiMAX service provider to offer the same programming as cable or satellite TV service providers. IPTV, depending on compression algorithms, requires at least 1 Mbps of bandwidth between the WiMAX base station and the subscriber.

In addition to IPTV programming, the service provider can also offer a variety of video on demand (VoD) services. The subscriber can select programming for their television both home and mobile viewing needs.

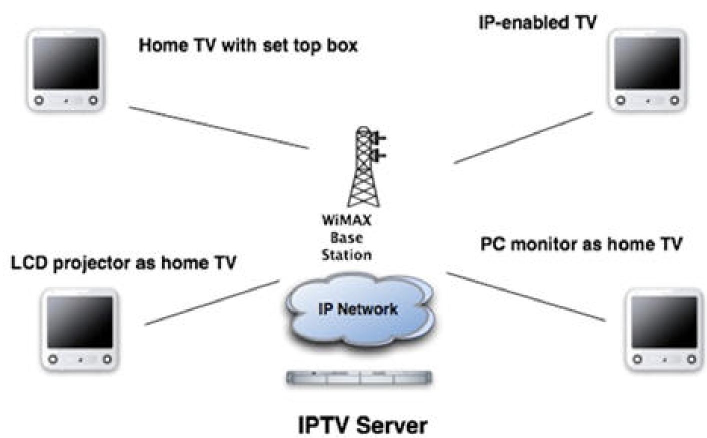

Figure 1.9: IPTV over WiMAX

CHAPTER 2

LITERATURE SURVEY

WiMAX Handover involves various Physical as well as MAC Layer issues. These issues corresponding to each layer are described in this section.

2.1 Physical Layer

The physical layer specifications can be divided into two groups: that for operation in the 10-66 GHz range, and that for operation in the 2-11 GHz range.

Operation in 10-66 GHz range

In the IEEE 802.16-2004 standard, the PHY specification for this range is referred to as the Wireless MAN-SC, the SC standing for Single Carrier Modulation. This was chosen at such high frequencies, it was assumed that Line of Sight was necessary. The BS transmits a Time Division Multiplexing, TDM, signal and provides access by means of Time Division Multiple Access, TDMA. In TDMA, symbols are transmitted in non-overlapping time slots and each client gets access to a given time slot.

Operation in 2-11 GHz range

Given that in a metropolitan area, NLOS operation was deemed important, the IEEE 802.16a standard introduced operation in the 2-11 GHz range.

There are three schemes specified in the IEEE 802.16-2004 standard:

- Single carrier
- Orthogonal Frequency Division Multiplexing(OFDM)
- Orthogonal Frequency Division Multiple Access(OFDMA)

OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications. It is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment. In this section, we cover the basics of OFDM and other physical layer issues.

2.1.1 Multicarrier Modulation (OFDM)

OFDM belongs to a family of transmission schemes called multicarrier modulation, which is based on the idea of dividing a given high-bit-rate data stream into several parallel lower bit-rate streams and modulating each stream on separate carriers—often called subcarriers, or tones. Multicarrier modulation schemes eliminate or minimize Inter Symbol Interference (ISI) by making the symbol time large enough so that the channel-induced delays—delay spread being a good measure of this in wireless channels. Therefore, in high-data-rate systems in which the symbol duration is small, being inversely proportional to the data rate, splitting the data stream into many parallel streams increases the symbol duration of each stream such that the delay spread is only a small fraction of the symbol duration. OFDM is a spectrally efficient version of multicarrier modulation, where the subcarriers are selected such that they are all orthogonal to one another over the symbol duration, thereby avoiding the need to have non-overlapping subcarrier channels to eliminate intercarrier interference.

2.1.2 Subchannelization (OFDMA)

The available subcarriers may be divided into several groups of subcarriers called subchannels. Fixed WiMAX based on OFDM-PHY allows a limited form of subchannelization in the uplink only. The standard defines 16 subchannels, where 1, 2, 4, 8, or all sets can be assigned to a subscriber station (SS) in the uplink.

Mobile WiMAX based on OFDMA-PHY, however, allows subchannelization in both the uplink and the downlink, and here, subchannels form the minimum frequency resource-unit allocated by the base station. Therefore, different subchannels may be allocated to different users as a multiple-access mechanism. This type of multiaccess scheme is called Orthogonal Frequency Division Multiple Access (OFDMA).

OFDM takes a block of serial symbols and transmits them in parallel using carriers, which are mathematically orthogonal. Say we have N symbols to be transmitted serially, with period Ts. If we take those N symbols and transmit them on N parallel orthogonal carriers, each with period T, we in effect reduce the symbol rate on each sub-carrier, as we have T = NTs. This reduction in symbol rate means that the effect of delay spread is reduced, and so there is no need for equalization at the receiver. OFDMA works by assigning a certain subset of the sub-carriers to each client to provide multiple-access.

2.1.2 Adaptive Modulation and Coding (AMC)

The physical layer also provides adaptive modulation. This means that transmission parameters (modulation scheme, channel coding and FEC settings) can be modified on a frame by frame basis for each SS. Therefore, an SS who is far away from the BS and may see poor channel conditions will use more robust transmission parameters than a SS who is closer to the BS. The parameters a SS uses are known as its burst profile. This burst profile will have to be negotiated between the BS and the SS. The modulation schemes provided are 64-QAM, 16-QAM and QPSK, in order of decreasing efficiency and increasing robustness. For example, the use of 64-QAM will require a better signal to noise ratio than 16-QAM.

Table 2.1 lists the various modulation and coding schemes supported by WiMAX. In the downlink, QPSK, 16 QAM, and 64 QAM are mandatory for both fixed and mobile WiMAX; 64 QAM is optional in the uplink. FEC coding using convolutional codes is mandatory.

Table 2.1 Modulation and Coding Supported in WiMAX [13]

	Downlink	**Uplink**
Modulation	BPSK, QPSK, 16 QAM, 64 QAM; BPSK optional for OFDMA-PHY	BPSK, QPSK, 16 QAM; 64 QAM optional
Coding	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6 Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC, RS-Codes for OFDM-PHY	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6 Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC

2.2 MAC-Layer

The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the physical layer. The MAC layer takes packets from the upper layer—these packets are called MAC service data units (MSDUs)—and organize them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse. WiMAX supports only IP and Ethernet at this time.

2.2.1 WiMAX Reference Model

Various sub-layers of MAC layer and corresponding issues are clear from figure 2.1 WiMAX Reference model:

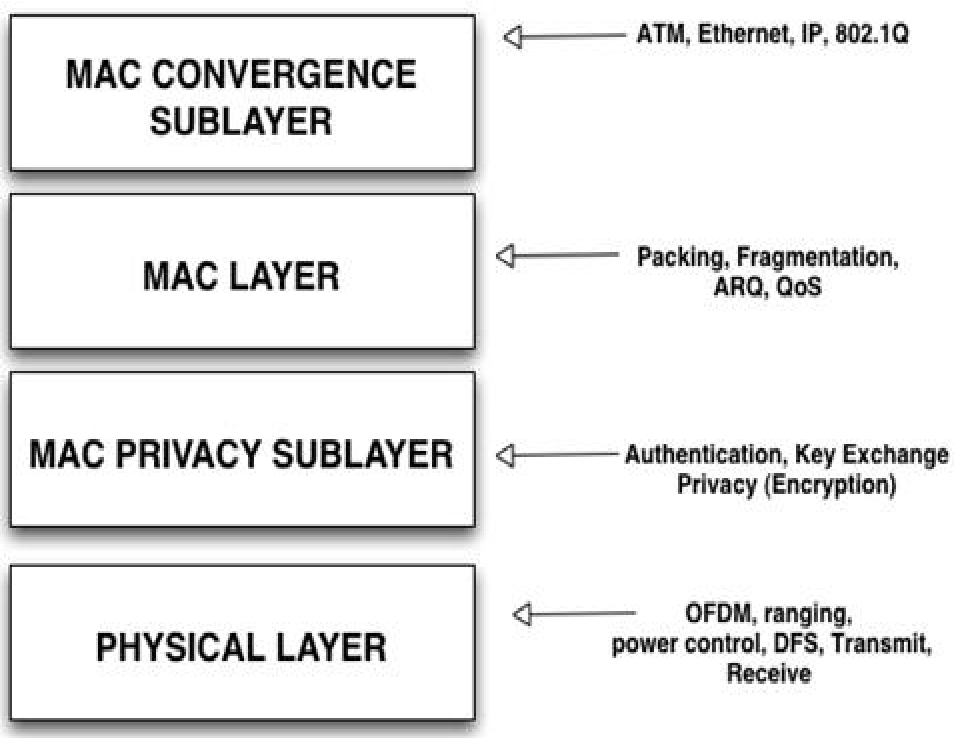

Figure 2.1: WiMAX Reference Model [14]

(1) Service Specific Convergence Sublayer

The IEEE 802.16 standards are very much connection oriented. Each service is assigned a connection with a varying level of quality of service, QoS. There are three management connections, coupled with transport connections for transmission of data. The purpose of the Service Specific Sublayer, is to accept higher layer PDUs and classify them. Based on this classification, they are assigned to a given connection, with a given QoS. The Service Specific Sublayer supports ATM services as well as packet based IP services.

(2) Common Part Sublayer

The purpose of the Common Part Sublayer is to facilitate the sharing of the transmission medium. The system works on a PMP basis, where every station hears the same downlink transmission. The BS grants access to the uplink. This access is very much driven by the class of service and the QoS provisions such a service requires.

2.2.2 MAC Management Messages

In total, there are 49 MAC management messages. The most important ones as regarding this thesis are illustrated below:

RNG-REQ, Ranging Request (Transmitted on Basic or Initial Ranging connection)

This message is transmitted periodically to determine network delay and to request a power or burst profile change.

RNG-RSP, Ranging Response (Transmitted on Basic or Initial Ranging connection)

This message contains the response to RNG-REQ message, containing such parameters that are relevant to the request. If RNG-REQ was sent on the initial ranging connection, this message also contains the connection identifier for the basic and primary connection assigned to this SS.

REG-REQ, Registration Request (Transmitted on Primary connection)

Sent by a SS in order to register with the BS and to negotiate the SS's capabilities, such as its IP version, ARQ parameters and convergence layer capabilities.

REG-RSP, Registration Response (Transmitted on Primary connection)

Sent by BS in response to a REG-REQ. It contains the connection identifier for the SS's secondary connection, in addition to relevant parameters for the SS's capabilities.

2.2.3 IEEE 802.16 Frame Structure

Each frame is a fixed length, and is divided into first the Downlink Sub-frame and then the Uplink Sub-frame. The division between these two sub-frames is dynamic.

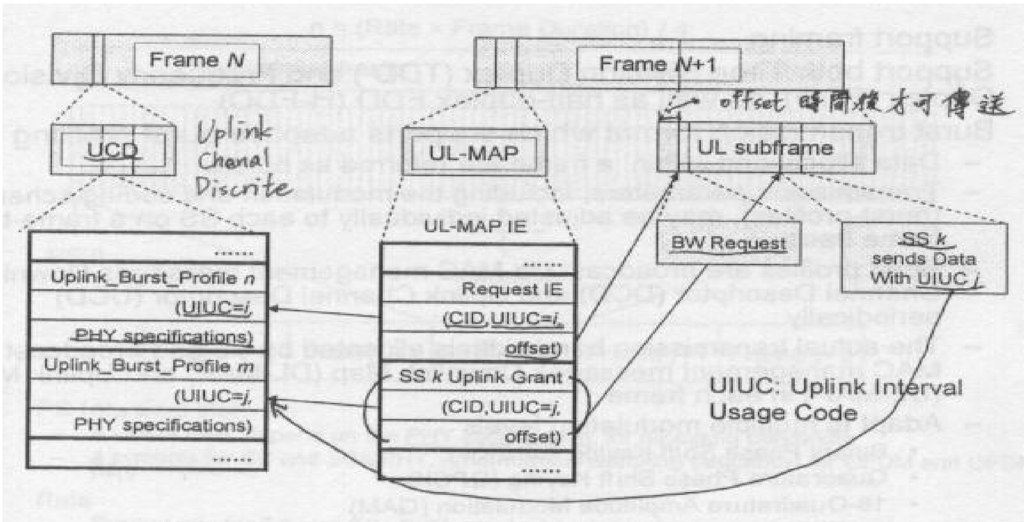

Figure 2.2 : Transmission Parameters in MAC Messages[14]

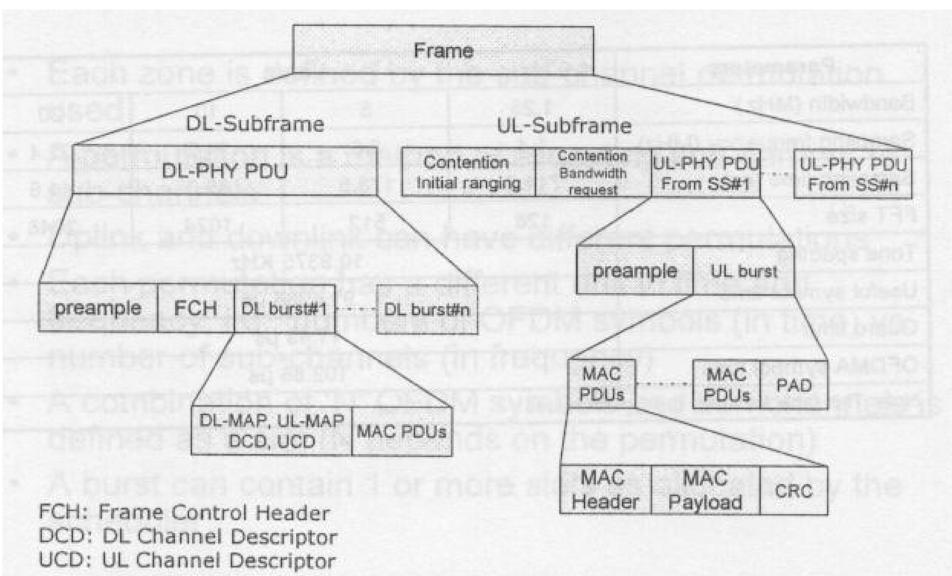

Figure 2.3: Frame Structure of OFDMA [14]

- DL frame
  - Start with a preamble
  - Frame Control Header (FCH)
  - DL-MAP, specifies the downlink allocations for each user
  - UL-MAP, provides the uplink allocations for each user
  - DCD and UCD
- UL frame
  - Contains user-specific data bursts of various size based on the available power and QoS
  - Contain a contention-based Ranging channel, which consists of multiple subchannels and is used by SSs to gain access and maintain connections

Downlink Sub-frame

In a given frame, the downlink sub-frame occurs first. As can be seen from figure 2.4, first there is a preamble. The purpose of this is to enable the SS to synchronize to the frame, as it may have lost synchronization at the end of the previous frame. Following this preamble, there is a Frame Control Section.

The following messages may be present here, DL-MAP, UL-MAP, DCD and UCD. The DCD and UCD get transmitted at a given interval, whereas the DL-MAP and UL-MAP must be present at the start of every frame.

Downlink-MAP, DL-MAP:

The purpose of the downlink map is to define the access to the downlink information. It tells each SS at what time changes in modulation and coding will occur. The subscriber station listens to all the data it is able to until it reaches data for itself.

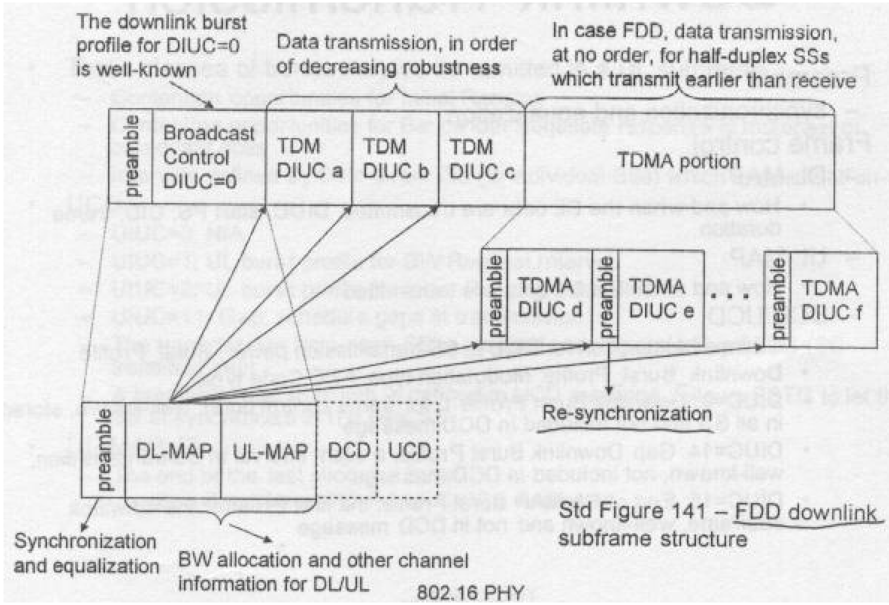

Figure 2.4: Downlink Sub-frame [15]

Uplink-MAP, UL-MAP:

The purpose of the UL-MAP is to define access to the uplink channel. It specifies a burst profile and a time for each SS to transmit its data.

Downlink Channel Descriptor, DCD:

The purpose of DCD is to specify characteristics of a given downlink physical channel. The BS transmits it at given interval, which can have a maximum value of 10 seconds.

Uplink Channel Descriptor, UCD:

The purpose of this is similar to the DCD, in that it specifies the characteristics of the uplink channel and is transmitted at a given interval, which cannot exceed 10 seconds. This message also contains required information for initial ranging contention. Following this frame control section, the BS transmits its TDM data.

Uplink Sub-frame structure

The structure of the uplink sub-frame is more straightforward and can be seen in Fig 2.5.

- Three class of bursts may be transmitted in a UL subframe
    - Initial Ranging
    - Bandwidth Requests response to multicast or broadcast polls
    - Data Grant IEs
- UCD
    - UIUC=0 : N/A
    - UIUC=1 : UL burst profile for BW Request Interval
    - UIUC=2 : UL burst profile for Initial Ranging Interval
    - UIUC=11 : Gap, schedule gaps in transmission
- UL-MAP_IE
    - The end of the last allocated burst

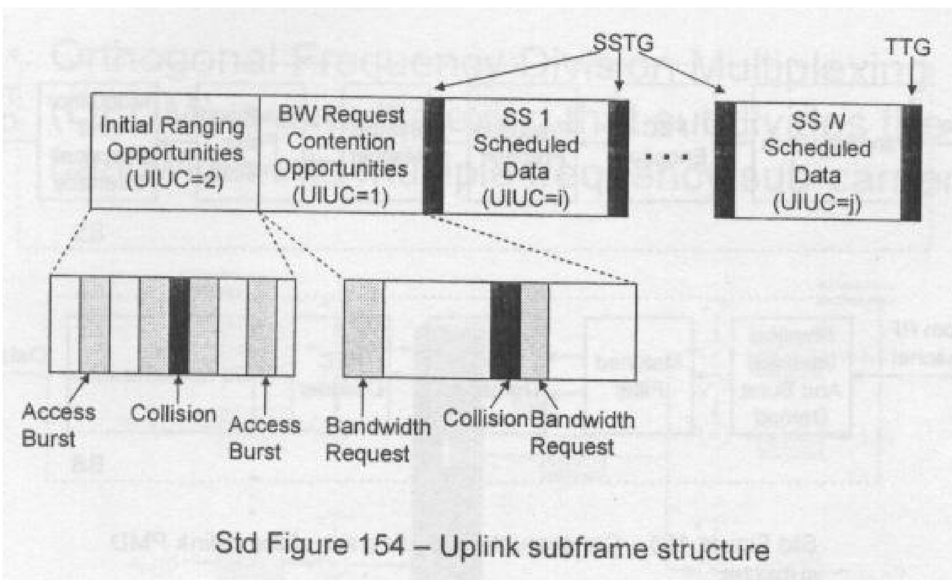

Figure 2.5: Uplink Sub-Frame [15]

Firstly we have initial ranging opportunities. This is to allow any SS, which have not already registered to send a ranging request message. The purpose of this message for a SS, which is not registered, is to discover network delay and to negotiate a burst profile or power change. Because this is the first communication this SS is having with the BS, there are no pre defined uplink opportunities. All SS's, without such uplink opportunities, transmit their range request in this initial ranging opportunity period. Following this initial ranging opportunity, the SS's transmit their data via TDMA, in the time slot provided to them by the UL-MAP.

2.3 Handover in IEEE 802.16 Standard

The section of the report will focus on Handover in WiMAX. The standard defines Mobile Stations, MS's. It also defines HandOver, HO, to be the process in which, "an MS migrates from the air interface provided by one BS to the air interface provided by another BS" [16]. The best way to look at the amendments to the MAC layer, is to follow through the HO process for various scenarios.

2.3.1 MAC Layer Handover Procedure

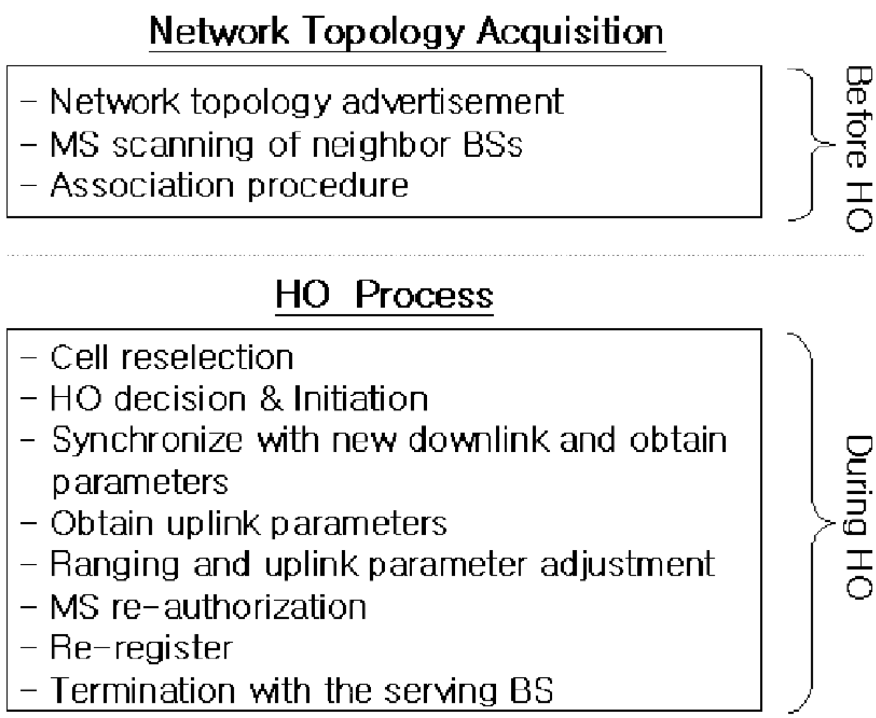

Figure 2.6: MAC Layer Handover Procedure [17]

A. Network Topology Advertisement

The BSs periodically broadcast Mobile Neighbor Advertisement (MOB_NBR_ADV) control messages . These messages contain both physical layer (i.e., radio channel) and link layer (e.g., MAC address) information.By means of such broadcasts, the MS becomes aware of the neighboring BSs. The MS then triggers the second-phase.

B. Scanning/ranging Procedure

In the second phase of HO, the MS scans and synchronizes with the neighboring BSs based on channel information from the neighbor advertisement. If the synchronization successes, it then starts the ranging procedure.The scanning and ranging processes are shown in Fig 2.7. The MS first sends a Mobile Scanning Request (MOB_SCNREQ) message to the neighboring BS with a potential target BS list (selected in the previous phase). The serving BS replies a Mobile Scanning Response (MOB_SCN-RSP) message to the MS to allocate a scanning duration. The serving BS may negotiate directly with the listed BSs the allocation of a unicast ranging opportunity. If successful, the ranging procedure can be non-contention-based.

Else, the MS starts a contention-based CDMA procedure to be allocated a ranging slot by the neighboring BS. For the sake of simplicity, in analysis we always assume non-contention-based-ranging. Then the MS starts a hand-shake ranging procedure with the neighboring BS for the OFDMA uplink synchronization and parameter (e.g., transmission power) adjustment. This process may contain multiple message (Ranging Request (RNG-REQ) and Ranging Response (RNG-RSP) transmission and parameter adjustment transactions. This procedure ends after the MS has completed ranging with all its neighbors. In the ranging phase, a MS may switch to a new channel, thus temporally loosing connection with the serving BS.

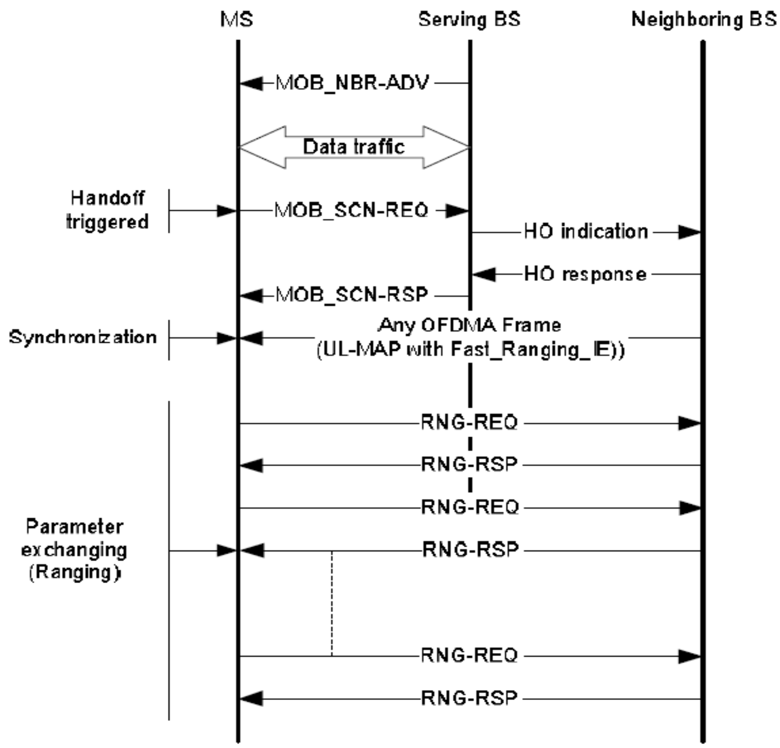

Figure 2.7: Scanning and Ranging [17]

C. HO Decision and Initiation

The HO trigger decision and initiation can be originated by both the MS and the BS using a MS HO Request message (MOB_MSHO-REQ) or a BS HO Request message (MOB_BSHO-REQ) respectively. Here we use the HO started by the MS as an example as illustrated in Fig. 2.8. The MS makes a decision about which BS(s) is (are) its target(s). A HO begins with when the MS sends a MOB_MSHO-REQ message to its serving BS indicating one or more possible target BSs. The serving BS may obtain directly from potential target BSs the expected MS performance at the target BSs through the exchange of HO indication and response messages. After receiving a response from a target BS (MOB_BSHORSP), the MS notifies the serving BS about its decision to perform a HO by means of a HO Indication (MOB_HO-IND) message. The MS can also ask the serving BS to negotiate with the target BS the allocation of a ranging opportunity. If necessary, the MS may start ranging after HO initiation. The HO decision and initiation process does not provoke connectivity break-up nor does it add latency. However, the possible ranging procedure after does introduce additional latency.

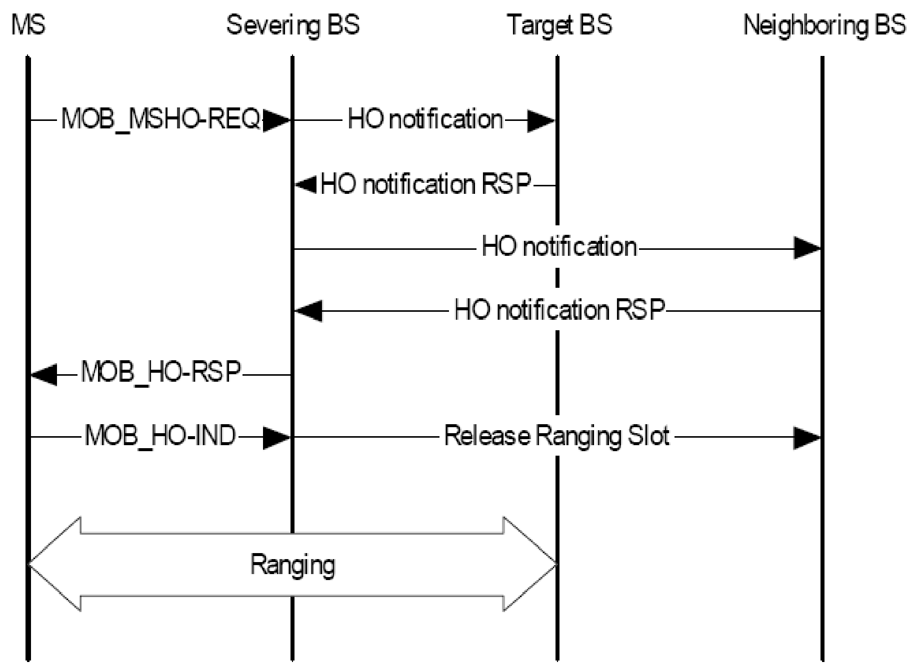

Figure 2.8: HO decision and Initiation [17]

D. Network Re-entry

After all the physical parameter adjustments have been completed successfully, the network re-entry process is initiated to establish connectivity between the MS and the target BS. As defined in IEEE 802.16e, this procedure may include capability negotiation, authentication and registration transactions.Because the MS must wait until the re-entry procedure is completed successfully before it can restore communication, duration of this phase should be taken account into the entire HO latency.

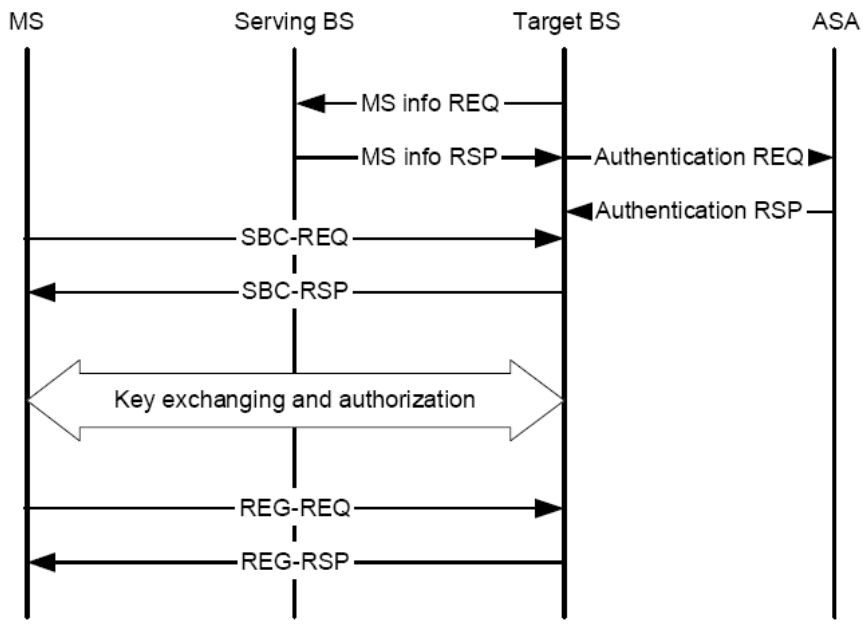

Figure 2.9: Network Re-entry Process [17]

2.3.2 Types of Handover

In an attempt to cover all eventualities, provision has been made for several different types of HO:

2.3.2.1 MS Initiated HO

When an MS is losing signal quality with its serving BS it may wish to move to a new BS. This is inherently linked with mobility and may be used when an MS is moving out of the coverage of its serving BS. Another scenario is that the MS may wish to move if it can get a higher QoS at another BS. In such situations, the MS will initiate HO. As this will be the most common type of HO, it is the one implemented in simulation. It is important to note the methodology of deciding whether or not to perform HO is not included in the standard. The standard provides a means to gain information about neighbouring stations in order to make this decision.

(a) Neighbour Advertisement

BS's should be capable of transmitting a Mobile Neighbour Advertisement, MOB_NBRADV message at a given interval. The purpose of this message is to inform all listening stations of the characteristics of any neighbouring base stations, which they may or may not wish to move to. It contains information such as the frequency of this BS, its BS identifier, the types of services it supports and its available radio resources (available channels etc.). This message is transmitted on the broadcast connection. An important parameter of this message is the frequency with which it is sent. The standard specifies a maximum of 1s. This is of relevance because if we have a mobile station moving at large speed, it may be moving through the range of coverage of each BS quicker than it receives the MOB_NBR-ADV message. In this case, it would be unable to perform HO. This parameter is thus one limit to the speed with which an MS can move through the network. The network administrator should decide on a value which is regular enough to facilitate all users, and yet not too frequent to disrupt efficiency.

(b) Neighbour Scanning

To facilitate a HO decision, the MS may perform scanning on possible target BS's. To do so, it first sends its serving BS a MOB_SCN-REQ message. This message tells the BS that it wishes to scan its neighbours. It specifies a length of time in frames for this interval and the type of association it will scan its neighbours with. There are three levels of association:

- Without Coordination: Target BS has no knowledge of approaching MS
- With Coordination: Serving BS coordinates association with requested target BS's.
- Network Assisted Association Reporting: Similar to previous method, with the exception that the RNG-RSP message is sent over the network backbone to the serving BS. The serving BS then puts all received RNG-RSP messages (from all BS that were canned) and transmits them to the MS in the form of an MOB_ASC_REPORT message.

The BS will then respond with a MOB_SCN-RSP message, which indicates the length of the approved scan and the association type for the scanning. The MS is now free to scan its neighbours. It can synchronise with a given BS's downlink transmissions and estimate the quality of the physical channel.

(c) Negotiating Handover with Serving BS

The next stage in the HO process is to send a MOB_MSHO-REQ message to the serving BS. This message is transmitted on the basic connection and contains a list of stations the MS recommends as targets. This list is generated by the results of scanning. On receipt of this message, the serving BS sends a HO-pre-notification message to all BS's on this list. It should then receive a HO-pre-notification-response from these stations. From these responses, the serving BS generates a list of target stations, which it sends to the MS in the MOB_BSHO-RSP message, also transmitted on the basic connection. Upon receipt of the MOB_BSHO-RSP message, the MS may perform HO. The serving BS is informed via a MOB_HO-IND message, transmitted on the basic connection. The MS may also cancel the HO in this message. If it is continuing with HO, it tells the BS that it is leaving that BS and it tells it the parameters of the target BS. The MS is now ready to register with the target BS and does this in the exact same way as outlined in the previous standards. The two diagrams on the following page illustrate the process discussed above. It is also possible for the target BS, on receipt of a HO-pre-notification message, to include in its UL-MAP a fast ranging Information Element, IE, which provides the MS undergoing HO, a non-contention based initial ranging opportunity. This is to decrease the overall speed of the HO process.

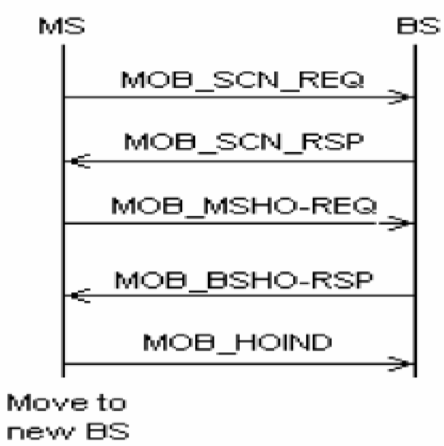

Figure 2.10: MS initiated HO Message exchange

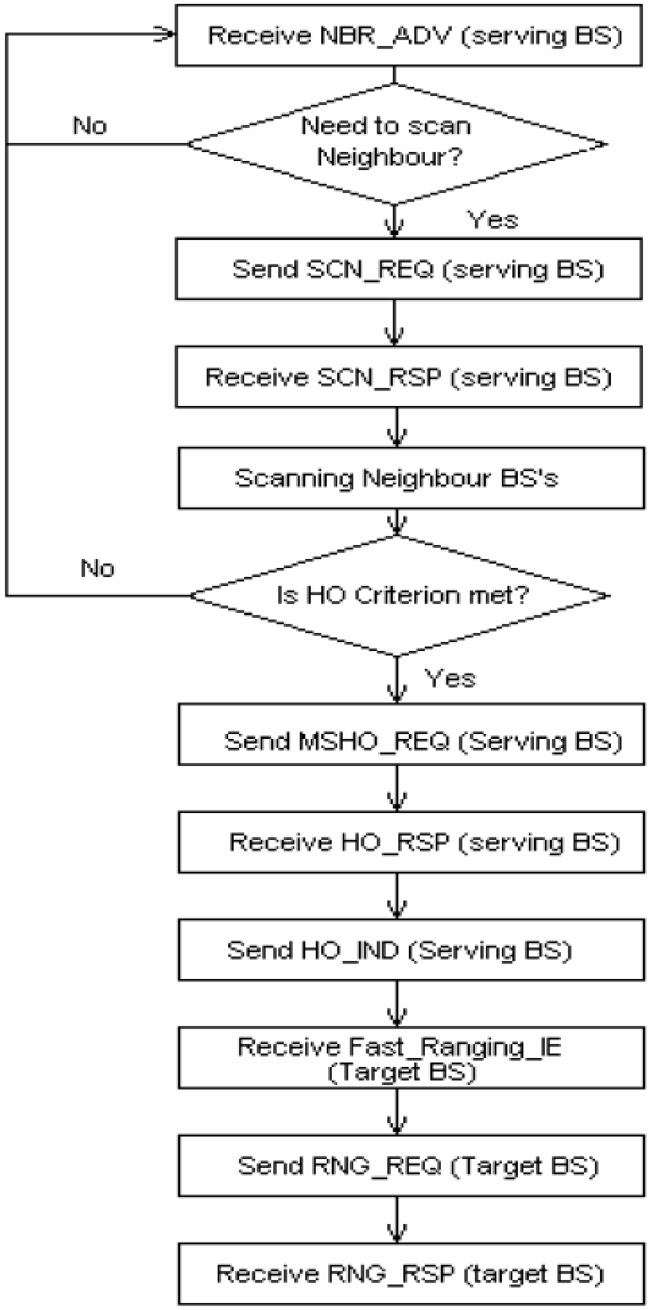

Figure 2.11: MS initiated HO (in the MS)

2.3.2.2 BS Initiated HO

The next case to look at is when the BS decides that the MS should move to another BS. This may be required if the serving BS decides it can no longer provide its client with the required QoS. It may also be used if the BS decides that the MS is moving out of range. These are similar examples as in the case where the MS initiates HO. However, it may be useful to have the BS make these decisions so as to centralise the HO procedure. This is because mobile users may have limited power resources and so any computation, which can be performed by the BS, is welcome.

Assuming that the MS has received the MOB_NBR-ADV message as described in the previous section, the first step here is for the BS to send the MS a MOB_BSHO-REQ message, to tell the MS it needs to perform HO and so to start scanning its neighbours. This message contains the BS's list of recommended target stations together with such relevant information as service level predictions and channel details. This message is transmitted on the basic connection.

On receipt of the MOB_BSHO-REQ message, the MS may scan the BS's detailed in this message. It then sends a MOB_BSHO-RSP to the serving BS, with its list of recommended stations. From here, the HO process is the same as for the MS initiated case. The process is illustrated in the flow chart on the next page.

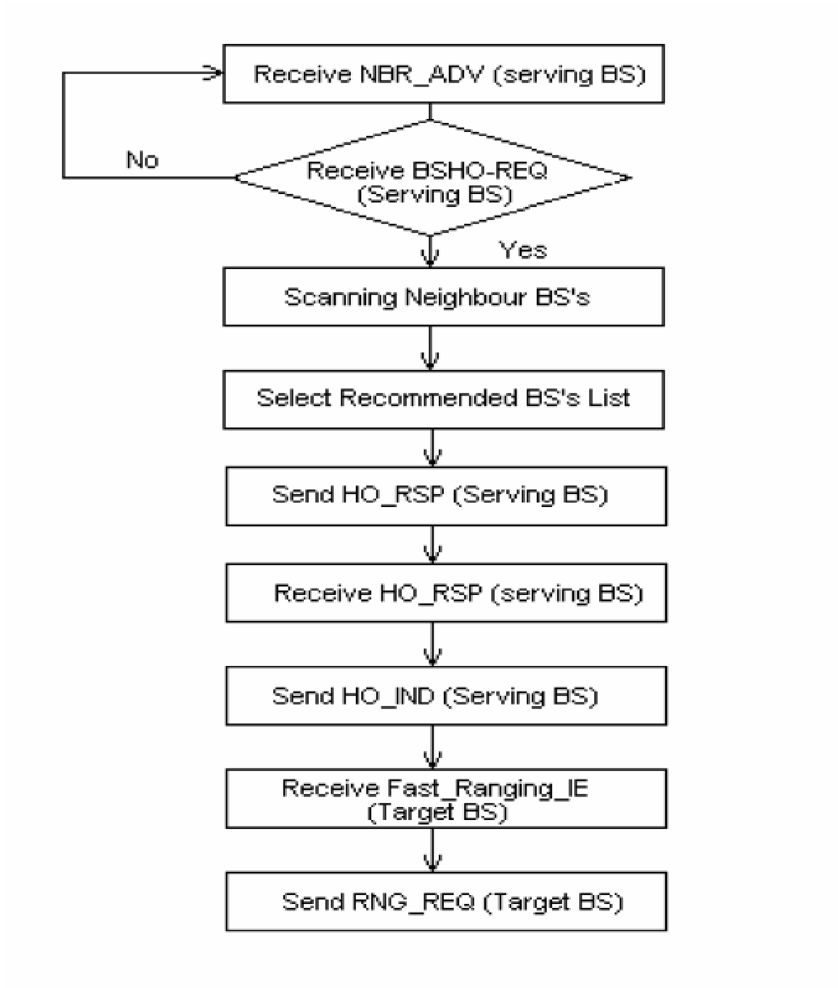

Figure 2.12: BS initiated HO (in the MS)

2.3.2.3 Sleep Mode

One final amendment worth noting is that of sleep mode. When mobility is introduced to the equation, clearly power becomes a concern. If a user is mobile, they may not be able to recharge their unit for quite some time, and so it is important to look at ways in which power can be conserved, much more so than in a fixed setting.

The IEEE 802.16e defines a new mode the MS can occupy, sleep mode. In sleep mode, the MS is no longer receiving any traffic from the BS and so it can set its power usage to the minimum. To enter sleep mode[18], the MS sends a MOB_SLP-REQ to the BS, requesting to enter sleep mode for a given duration. The BS may or may not approve, and does so in the form of a MOB_SLP-RSP message. Initially, the MS may go into sleep mode for a requested period of time, T. When this has expired, the MS leaves sleep mode and has a short listening interval to see if there is any traffic from the BS for it. If not, it resumes sleep mode, this time for an interval twice as long. This continues until the MS reaches a sleep interval a T_{max}. Therefore, the j_{th} sleep interval will be $2_j T$, or T_{max}, whichever is smaller. T_{max} is quite an important value. It has been shown that the larger this is, the more energy will be saved. However the trade off of this is that frame response time (the length of time it takes for an MS to respond to a frame destined for it) increases[13].

2.3.3 Criterion Effecting Handover in MAC Layer

Now Various Criterion effecting Handover Process in MAC layer are considered as follows:

2.3.3.1 Channel Access Mechanisms

The WiMAX standard supports several mechanisms by which an MS can request and obtain uplink bandwidth.The BS allocates dedicated or shared resources periodically to each MS, which it can use to request bandwidth. This process is called polling. Polling may be done either individually (unicast) or in groups (multicast). Multicast polling is done when there is insufficient bandwidth to poll each MS individually. When polling is done in multicast, the allocated slot for making bandwidth requests is a shared slot, which every polled MS attempts to use. WiMAX defines a contention access and resolution mechanism for the case when more than one MS attempts to use the shared slot. If it already has an allocation for sending traffic, the MS is not polled. Instead, it is allowed to request more bandwidth by:

(1) transmitting a stand-alone bandwidth request MPDU

(2) sending a bandwidth request using the ranging channel

(3) piggybacking a bandwidth request on generic MAC packets.

2.3.3.2 Quality of Service

Strong Quality of service control is achieved by using a connection-oriented MAC architecture, where all downlink and uplink connections are controlled by the serving BS. Before any data transmission happens, the BS and the MS establish a unidirectional logical link, called a connection, between the two MAC-layer peers. Each connection is identified by a connection identifier (CID), which serves as a temporary address for data transmissions over the particular link. To support a wide variety of applications, WiMAX defines five scheduling services (Table 2.2) that should be supported by the base station MAC scheduler for data transport over a connection.

Table 2.2: Service classes supported in WiMAX for prioritizing traffic [19]

Service Class	**Applications**	**QoS Specifications**
Unsolicited Grant Service (UGS)	VoIP	Jitter Tolerance Maximum Latency Tolerance Maximum Sustained Rate
Real-time Polling Service (rtPS)	Streaming audio or video	Traffic Priority Maximum Latency Tolerance Maximum Reserved Rate Maximum Sustained Rate
Extended real time Polling Services (ErtPS)	VoIP (Voice with Activity Detection)	Traffic Priority Maximum Latency Tolerance Jitter Tolerance Maximum Sustained Rate Maximum Reserved Rate
Non-real time polling services (nrtPS)	FTP	Traffic Priority Maximum Reserved Rate Maximum Sustained Rate
Best- Effort (BE)	Data Transfer, Web Browsing etc.	Traffic Priority Maximum Sustained Rate

2.3.3.3 Mobility Support

In addition to fixed broadband access, WiMAX envisions four mobility[19] related usage scenarios:

1. Nomadic. The user is allowed to take a fixed subscriber station and reconnect from a different point of attachment.

2. Portable. Nomadic access is provided to a portable device, such as a PC card, with expectation of a best-effort handover.

3. Simple mobility. The subscriber may move at speeds up to 60 kmph with brief interruptions (less than 1 sec) during handoff.

4. Full mobility: Up to 120 kmph mobility and seamless handoff (less than 50 ms latency and <1% packet loss) is supported.

2.3.3.4 Security Functions

Security is handled by a privacy sublayer within the WiMAX MAC. The key aspects of WiMAX security are as follow:

Support for privacy: User data is encrypted using cryptographic schemes using AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard).The 128-bit or 256-bit key used for deriving the cipher is generated during the authentication phase and is periodically refreshed for additional protection.

Device/user authentication: The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards. WiMAX terminal devices come with built-in X.509 digital certificates that contain their public key and MAC address.

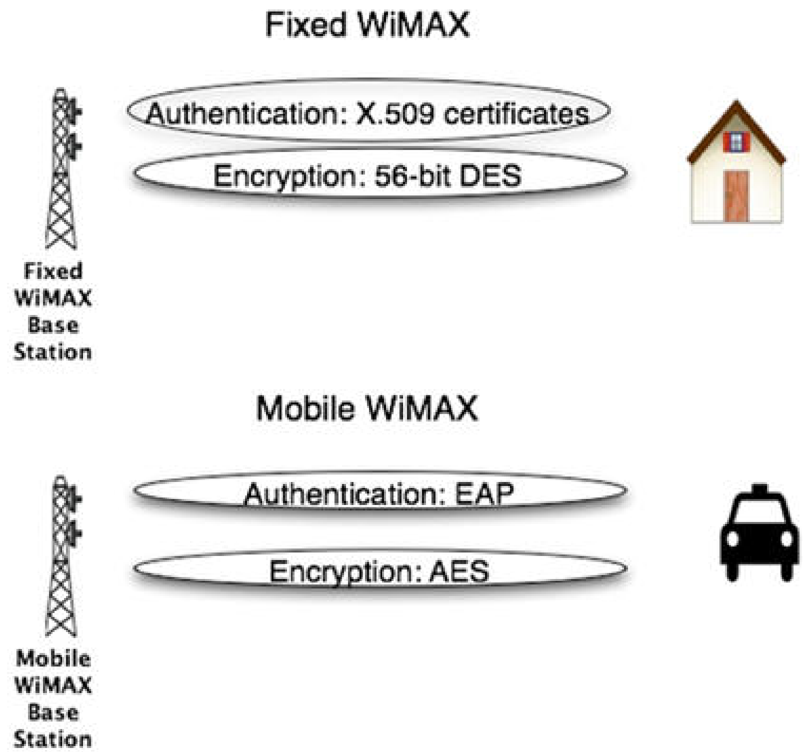

Figure 2.13: WiMAX Security through Authentication and Encryption [20]

Flexible key-management protocol: The Privacy and Key Management Protocol Version 2 (PKMv2) [21] is used for securely transferring keying material from the base station to the mobile station, periodically reauthorizing and refreshing the keys. PKM is a client-server protocol: The MS acts as the client; the BS, the server. PKM uses X.509 digital certificates and RSA (Rivest-Shamer-Adleman) public-key encryption algorithms to securely perform key exchanges between the BS and the MS.

Support for fast handover: To support fast handovers, WiMAX allows the MS to use preauthentication with a particular target BS to facilitate accelerated reentry. A three-way handshake scheme is supported to optimize the reauthentication mechanisms for supporting fast handovers, while simultaneously preventing any man-in-the-middle attacks.

2.3.3.5 Multicast and Broadcast Services

The mobile WiMAX MAC layer has support for multicast and broadcast services (MBS). MBS- related functions and features supported in the standard include:

- Signaling mechanisms for MS to request and establish MBS
- Subscriber station access to MBS over a single or multiple BS, depending on its capability and desire
- MBS associated QOS and encryption using a globally defined traffic encryption key
- A separate zone within the MAC frame with its own MAP information for MBS traffic
- Methods for delivering MBS traffic to idle-mode subscriber stations
- Support for macro diversity to enhance the delivery performance of MBS traffic

CHAPTER 3
OBJECTIVE

3.1 Research Challenges

Handover schemes serve an important role in WiMAX to complete the handover process and to satistfy QoS requirements. Various Handover schemes are proposed for reducing the handover latency and ensuring QoS requirements of various service flows. In general, fast handover scheme should satisfy following features and criteria for optimizing handover performance.

1) Minimum Scanning Time

Minimum Scanning Time is the most important in the handover process.The handover scheme must utilize the channel efficiently and apply such a procedure so as to reduce the time it takes to scan the neighboring base stations.This implies that the un-necessary scanning of neighboring base stations should be avoided.

2) Fairness

All MS should get equal time interval to scan and use the resources. The handover policy should assign available resource that is base station fairly in case of multiple MS requesting for services. The fairness should be provided for both short term and long term.

3) Handover Latency

Fast handover scheme should be such that the time it takes to complete the handover process should be reduced. Thus, Fast handover policy must take in to consideration the handover latency it takes to complete the handover process.

4) QoS requirements

The proposed fast handover scheme should support different applications to exploit better QoS. To support delay-sensitive applications, the handover policy provides the delay bound provisioning. Thus, to ensure that if some real time application needs to be serviced then appropriate fast handover scheme must fasten up the handover process taking scan time and handover delay in considerations.

5) Mobility

Fast handover scheme must also consider the mobility factor which plays an important role during handover process. Since, MSs move towards or away from the BSs, it becomes necessary that handover process with the nearest MS be completed.

6) Network Topology

Fast handover scheme should be able to deliver the same performance even if there is change in network topology or network parameters.

7) Implementation complexity

In a high-speed network, the handover decision making process must be completed very rapidly. A low-complexity handover scheme is desirable.

8) Scalability

The fast handover scheme must operate efficiently as the number of connections or users sharing the channel increases.

An ideal fast handover scheme should try to satisfy all of above criteria for efficient handover.

3.2 Problem Statement

IEEE 802.16 standard were developed to extend the wired networks with more efficient deployment and lower maintenance cost. Modern wireless networks require wide bandwidth and high-speed mobility, and IEEE 802.16e is considered to be a technology capable of meeting such requirements. IEEE 802.16e standard is proposed to support the mobility up to 60km/h with the data transmission rate up to 2Mbps, so handover has become one of the most important factors that impact the performance of IEEE 802.16e system. Data transmission to the terminal device is interrupted while scanning is performed for the handover procedure. Naturally, prolonged scanning undermines the network's performance. In order to resolve this problem, a number of handover schemes have been proposed. In order to reduce the redundancies in IEEE 802.16e handover process, several fast handover schemes, including Single Neighbor Target BS scanning, CTBS, fast ranging and pre-registration, have been proposed. Single Neighbor BS scanning handover scheme performs scanning followed by negotiation with the neighboring base stations. The new and improved handover scheme called CTBS reduces the number of base stations to be scanned by performing negotiation prior to scanning.

In this thesis, Scanning time and Handover latency of CTBS, Fast Ranging and Pre-registration is analyzed and compared. The simulation results show that these fast handover schemes can reduce scan time and handover latency during handover process , and thus improve the QoS of IEEE 802.16e.

CHAPTER 4
FAST HANDOVER SCHEMES

In IEEE 802.16e-2005 standard, three kinds of handover types are supported:

(a) Hard handover (HHO)

(b) Fast BS switching (FBSS) and

(c) Macro Diversity Handover (MDHO)

Among them, HHO is the simplest one while the other two types are more complicated and optional. Up till now, only HHO and FBSS are adequately defined in the standard for practical use. In this thesis, when handover is mentioned, it refers to HHO.

The MAC layer handover of IEEE 802.16e includes the following phases:

1) network topology acquisition before handover, which includes network topology advertisement, and MS scanning or association of neighbor BSs.

2) handover execution phase, which mainly includes cell reselection, handover initialization and handshake process, connection release, and target network re-entry. Although handover process has been studied in literature survey but it is important to discuss it in context of proposed handover scheme CTBS.

4.1 Handover Process

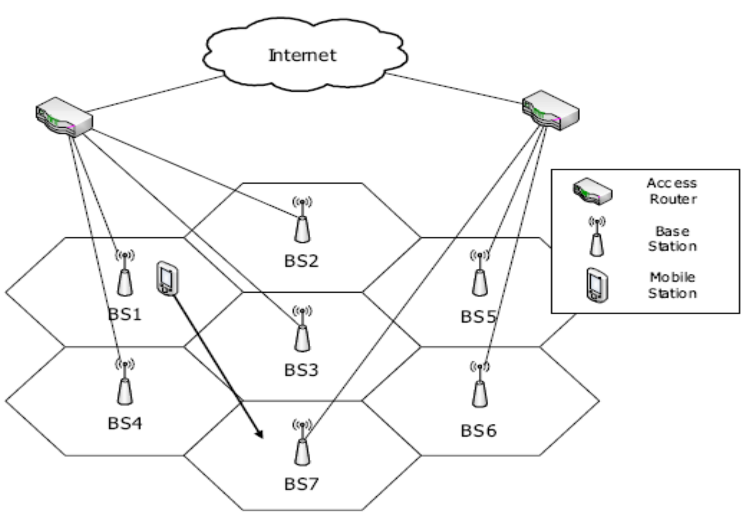

Figure 4.1: Handover Topology

Handover occurs in an IEEE 802.16e network when a terminal device MS, while communicating with a BS, moves into another cell and is then serviced by a different BS. Fig.4.1 exhibits the network topology of the IEEE 802.16e system. The MS is the served device, BS1~BS7 are base stations regionally managing and controlling the MS, and the hexagons indicate the cell regions served by the BSs. it displays the MS being serviced by BS1 and moving toward BS7. Once the MS move out of cell BS1, handover becomes necessary

The handover procedure is shown in Fig. 4.2.

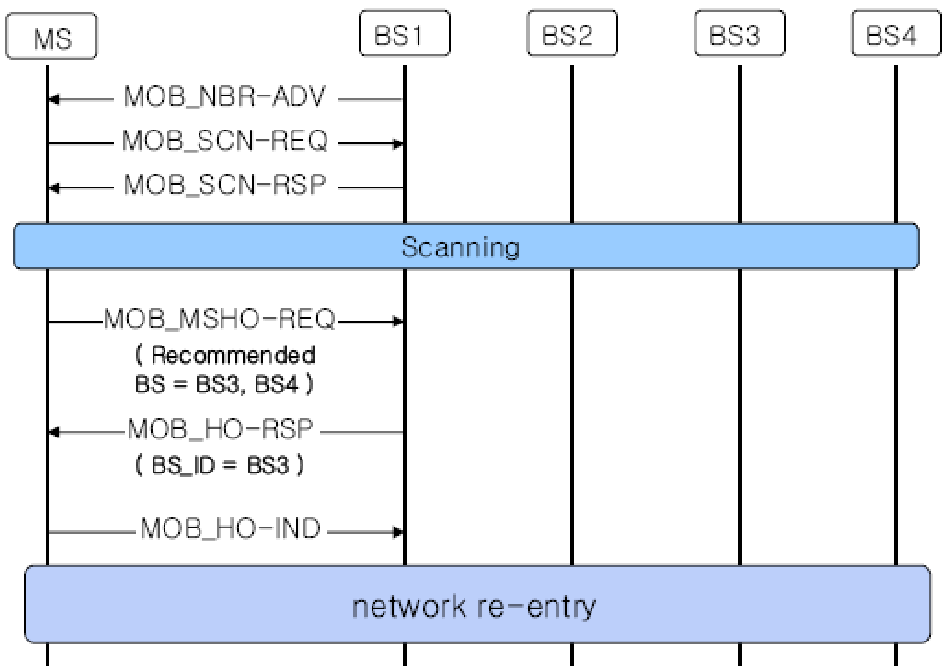

Figure 4.2: Handover Procedure [22]

The MS regularly receives channel information about the neighboring BSs through the MOB_NBR-ADV message from the servingBS. If the signal strength weakens, the MS sends an MOB_SCN-REQ message to the serving BS and receives a MOB_SCN-RSP message in return, to acquire a time interval for scanning. Then the MS selects candidate target BSs based on the signal strength and response time of each BS, acquired from scanning. Upon completion of scanning, the MS transmits an MOB_MSHO-REQ message, which includes a list of recommended target BSs (BS3 and BS4) to the serving BS, and receives an MOB_MSHO-RSP message as a response to finally select the target

BS (BS3). The actual handover takes place with an MOB_HO-IND message from the MS, leading to network re-entry.

• **Scanning:** Fig. 4.3 displays the detailed scanning procedure.

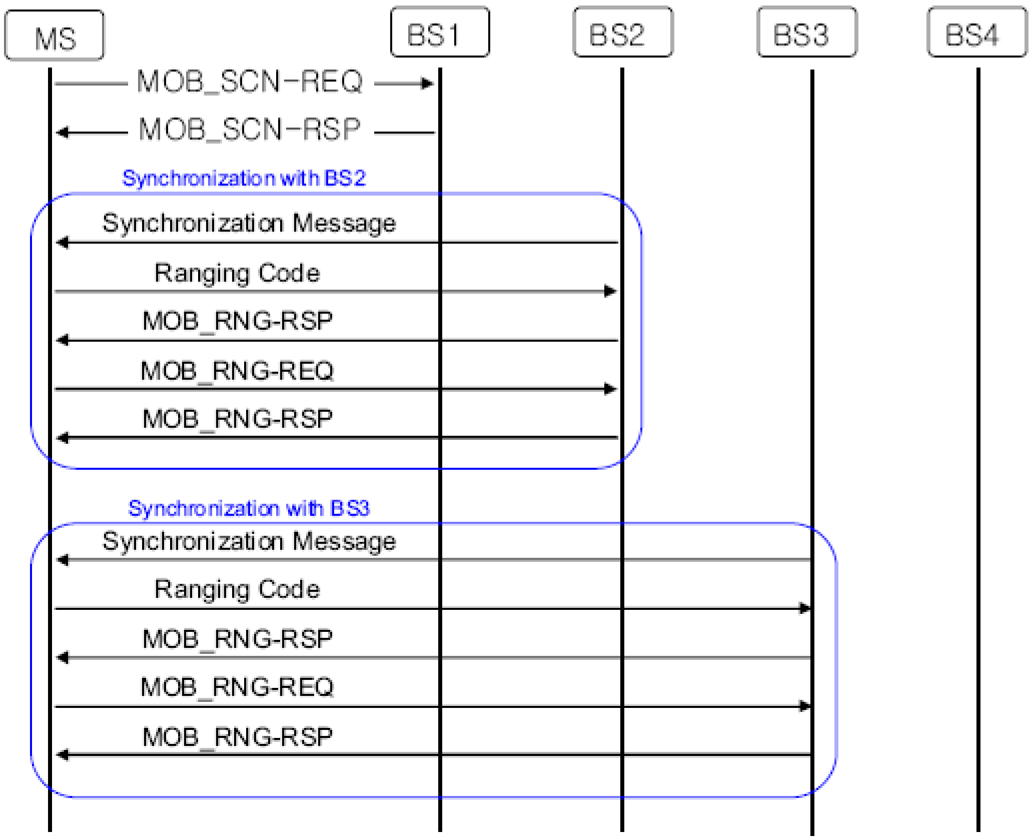

Figure 4.3: Scanning Procedure

After exchanging the MOB_SCN-REQ and MOB_SCN-RSP messages, the MS obtains the time interval for scanning. The MS then scans all neighboring BSs through synchronization and association, evaluates the CINR (carrier-tointerference-and-noise ratio) [23] and the relative delay for each of the neighboring BS and selects candidate target BSs. While scanning, the MS suspends data transmission and incoming data to MS are buffered for the duration. Furthermore, the neighboring BSs are not scanned simultaneously but sequentially. In turn, prolonged scanning further extends the suspension of data transmission, undermining the system's performance.

• **Negotiation:** Once scanning is complete, the MS sends an MOB_MSHO-REQ message, which includes a list of target BS candidates generated from the scanning procedure, to the serving BS. Based on this list, the serving BS then carries out the HO pre_notification process, which involves transmitting the MS' ID, as well as the bandwidth (BW), and the QoS required by the MS via backbone network. The serving BS receives a HO pre_notification response, which validates the MS' expected performance when service is provided by each target BS candidate. This process is referred to as "negotiation" and is a tool for selecting the final target BS.

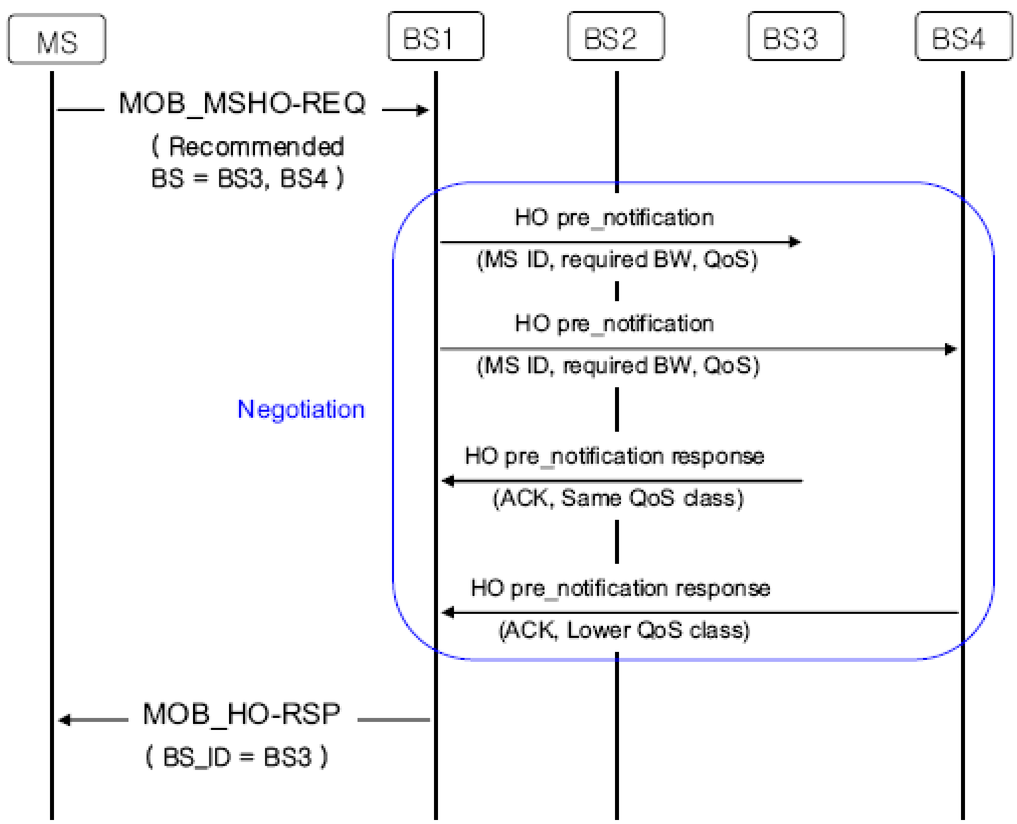

Figure 4.4: Negotiation Procedure [25]

The negotiation procedure is shown in Fig. 4.4. Here, BS1 is the serving BS, an BS3 and BS4 are target BS candidates. The figure displays how negotiation is conducted through the backbone network, and shows the process of selecting BS3 as the target BS based on its ability to provide the QoS required by the MS.

The proposed scheme focuses on the fact that the process of selecting the target BS takes place in two stages for the handover procedure. According to IEEE 802.16e, the MS scans all of the neighboring BSs before selecting the target BS candidates, and the serving BS selects the final target BS based on the negotiation process. Whereas the conventional algorithm selects the target BS with the "scanning negotiation" approach, the proposed scheme reverses the sequence to "negotiation-scanning" in order to reduce the number of BSs to be scanned. When the MS sends an MOB_SCN-REQ message to request the time interval for scanning, the serving BS performs negotiation with all of the neighboring BSs through the backbone network. When the serving BS notifies all of the neighboring BSs of the MS' ID, required bandwidth and QOS through the HO pre-notification process, they respond by returning HO pre_notification responses, which give the serving BS information regarding the MS performance when it is serviced by the corresponding neighboring BS. Based on this information, the serving BS eliminates the BSs that cannot provide the QOS required by the MS, and sends out an MOB_SCN-RSP message. Then the MS has to scan only the BSs that satisfy the requirements, and the target BS is determined as soon as scanning is complete. After BSs that satisfy QoS are left, then single target BS estimation is done by checking the CINR of neighboring BS. MS only scans or associates the neighbor BS with the best CINR.

4.2 Redundancies in MAC Layer Handover Process

Two phases are included in the IEEE 802.16e MAC layer handover process: the network topology acquisition phase before handover and the real handover execution phase [26]. At the network topology acquisition phase, firstly, there is only one BS that can be selected as target BS for handover actually, so it will bring redundant scan processes if several neighbor BSs are chosen as target BS for scan or association. Secondly, although data transmitting does not stop (scan intervals and normal operations appear alternately, and data transmitting will stop in scan intervals until normal operation starts), the throughput will decrease if scan processes occupy too many resources. Thirdly, the time for scan process is indeterminable. Since the results gained from scan may be invalid because of the changes of neighbor BSs channel quality, the system resources are wasted in this case. During the process of cell reselection, handover initialization and three-way handshake, MS still can receive downlink data from current serving BS and gain opportunity to send uplink data. The connection between MS and serving BS will be ended only after serving BS receive HO-IND message including handover start and connection release information from MS. After MS finished the process of re-entering target BS network, interrupted data transmission will be continued. Therefore, interruption of data transmission only happens during the network re-entering process. The time of interruption is called handover latency. Some kinds of service will be terminated if the handover delay is too long to tolerate by applications. Hence, the performance of IEEE 802.16e broadband wireless networks can be improved by optimizing network re-entering process, which reduces the handover delay. In a word, implement fast handover schemes to avoid unnecessary neighbor BS scanning and optimize network re-entering stage of handover process can reduce the handover delay and the waste of wireless resources, thus improve the performance of IEEE 802.16e broadband wireless networks.

4.3 Cost-Effective Target BS Selection Scheme

The handover procedure in the IEEE 802.16e protocol consists of cell re-selection, handover decision and initialization, synchronization with the target base station (BS), ranging and network re-entry. Prior to making decision for handover, the MS scans the neighboring BSs based on the channel information provided by the serving BS. Once scanning is complete, the serving BS performs negotiation with the target BSs through a backbone message, and selects a single target BS that meets the bandwidth and QoS requirements requested by the MS. While the MS scans, data cannot be transmitted, causing data buffering and undermining the system's performance.Also we have to take care of the MS mobility factor in account. So, adaptive channel scanning [27] technique also is taken into consideration. The proposed scheme involves eliminating unnecessary BSs by performing negotiations with neighboring BSs prior to scanning. Through the backbone message, a BS sends information to neighboring BSs regarding the bandwidth and the QoS required by the MS before the MS scans [28]. A response from neighboring

BSs allows the protocol to assess the MS's expected performance if the service is provided by the corresponding BS. Then the MS scans only the BSs that satisfy its requirements. This approach reduces the number of BSs to be scanned and the time required for scanning, ultimately reducing system interruptions.

Performance analysis conducted by comparing the proposed scheme to the conventional method shows that the scanning time is reduced in accordance with the number of eliminated BSs eliminated based on the negotiations.

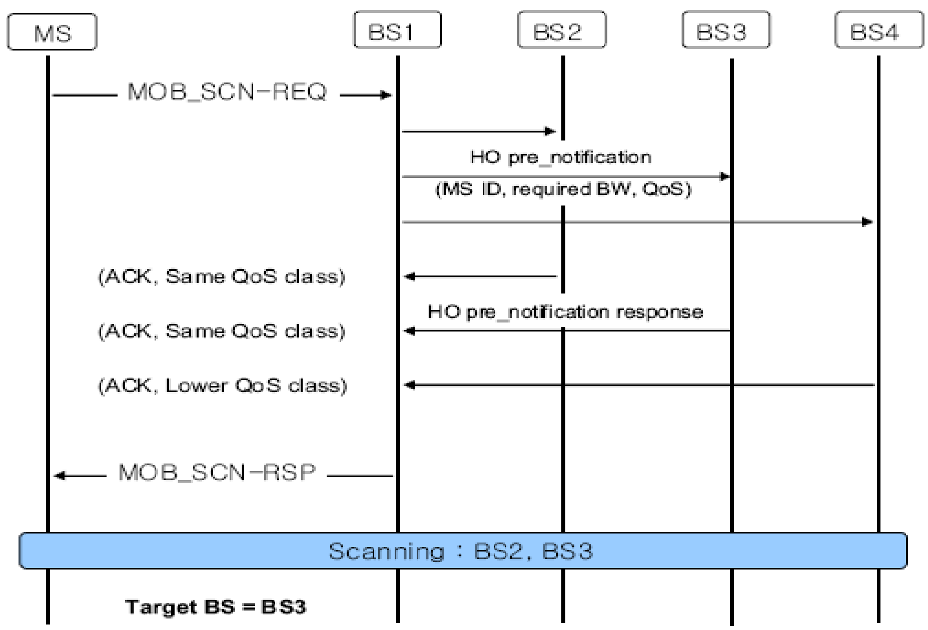

Figure 4.5: CTBS Scheme [29]

BS1 is the serving BS, and BS2, BS3 and BS4 are neighboring BSs. Whereas BS2 and BS3 satisfy the MS' requirements, BS4 cannot provide the necessary QoS. Target BS selection takes place in the order of negotiation scanning, BS4 is eliminated during the negotiation process, and therefore is no longer subjected to scanning. Scanning is performed only on BS2 and BS3. Upon receipt of the MOB_SCN-REQ message, BS1 (the serving BS) transmits an HO pre_notification to BS2, BS3 and BS4 to notify them of the MS' ID, as well as its required bandwidth and QoS. The HO pre_notification response informs BS1 that although BS2 and BS3 can provide the QoS that the MS requires, BS4 can only offer a lower QoS. The MS then receives the MOB_SCN-RSPmessage containing this data, and scans only BS2 and BS3, but not BS4. Based on the values obtained from scanning, BS3 is selected as the target BS. The conventional procedure involves scanning every neighboring BS, which decreases the system's performance due to suspended data transmission during the scanning process. On the other hand, the negotiation process takes place through the backbone network, and does not interrupt data transmission. Therefore, negotiation is performed prior to scanning, to identify the BSs that satisfy the MS requirements. Only the selected BSs are scanned, decreasing the number of scans. This ultimately reduces the suspension of data transmission.

4.4 Fast Ranging and Pre-registration

In IEEE 802.16e broadband wireless networks, handover delay is mainly caused by target network re-entering process. Decreasing handover delay can improve the successful probability of handovers. Therefore, optimizing the network re-entering process to reduce handover delay can improve the overall system performance. In fast ranging [30], target BS is informed to provide a dedicated ranging opportunity for MS. It uses a Fast_Ranging_IE to grant an uplink ranging opportunity to MS in its broadcasting UL-MAP message. After receiving the dedicated ranging opportunity from target BS, MS does not need to do contention-based ranging, thus the time for ranging is reduced.

In pre-registration [31], target BS obtains the service flow and authentication information of this MS through backbone networks before handover. So target BS does not need to spend time on getting authorization information from the authorization server via backbone networks. Although target BS knows the service flow and authentication information about this MS, it still has to send CID updating message to the MS by using REQ-RSP message. Therefore, the average time of pre-registration process is half of the average time for the overall registration process. By using Fast_Ranging_IE , target BS provides a dedicated ranging opportunity to MS; and through pre-registration, target BS obtains the service flow and authentication information of this MS. Consequently, the process for MS to re-enter into target network is accelerated; the handover delay is reduced; the successful probability of handover is increased.

CHAPTER 5

SIMULATION AND PERFORMANCE ANALYSIS

5.1 Assumptions

In order to analyze and compare the performance of these fast handover schemes, handover delay is studied in the IEEE 802.16e OFDMA TDD model. The frame length is assumed to be 5ms and the cell load ratio is Rload ($0 \le Rload \le 100\%$). Required time parameters of each stage are defined as follows[32]:

1) TSync: average time required for downlink synchronization;

2) TCont_rng: average time required for contention-based ranging;

3) TRng: average time required for fast ranging;

4) TAuth: average time required for authorization;

5) TReg: average time required for registration.

The average time required for downlink synchronization is assumed to be two frames, i.e. TSync = 10ms. Since contention based ranging mainly consists of CDMA code detecting and random backoff, thus TCont_rng depends on the CINR and cell load ratio. Because CINR is very low at the cell boundary, and the probability of collision in ranging process will increase when the cell load ratio increases, so the average time required for contention-based ranging is assumed to be directly proportional to the cell load ratio. For the average time required for each stage should be a multiple of the frame length, TCont_rng is calculated as following equation:

$$T_{Cont\_rng} = 75 + \lceil (1.5 \times 100 \times R_{load}) / 5 \rceil \times 5$$

The average time required for fast ranging is also assumed to be directly proportional to the cell load ratio. It can be calculated as:

$$T_{Rng} = 25 + \lceil (0.5 \times 100 \times R_{load}) / 5 \rceil \times 5$$

Since target BS needs to obtain the authorization information of MS from the authorization server during the authorization process, TAuth is assumed to be 150ms.The average time required for registration is assumed to be 7 frames, i.e. TReg =35ms.

5.2 Simulations for SCAN Time

CTBS Scheme

In order to analyze the proposed scheme's performance, a network topology was constructed and the scanning times of the proposed and conventional algorithms were compared. Fig. 5.1 displays the network topology. There are six neighboring BSs (BS1~BS6) around the serving BS. The MS is moving in the direction of BS3 and BS4. The hexagons are the BSs' cell areas. A hexagon's color represents the signal strength received by the MS, and darker hexagons indicate stronger signals. It is assumed that BS3 and BS5 do not meet the QoS class requirement of the MS.

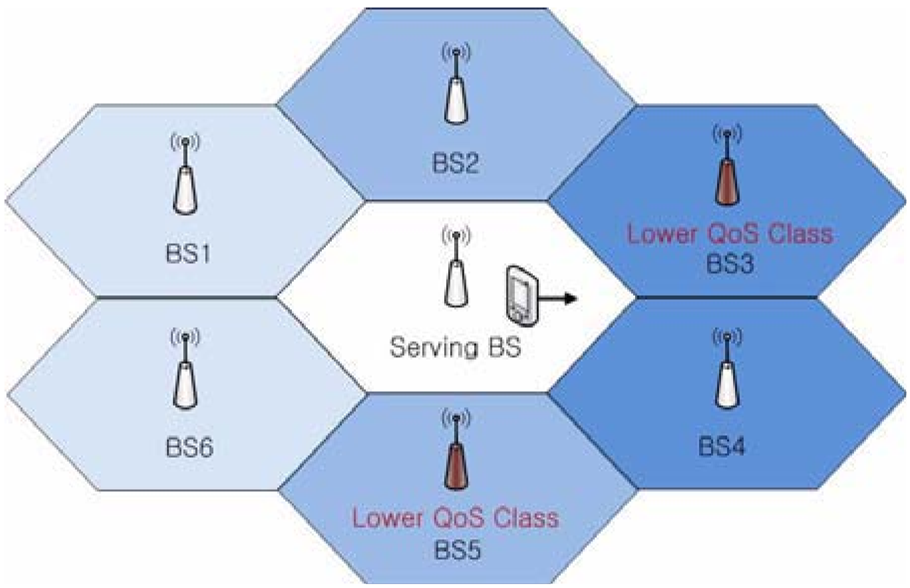

Fig 5.1: Assumed Network Topology [29]

First of all Single neighbour Target BS selection scheme is selected and is compared against the conventional mechanism. Then CTBS is compared with conventional mechanism followed by comparison with single target BS scheme.

The conventional mechanism [30] selects target BS candidates in the order of scanning-negotiation. Each BS is scanned sequentially, and BS3 and BS4 are selected as target BS candidates due to their sufficient signal strengths. The serving BS then performs negotiation with the two BSs, and BS4 is chosen as the target BS because BS3 cannot provide the QoS required by the MS. On the other hand, the proposed scheme selects the target BS based on the negotiation-scanning sequence. Negotiation is first performed with the six neighboring BSs, and BS3 and BS5 are eliminated because they cannot provide the QoS required by the MS. Then BS1, BS2, BS4 and BS6 are scanned, and BS4 is selected as the target BS because it offers the strongest signal.

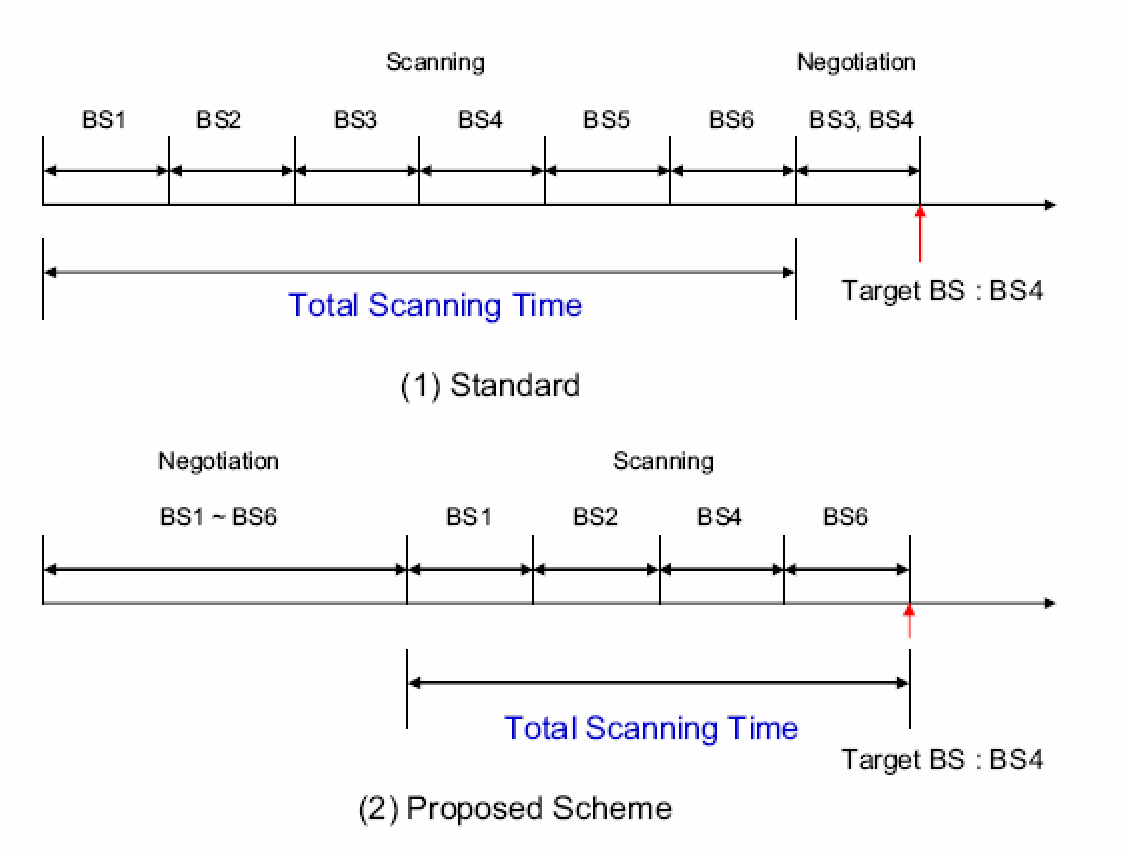

Figure 5.2: Comparison of time required for Scanning [29]

Fig. 5.2 compares the target BS selection processes of the IEEE 802.16e standard and the proposed algorithms along a time line. Although both methods yield BS4 as the final target BS, the figure shows that the proposed scheme requires less scanning time than the standard scheme.

Because data transmission is suspended while the BSs are being scanned, a shorter scanning time improves the system's performance. The total time required for scanning isproportional to the number of BSs to be scanned. Rather than scanning every neighboring BS, the proposed algorithm eliminated the two BSs (BS3 and BS5) that cannot provide the QoS required by the MS, which reduces the overall scanning time.

Different Scan Type Scenarios have been defined to analyze the performance of CTBS against the conventional scheme. The number of neighbor BSs that need to be scan or associate is assumed to be *n*.

TScn_0, TScn_1, TScn_2, TScn_3 and TScn_4 are defined as the average time required for scanning or association when 'Scan Type' equals to 0, 1, 2, and 3 respectively.

When 'Scan Type' = 0, i.e. MS scans neighbor BSs without association, MS only needs to downlink synchronize with the target BS so as to get the quality information of its physical channel, so Scn_0 T can be calculated as:

$$T_{Scn\_0} = n \times T_{Sync}$$

When 'Scan Type' equals to 1, i.e. scan/association without coordination mode, MS not only needs to downlink synchronize with target BS, but also needs to execute a contention-based ranging.

$$T_{Scn\_1} = n \times (T_{Sync} + T_{Cont\_rng})$$

When 'Scan Type' equals to 2, i.e. association with coordination mode, MS not only needs to downlink synchronize with target BS, but also needs to execute a fast ranging process. So TScn_2 is calculated as

$$T_{Scn\_2} = n \times (T_{Sync} + T_{Rng})$$

When 'Scan Type' equals to 3, i.e. network assisted association reporting mode, the only difference to association with coordination mode is that target BS does not send RNG-RSP message directly to MS. RNG-RSP message is firstly sent to serving BS through backbone networks. Then serving BS packs all RNG-RSP messages from scanned neighbor BSs into a MOB_ASC-REPORT message and sends it to MS during interleaving intervals of scan duration or normal operation time. Therefore, the average time required for fast ranging is half of that for a contention-based ranging. TScn_3 is shown as:

$$T_{Scn\_3} = n \times (T_{Sync} + \lceil 1/2 \times T_{Rng} / 5 \rceil \times 5)$$

When choosing a single BS with best CINR as the target BS for scanning (n=1), the scan time of different scan types under different cell load ratio is shown in Figure 5.3-5.5.

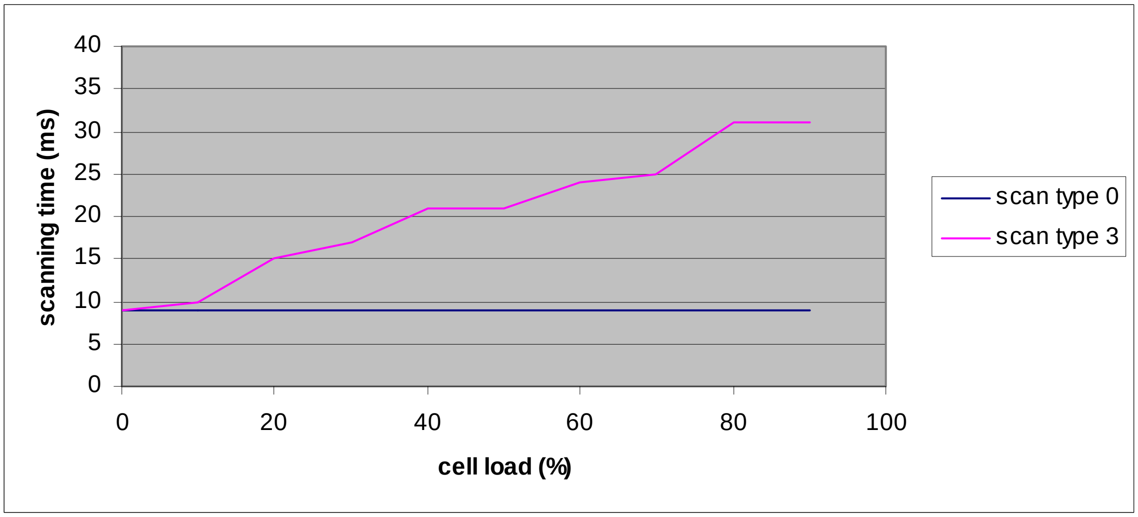

Figure 5.3: Scan time for Scan type 0 and 3

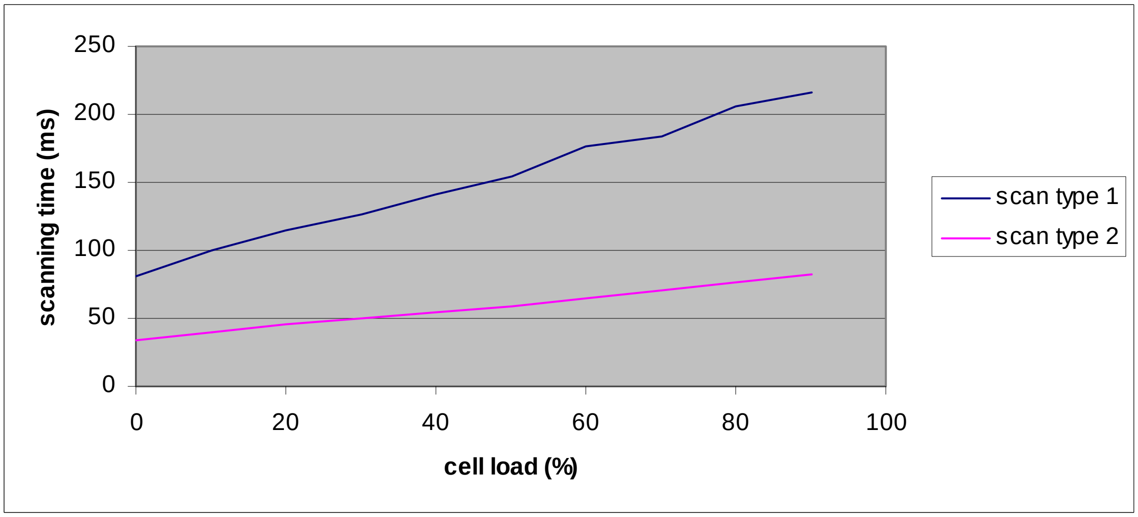

Figure 5.4: Scan time for Scan type 1 and 2

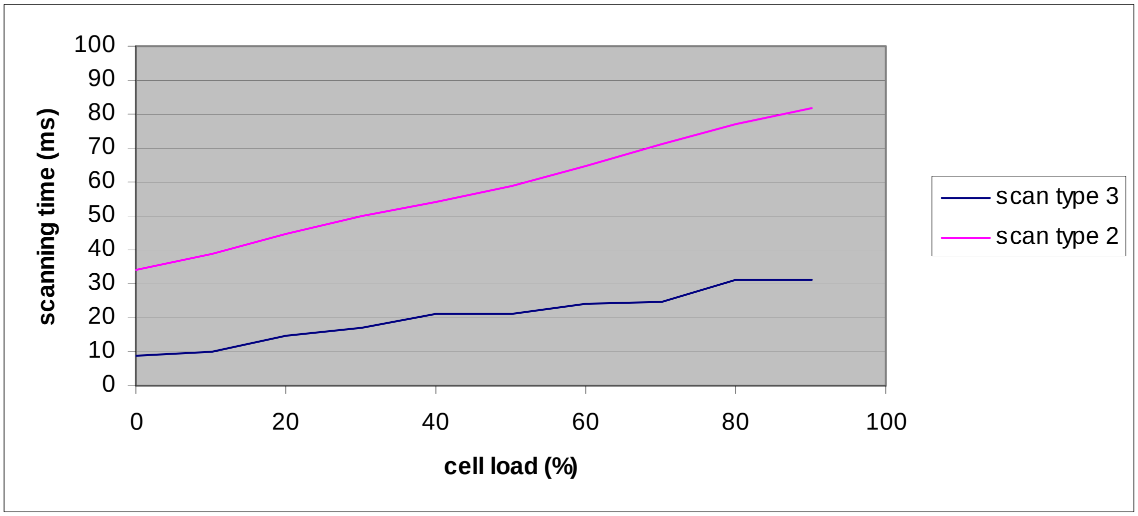

Figure 5.5: Scan time for Scan type 2 and 3

Figure 5.3-5.5 shows that, when the cell load ratio keeps invariable, the scan time in different scan/association types ranks from low to high as follows: scan without association, network assisted association reporting, association with coordination, and scan/association without coordination. In scan without association mode, which is the simplest scan type, scan time keeps the same when load increases. In the other three types, scan time increases when cell load ratio increases. Since scan/association without coordination adopts contention-based ranging, the increase of cell load ratio will cause more collisions and backoffs. So the scan time of this scan type can easily be influenced by load ratio, and increases fastest when load ratio increases. If the parameters got from association are still valid when handover occurs, adopting association method will reduce the time for ranging during the handover process, but association increases the scan time especially in scan/association without coordination mode. Because service will be interrupted during scan duration, the increase of scan time will decrease the throughput. On the other hand, since scan time is directly proportional to the number of BSs that needed to be scanned, so in association modes especially in network assisted association reporting mode, when MS choose a single target BS for scan, the scan time can be greatly reduced, i.e. the probability of service interruption can be reduced.

Furthermore, following parameters are defined to express the scanning time with an equation in case of more than one number of neighboring BSs .

Ttotal : Total time required for scanning

N : Number of neighboring BSs

k : Number of neighboring BSs unable to provide the QoS requested by the MS.

The number of BSs to be scanned in the conventional and the proposed methods are N and N−k, respectively.

$$T_{total(proposed)} = T_{total(standard)} * \frac{N-k}{N}$$

$$\text{Because } \frac{N-k}{N} \leq 1,$$

$$T_{total(proposed)} \leq T_{total(standard)}$$

If N=5

And k = 3

Then N−k = 5−3 = 2

Ttotal(proposed) = Ttotal(standard)* 2/5;

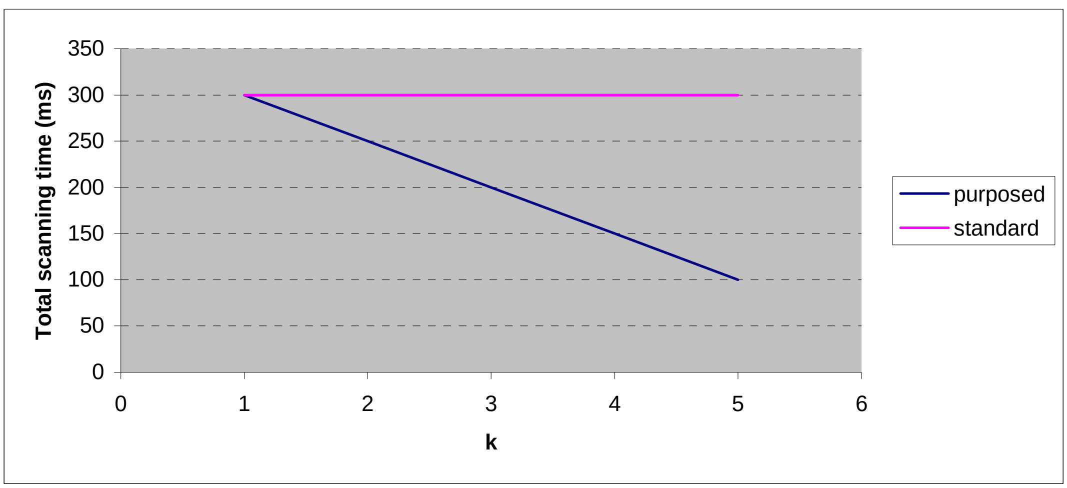

Figure 5.6: Comparison of the scanning times for CTBS and conventional scheme

Whereas the time required for scanning remains constant in the conventional approach, the total scanning time decreases with the proposed scheme as the value of k increases.

Now, the comparison of various scan types is done with CTBS for different k values. Graphs showing scan time for k = 1, 2, 3 are shown for scan type 1 and scan type 3 along with the cell load ratio along the x-axis.

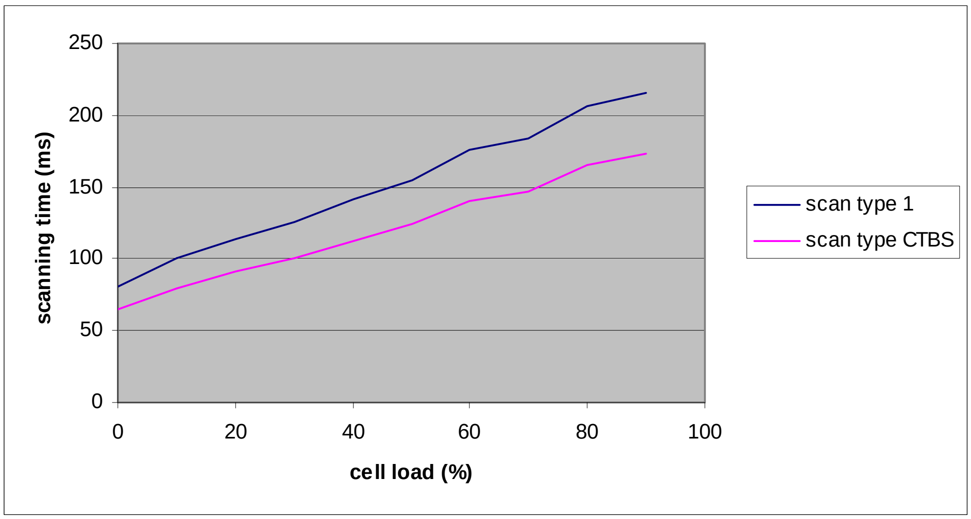

Figure 5.7: Scan time for Scan type 1 and CTBS for k = 1

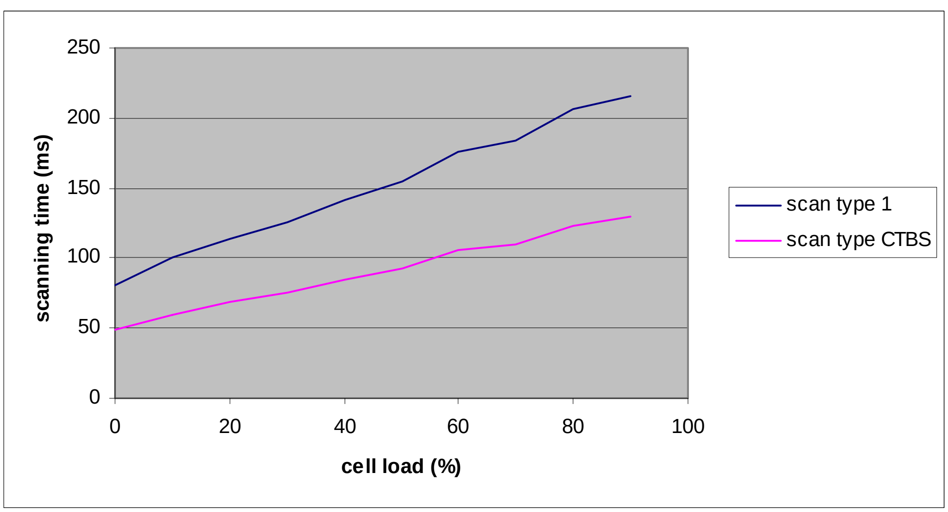

Figure 5.8: Scan time for Scan type 1 and CTBS for k = 2

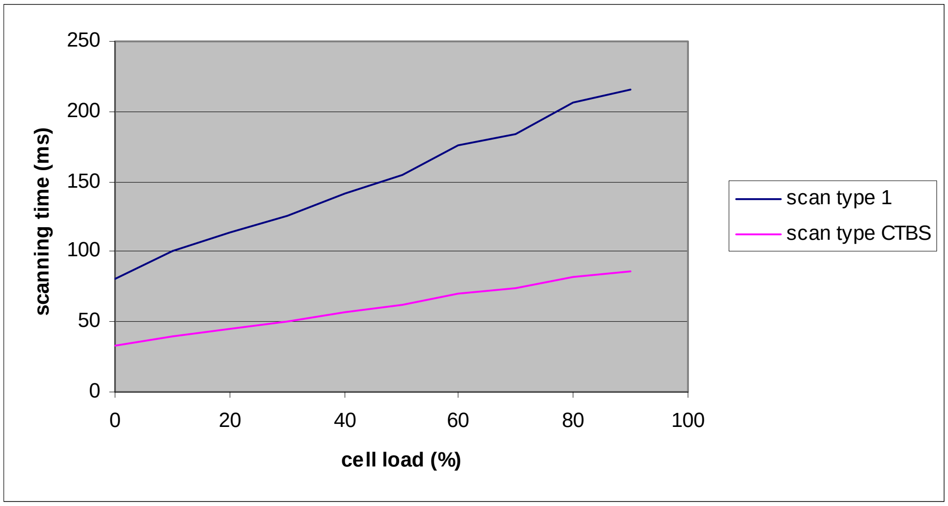

Figure 5.9: Scan time for Scan type 1 and CTBS for k = 3

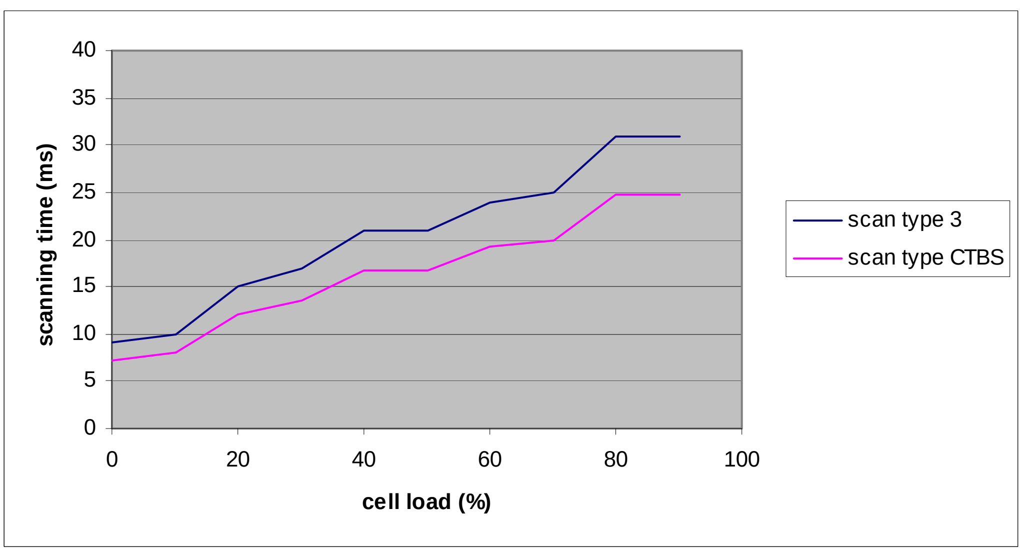

Figure 5.10: Scan time for Scan type 3 and CTBS for k = 1

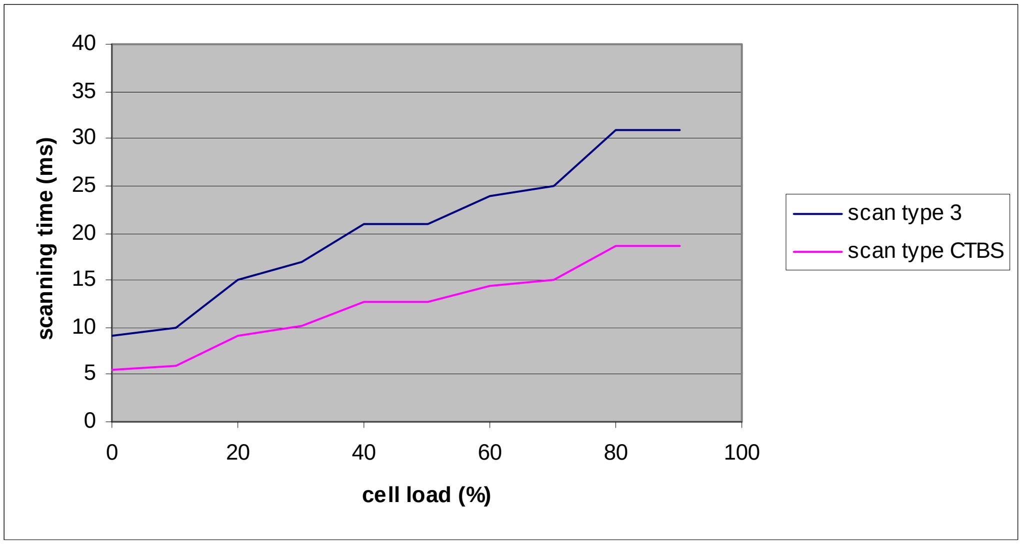

Figure 5.11: Scan time for Scan type 3 and CTBS for k = 2

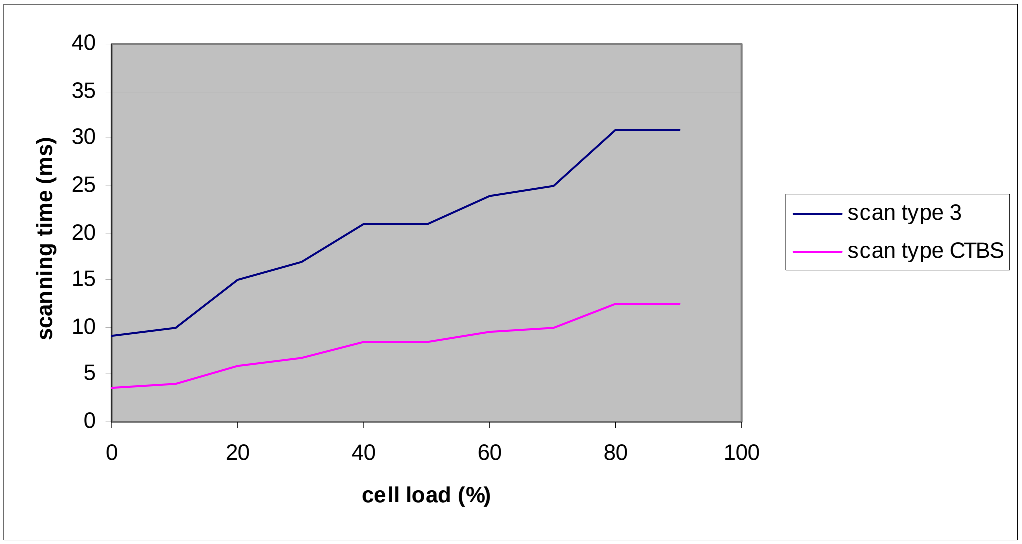

Figure 5.12: Scan time for Scan type 3 and CTBS for k = 3

5.3 HANDOVER Latency

Four different handover policies are defined as follow:

Policy 1: handover with contention-based ranging;

Policy 2: handover with fast ranging;

Policy 3: handover with contention-based ranging and pre-registration;

Policy 4: handover with fast ranging and pre-registration.

In policy 1, after serving BS received HO-IND message with handover start or service release indicator, target BS is not informed to provide dedicated ranging opportunity for MS. During the network re-entering process, MS must send CDMA code and execute random backoff if collision happens, i.e. MS must obtain a ranging opportunity through contention. Moreover, target BS does not get the registration information (such as authorization and service flow information) of MS from backbone networks. Therefore, handover delay of policy 1 is shown as:

$$D_{HO\_P1} = \lceil (T_{Sync} + T_{Cont\_rng} + T_{Auth} + T_{Reg}) / 5 \rceil \times 5$$

Policy 2 includes a fast ranging process. However, target BS does not get the registration information of MS from backbone networks. So MS has to execute a re-authorization and reregistration process. Handover delay of policy 2 is shown as:

$$D_{HO\_P2} = \lceil (T_{Sync} + T_{Rng} + T_{Auth} + T_{Reg}) / 5 \rceil \times 5$$

Policy 3 adopts contention-based ranging and pre-registration. Target BS can obtain the registration information of MS from backbone networks. Although target BS knows the information of MS, it still should send REQ-RSP message including CID updating information to MS. Therefore, average time for preregistration is half of the average time of a complete registration process. Handover delay of policy 3 is shown as:

$$D_{HO\_P3} = \lceil (T_{Sync} + T_{Cont\_rng} + T_{Reg} / 2) / 5 \rceil \times 5$$

Policy 4 uses fast ranging and pre-registration schemes. In this policy, target BS not only provides a dedicated ranging opportunity to MS, but also obtains the service flow and authorization information of this MS from backbone networks, and needs to send REQ-RSP message including CID update information to the MS. So the average time required for registration is half of that for a complete registration. Handover delay of policy 4 is shown as:

$$D_{HO\_P4} = \left\lceil (T_{Sync} + T_{Rng} + T_{Reg} / 2) / 5 \right\rceil \times 5$$

Figure 5.7 - 5.9 shows that the handover delay of four handover policies increases when the cell load ratio increases. Policy 1 has the fastest increasing rate. And policy 4 has the minimal handover delay among all handover policies, which always less than 100 ms, so this policy is appropriate for real-time applications. However, the decrease of handover delay is obtained by increasing the traffic load of backbone networks. If the parameters gained from association are still available when handover occurs, the time required for ranging during handover can be reduced. Therefore, adopting fast ranging and pre-registration schemes can reduce handover delay, and thus increase the successful probability of handover and improve the system performance.

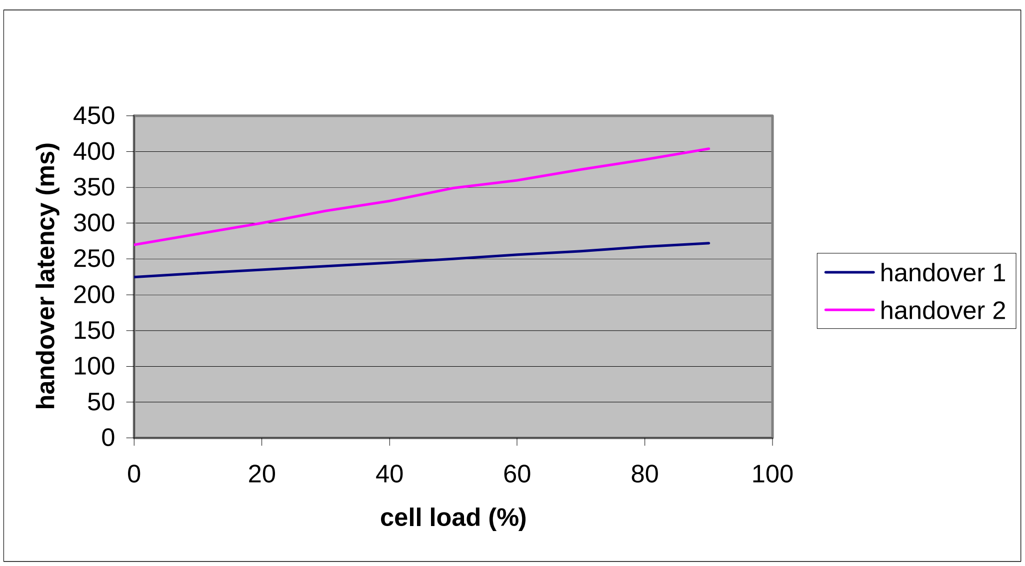

Figure 5.13 : Handover Latency for Handover Policy 1 and 2

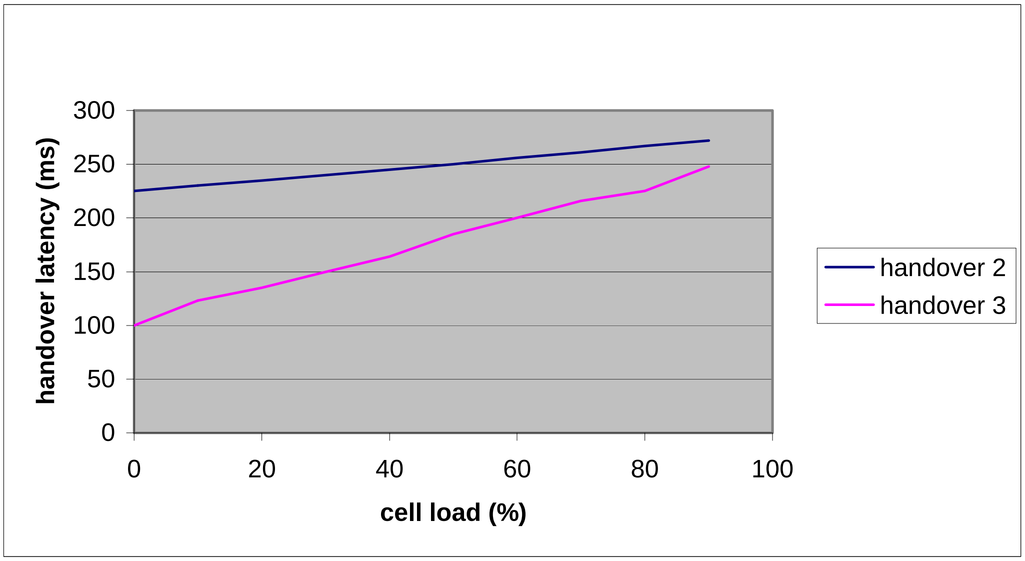

Figure 5.14 : Handover Latency for Handover Policy 2 and 3

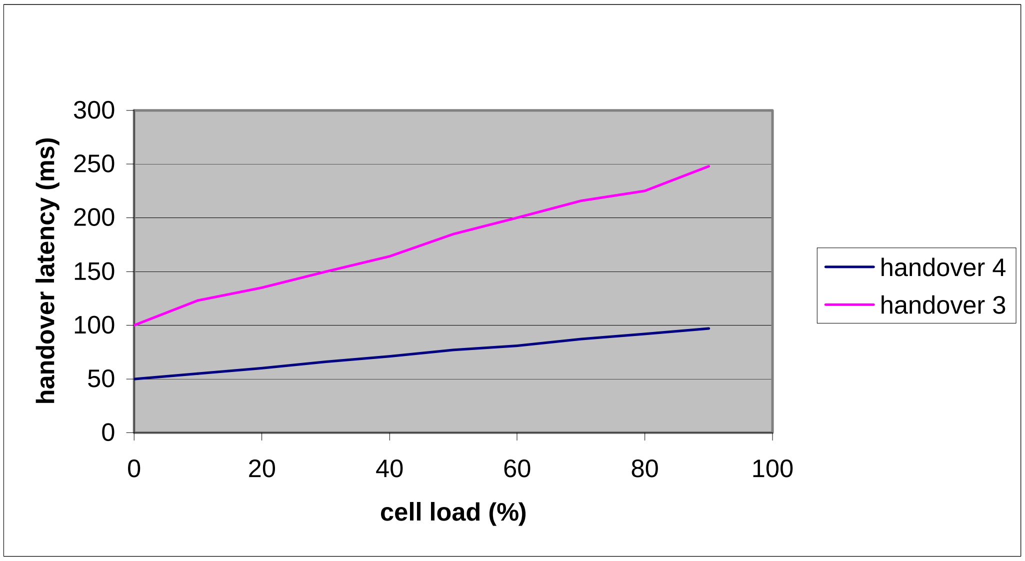

Figure 5.15 : Handover Latency for Handover Policy 3 and 4

Chapter 6

Conclusions and Future Directions

6.1 CONCLUSION

Since IEEE 802.16e standard is proposed to support mobility, it has become one of the most important QoS factors. In this thesis, several fast handover schemes for IEEE 802.16e broadband wireless networks are analyzed. Single target BS with best CINR is chosen for scanning, CTBS performs negotiation prior to scanning procedure and fast ranging and pre-registration schemes is used to optimize network re-entering process. The analysis results show that the CTBS scheme as compared to Single target BS can reduce the scan time in network topology acquisition process especially in association modes, and the other two schemes can reduce handover delay. In a word, these fast handover schemes can reduce the waste of wireless resources and improve the performance of IEEE 802.16e broadband wireless networks.

6.2 Extensibility

We have analyzed fast handover schemes performance during handover process and these handover schemes can be considered as a viable alternative for handover process in IEEE 802.16. In fact it can be considered for wireless network where QoS requirements have to be satisfied which are mandatory feature for emerging applications.

6.3 Future Work

Handover in WiMAX is quite a challenging research topic. There are many issues which can be further investigated.

- Since performance of fast handover schemes has been analyzed. So, new fast handover schemes can be suggested and analyzed by simulation against the conventional fast handover schemes.
- Performance of other purposed fast handover schemes are also issues to further investigate.
- Performance of proposed handover schemes to actual network environment is also worth further study.

REFERENCES

[1] http://www.wirelessman.org. accessed on 15/1/2008

[2] http://www.wimaxforum.org/technology accessed on 21/1/2008

[3] www.wimax.com/research/whitepapers accessed on 6/2/2008

[4] http://www.wimax.com/education/learning-center/wimax-com-resource-center accessed on 11/2/2008

[5] www.wimax.com/education/wimax/wimax_overview accessed on 17/2/2008

[6] IEEE. Standard 802.16-2004. Part16: Air interface for fixed broadband wireless access systems. October 2004.

[7] http://www.wimax.com/education/wimax/wireless_architectures accessed on 16/1/2008

[8] WiMAX Forum. WiMAX Forum Mobile System Profile. 2006–07.

[9] Fundamentals of WiMAX : Understanding Broadband Wireless Networking By Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed

[10] http://www.wimax.com/education/wimax/antennas accessed on 25/5/2008

[11] R.Guerin and V.Peris, "Quality-of-service in Packet Networks: Basic Mechanisms and Directions," Computer Networks, vol.31, pp.169-89, Feb. 1999.

[12] IEEE. Standard 802.16e-2005. Part16: Air interface for fixed and mobile broadband wireless access systems—Amendment for physical and medium access control layers for combined fixed and mobile operation in licensed band. December 2005.

[13] WIMAX in 50 Pages: A SIMPLE EXPLANATION TO A COMPLEX SUBJECT, BY Frank Ohrtman .

[14] C. Eklund, R. B. Marks, K. L. Stanwood and S. Wang, "IEEE Standard 802.16: A technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access", IEEE Communications Magazine, pp. 98-107, June 2002.

[15] WiMAX Forum: Mobile WiMAX—Part I: A technical overview and performance evaluation. White Paper. March 2006. http://www.wimaxforum.org/

[16] Handover issues in heterogeneous wireless network environments WiFi and WiMAX by Roberto Albanese.

[17] Analysis of Handover Performance in Mobile WiMAX by Antti Makelainen Helsinki University of Technology

[18] Y. Xiao, "Energy Saving Mechanism in the IEEE 802.16e Wireless MAN", "IEEE Communications Letters, vol. 9, No. 7", pp. 595-598.

[19] WiMAX Forum. Mobile WiMAX—Part II: A comparative analysis. White Paper. April 2006. http://www.wimaxforum.org/

[20] Security Issues of IEEE 802.16 (WiMAX) by Jamshed Hasan.

[21] Security Vulnerabilities and Solutions in Mobile WiMAX by Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka

[22] 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.

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

[24] IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16> Neighbor BS Coordination via MS

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

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

[27] 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.

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

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

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

[31] H. Jang, J. Jee, Y-H. Han, S.D. Park, J.Cha, "Mobile IPV6 Fast Handovers over

IEEE 802.16e Networks," MIPSHOP Working Group, Internet Draft.
[32] Liping WANG Fuqiang LIU Yusheng JI, "Performance analysis of fast handover schemes in IEEE 802.16e Broadband Wireless Networks".

List of Papers Published/Communicated

[1] Mohit Saini, Ashish Jain and Dr. Anil K. Verma, "Comparison of Wi-Fi and WiMAX Wireless Technologies", in 11th Punjab Science Congress February 7-9, 2008 (Status: Accepted).

[2] Mohit Saini and Dr. Anil K. Verma, " Analysis of Handover Schemes in IEEE 802.16 (WiMAX)", in International Conference on Pervasive Computing And Governance November 23-25, 2008 (Status: Communicated).