Evaluation of Handover/Handoff in Mobile WiMAX

MS Final Year Dissertation *by:*

Muhammad Shoaib

This dissertation is submitted to I.I.U. in partial fulfillment of the requirements for the degree of

MS Electronic Engineering

Department of Electronic Engineering

Faculty of Engineering and Technology

International Islamic University, Islamabad.

2008

Certificate of Approval

It is certified that we have read the project report submitted by **Muhammad Shoaib [133-FET/MSEE/F-07]**. It is our judgment that this report is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad for degree of MS Electronic Engineering (MSEE).

Supervisor
Dr. Tanweer Ahmed Cheema
Dean, FET, IIU Islamabad.

External Examiner
Dr. Abdul Jalil
Associate Professor
PIEAS, Islamabad.

Naveed

Internal Examiner
Dr. Aqdas Naveed Malik
Assistant Professor, IIU, Islamabad.

Declaration

I hereby declare that this research and simulation, neither as a whole nor as a part thereof has been copied out from any source. It is further declare that I have developed this research, simulation and the accompanied report entirely on the basis of my personal effort made under the guidance of my supervisor and teachers.

If any part of this report to be copied or found to be reported, I shall standby the consequences, no portion of this work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

M. S

Muhammad Shoaib
133-FET/MSEE/F-07

I am grateful to all my friends for their support. I would specially like to thank Zia Mansoor my batch mate for his valuable advices. We would like to dedicate this document to my respected teacher **Prof. Dr. Tanveer Ahmed Cheema .**

بسم الله الرحمن الرحيم

Abstract

In the last few years, the telecommunication industries development has focused on an intensive use of broadband systems, which are characterized by high quality features with Mobile devices. For this issue, new technologies with high transmission abilities have been designed. The broadband wireless access has become the best way to meet escalating business demand for rapid internet connection and integrated "triple play" services. In addition to not only topographic but also technological limitations, wireless solution alternatives have been found. That is the very base of the WiMAX concept: a wireless transmission infrastructure that allows a fast deployment as well as low maintenance costs. Based on the IEEE 802.16e-2005 standard, WiMAX allows for an efficient use of bandwidth in a wide frequency range, and can be used as a last mile solution for broadband internet access.

The aim of this thesis is to implement all compulsory features of the WiMAX OFDM physical layer specified in IEEE 802.16e-2005 in Network Simulator.

The thesis gives an overview about the WiMAX standard and studies the performance of a Handoff in Mobile WiMAX, also covering the performance gains of some optional features, such as the MIMO extension. The influence of these parts on the system performance is shown and analyzed in great detail in simulation results.

Acknowledgements

This thesis was possible because of the will and wish of ALMIGHTY and I am grateful to Him. Next, I express thanks to my Teachers and Parents for their support during all these years of my education.

I am grateful to Wi-Tribe, Pakistan for allowing me to work at their office for the thesis, and my thanks to its employees for providing an encouraging environment, during my stay at the office.

I express my sincere thanks to my supervisors, Dr. Tanveer Ahmed Cheema for their guidance and invaluable time spent on those numerous discussions we had at the office. It is in those fruitful discussions that I learned many more things apart from thesis itself and I am sure those will be helpful in future. Thanks for everything.

My special thanks to him for helping me during the thesis and for the careful reviewing of my thesis report.

My thanks to Mr. Muhammad Haris, my thesis examiner, for his valuable ideas regarding using Network Simulator (NS),

TABLE OF CONTENTS

List of Figures

List of Tables

Acronyms

3GPP/2	3rd Generation Partnership Project/version 2
AAA	Authentication, Authorization, and Accounting
AAS	Advanced Antenna Systems
AC	Access Concentrator
ACK	Acknowledgment
AES	Advanced Encryption Standard
AES-CCM	AES-CTR mode with CBC-MAC
AK	Authorization Key
AKA	Authentication and Key Agreement
AMC	Adaptive Modulation and Coding
ASN	Access Service Network
ASN-GW	Access Service Network Gateway
BE	Best Effort
BPSK	Binary Phase Shift Keying
BS	Base Station
BSID	Base Station Identity
BSS	Basic Service Set
BTC	Block Turbo Code
CBC-MAC	Cipher Block Chaining Message Authentication Coder
CC (1)	Chase Combining
CC (2)	Convolution Coding
CCI	Co-Channel Interference
CDMA	Code Division Multiple Access
CID	Connection Identifier
CINR	Carrier to Interference plus Noise Ratio
CMAC	Cipher based Message Authentication Code
CP	Cyclic Prefix

CQICH	Channel Quality Indicator Channel
CRC	Cyclic Redundancy Check
CSN	Connectivity Service Network
CTC	Convolutional Turbo Coding
CTR	Counter Mode Encryption
DC	Direct Current
DCD	DL Channel Descriptor
DL	Downlink
DoA	Direction of Arrival
DP	Decision Point
DSA	Dynamic Service Addition Deletion
DSC	Dynamic Service Change
DSD	Dynamic Service Deletion
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EP	Enforcement Point
ertPS	Extended Real-Time Polling Service
FBSS	Fast Base Station Switching
FCH	Frame Control Header
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FSS	Frequency Selective Scheduling
FTP	File Transfer Protocol
FUSC	Full Usage of Sub-channels
GMC	Generalized Multi-Carrier
GPRS	General Packet Radio Service
GRD	Guard (interval)
GSM	Global System for Mobile communications

HA	Home Agent
HARQ	Hybrid Automatic Repeat Request
HHO	Hard Handoff
HMAC	keyed-Hash Message Authentication Code
HO	Handoff, or handover
HSDPA	High Speed Downlink Packet Access
HSOPA	High Speed OFDM Packet Access
HSPA	High Speed Packet Access
HSUPA	High Speed Uplink Packet Access
ID	Identifier
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IMT-A	International Mobile Telecommunications Advanced
IPV4	Internet Protocol (version 4)
IPV6	Internet Protocol (version 6)
IR	Incremental Redundancy
ISI	Inter Symbol Interference
ITU	International Telecommunication Union
KEK	Key Encryption Key
LDPC	Low Density Parity check Code
LSB	Least Significant Bit
LTE	Long Term Evolution
MAC	Medium Access Control
MAP	Map, mapping, definition
MBS	Multicast and Broadcast Service
MBWA	Mobile Broadband Wireless Access
MD5	Message-Digest algorithm 5
MDHO	Macro Diversity Handover

MIH	Media Independent Handover
MIMO	Multiple Input Multiple Output
MPEG	Moving Picture Experts Group
MS	Mobile Station
MSB	Most Significant Bit
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol
MSH-DSCH	Mesh Mode Schedule with Distributed Scheduling
NACK	Negative Acknowledgment
NAP	Network Access Provider
ND	Neighbor Discovery
NIST	National Institute of Standards and Technology
NRM	Network Reference Model
nrtPS	Non Real-Time Polling Service
NS-2	Network Simulator version 2
NSP	Network Service Provider
NWG	Network Working Group
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PKMv1/2	Privacy Key Management version 1 or 2
PMP	Point-to-multipoint
PRBS	Pseudo-Random Binary Sequences
PSTN	Public Switched Telephone Network
PUSC	Partial Usage of Sub-channels
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RA	Router Advertisement

RoF	Radio over Fiber
RRA	Radio Resource Agent
RRC	Radio Resource Controller
RRM	Radio Resource Management
RS	Router Solicitation
RSA	public key cryptography method developed by Rivest, Shamir,and Adleman
RTG	Receive/Transmit Transition Gap
rtPS	Real-Time Polling Service
SA	Security Association
SAID	Security Association Identity
SAP	Service Access Point
SDMA	Space-Division Multiple Access
SDU	Service Data Unit
SFN	Single Frequency Network
SIM	Subscriber Identity Module
SIMO	Single Input Multiple Output
SM	Spatial Multiplexing
SNR	Signal-to-Noise Ratio
SOFDMA	Scalable OFDMA (also SOFDMA)
SS	Subscriber Station
STBC	Space-Time Block Code
STC	Space-Time Coding
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
TLS	Transport Layer Security
TTG	Transmit/Receive Transition Gaps

TTLS	Tunneled TLS
TUSC	Tiled Use of Sub-channel
UCD	UL Channel Descriptor
UGS	Unsolicited Grant Service
UL	Uplink
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
WAVE	Wireless Access for the Vehicular Environment
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA(2)	Wi-Fi Protected Access (version 2)
WRAN	Wireless Regional Area Network
VR-(N)RT	Variable-Rate (Non-)Real-Time

Chapter 1

INTRODUCTION

The growth in the use of digital networks has led to the need for the design of new communication networks with higher capacity. The telecom industry is also changing, with a demand for a great range of services, such as video conferences, or applications with multimedia contents. The increased reliance on computer networking and the Internet has resulted in a wider demand for connectivity to be provided "any where, any time", leading to a rise in the requirements for higher capacity and high reliability broadband wireless telecommunication systems.

Broadband availability brings high performance connectivity to over a billion of user's worldwide, thus developing new wireless broadband standards and technologies that will rapidly span wireless coverage. Wireless digital communications are an emerging field that has experienced a spectacular expansion during the last several years. Moreover, the huge uptake rate of mobile phone technology, WLAN (Wireless Local Area Network) and the exponential growth of Internet have resulted in an increased demand for new methods of obtaining high capacity wireless networks.

Mobile WiMAX is a technology introduced in recent years. This technology is based on IEEE802.16e-2005 standard, also known as Mobile WiMAX (Worldwide Interoperability for Microwave Access), which consists of the physical (PHY) and the Medium Access Control (MAC) layers is network architecture of Mobile WiMAX is defined by the WiMAX Forum [1]. This is a wireless, but fixed, data transmission scheme for providing broadband connection to metropolitan areas. It allows communications which have no direct visibility, coming up as an alternative connection for cable, DSL, and T1/E1 systems, as well as a possible transport network for Wi-Fi hot-spots, thus becoming a solution to develop broadband industry platforms. Likewise, products based on WiMAX technology can be combined with other technologies to offer broadband access in many of the possible scenarios of utilization, as shown in Figure 1.1, where the deployment of WiMAX systems are illustrated. WiMAX will substitute other broadband technologies competing in the same segment and will become an excellent solution for the deployment of the well-known last mile infrastructures in places where it is very difficult to get with other technologies, such as cable or DSL, and where the costs of deployment and maintenance of such technologies would not be profitable. In this way, WiMAX will connect rural areas in developing countries as well as underserved metropolitan areas. It can even be used to deliver backhaul for carrier structures, enterprise campus, and Wi-Fi hot-spots. WiMAX offers a good solution for these challenges because it provides a cost-effective, rapidly deployable solution. WiMAX will represent a serious competitor to 3G (Third Generation) cellular systems as high speed mobile data applications will be achieved with the 802.16e-2005 specification.

The traditional WiMAX restricted the user ability for the user to move during the transmission. Therefore, the moving users need for the change of serving base stations, It is virtually called a Handoff/Handover. It creates demands for the Mobile WiMAX. The handoffs/Handovers should be fast enough so that the ongoing video call or Voice over IP (VoIP) conversation is not interrupted, at least for so long that the user notices it.

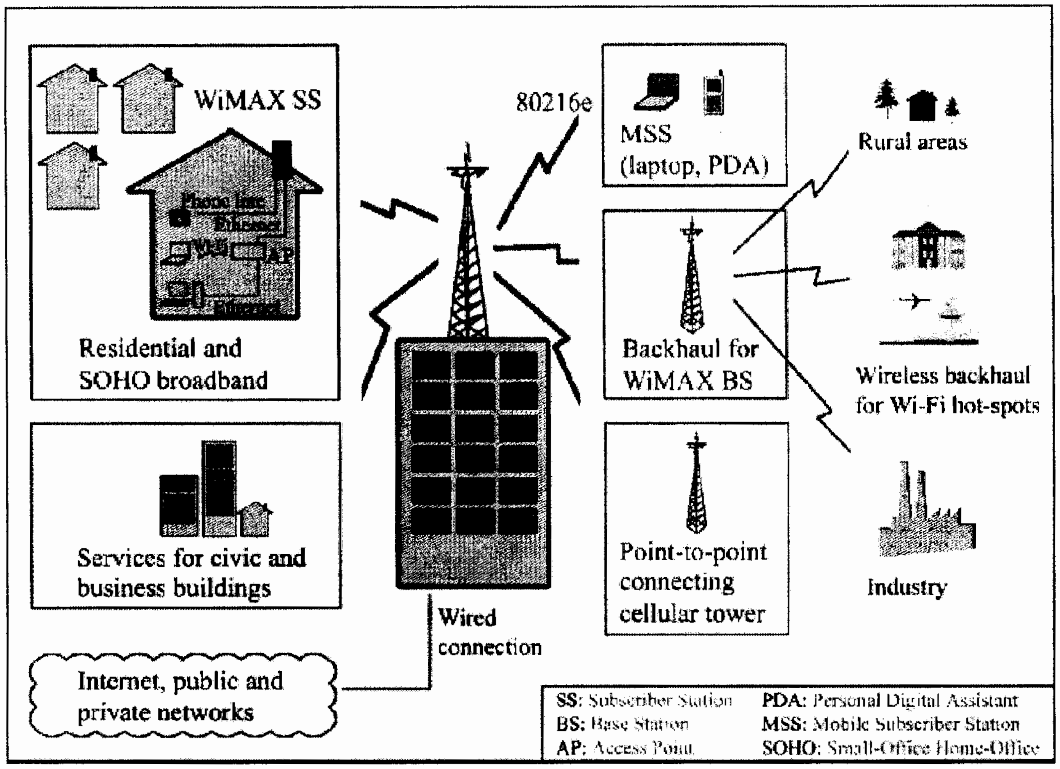

WiMAX SS
Phone line
Ethernet
WiFi
AP
Ethernet
Residential and SOHO broadband
Services for civic and business buildings
Internet, public and private networks
80216e
Wired connection
MSS (laptop, PDA)
Backhaul for WiMAX BS
Point-to-point connecting cellular tower
Rural areas
Wireless backhaul for Wi-Fi hot-spots
Industry
SS: Subscriber Station
BS: Base Station
AP: Access Point
PDA: Personal Digital Assistant
MSS: Mobile Subscriber Station
SOHO: Small-Office Home-Office

Figure 1.1 - Deployment Scenarios of the WiMAX

This thesis introduces a new 802.16e-2005 amendment to the 802.16-2004 standards, the 802.16e-2005, or the Mobile WiMAX, introduces the most significant new feature, the support for handoffs, which can be considered as a basic requirement for mobile communication system. The mandatory handoff method in Mobile WiMAX is the Hard Handover and the two optional soft handoff methods are called Macro Diversity Handover and Fast Base Station Switching. To support mobility, the Mobile WiMAX introduces also the Scalable OFDMA, which is a multiplexing scheme that allows adjustments of bandwidth according to the physical conditions of the used channel at a certain moment. This makes possible the versatile deployment of various environments with different propagation characteristics. The NS-2 simulator did not initially include support for Mobile WiMAX so two add-on modules from NIST had to be installed. The handoff latency was measured and the parameters of the simulator adjusted in order to achieve best possible handoff times. The find out which parameters had the greatest impact on the handoff duration and to compare the results to the objectives set by the WiMAX Forum. The WiMAX Forum says that the Mobile WiMAX supports mobility up to 120 km/h and the handoff should take less than 50 ms. the results showed that some of the parameters did not have an influence at all and some could be enhanced to achieve faster handoffs. The handoff times remained below the 50 ms limit up to 20 m/s (72 km/h). The promised higher speed handoffs are designed to use the soft handoff methods.

Chapter 2

MOBILE WIMAX RADIO NETWORKS

This chapter is dedicated the mobile WiMAX (802.16e.2005) technology. First physical and MAC layer properties are introduced. Later on the security issues are discussed with only inherent mobility capability [2], [3], [4] and [5] some possible competing or co-existing technologies in wireless communications technologies in wireless communications are also introduced.

2.1 Mobile WiMAX Physical (PHY) Layer

The 802.16-2004 specification and the 802.16e-2005 amendments define five PHY alternatives:

- Wireless MAN-SC (Wireless Metropolitan Area Network using Single Carrier Modulation for use in the 10-66 GHz bandwidth region)
- Wireless MAN-SCa (Wireless Metropolitan Area Network using Single Carrier Modulation for use on bandwidth below 11 GHz)
- Wireless MAN-OFDM (Wireless Metropolitan Area Network using OFDM)
- Wireless HUMAN (Wireless High-Speed Unlicensed Metropolitan Area Network)

Orthogonal Frequency Division Multiple Access (OFDMA) creates the fundamental functions of Mobile WiMAX.

2.1.1 Orthogonal Frequency Division Multiple Access Basics

Orthogonal Frequency Division Multiplexing (OFDM) is a digital modulation scheme suited especially well for terrestrial broadcasting. It can handle multipath propagation and delays between received signals. It is sensitive to frequency changes as Doppler shift while the mobile station is moving. OFDMA is the solution considered to be the modulation scheme in most future advanced wireless communications technologies. Another view, mobile WiMAX would have 40 percent share of wireless broad band markets. The actual figures are probably something between the mentioned. This is based on the success of newly launched technology. OFDMA has varied advantages over traditional Code Division Multiple Access (CDMA) versions used in post Global System for Mobile communications (GSM) 3rd Generation (3G) technology. In OFDMA data streams from different users are combined to sub-channels in both Downlink (DL) and Uplink (UL) [8].

OFDM Basic Principle: The OFDM used bandwidth is divided into several frequency sub-carriers so that they are orthogonal to each other. The stream of input data is separated into multiple, parallel sub-streams with reduced data rate. Then the sub-streams are modulated individually and sent on separate sub-carriers. Consequence of this is the increase in symbol duration. Since the long signal duration decreases Inter Symbol Interference (ISI) caused by multipath propagation, it is efficient to transmit the low-rate streams in parallel, instead of one high-rate stream. The signal duration is long, so by using a proper guard interval, the ISI can be avoided totally, assuming the guard interval is longer than the difference between the first and last multipath echo. The principle of several sub-streams combined at the transmitter and separated again at the receiver. In OFDM system architecture, information is coded and modulated across the sub-carriers before performing an Inverse Fast Fourier Transform (IFFT), as show in Figure 2.1.

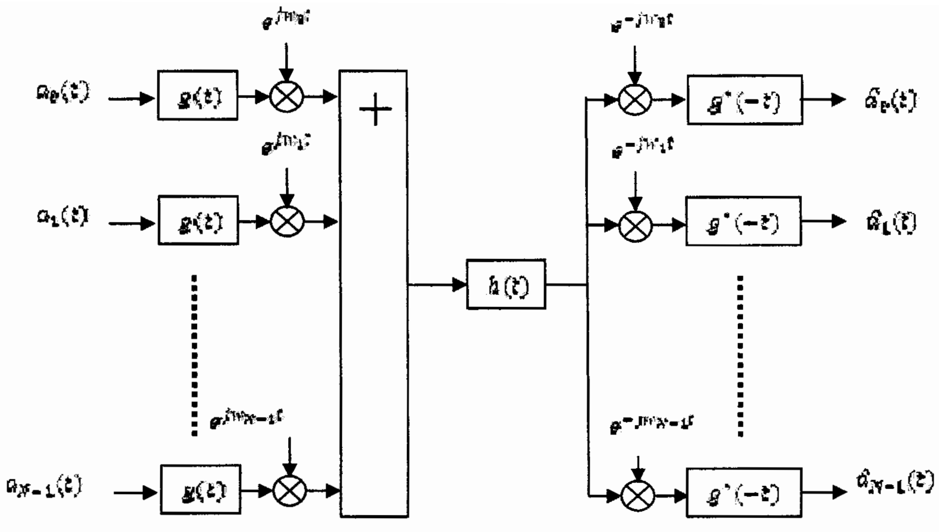


Figure 2.1 - Basic Architecture of an OFDM System

The IFFT takes advantage of the frequency diversity of the multi-paths channel. Consequently, before transmitting the data, the streams are combined to a single signal and sent to the air interface. The 802.16e-2005 defines as Fast Fourier Transform (FFT) size to be 128, 512, 1024 or 2048 with respective channel bandwidth 1.25, 5,10and 20MHz.OFDM available resources may be divided into time and frequency domains [4].

Scalable OFDMA: SOFDMA creates the basis for 802.16e-2005. Basically SOFDMA gives a mean of possibility to adjust the used bandwidth. This is required due to different environment with varying spectral requirements. The bandwidth adjustment can be chosen between 1.25-20 MHz as described in Table 2.1 below. The scalability is realized with FFT size variations and the frequency spacing of sub-carriers is defined to be10.94KHz.

Table 2.1 - OFDMA Scalability Parameters

Parameters	**Values**			
System Channel Bandwidth (MHz)	1.25	5	10	20
Sampling Frequency (MHz)	1.4	5.6	11.2	22.4
FFT Size	1.28	512	1024	2048
Number of Sub-Channels	2	8	26	32
Sub-Carrier Frequency Spacing	10.94kHz			
Useful Symbol Time (T_b=1/f)	91.4 µs			
Guard Time (T_g=T_b/8)	11.4µs			
OFDMA Symbol Duration (T_s=T_b+T_g)	102.9µs			
Number of OFDMA Symbols (5 ms frame)	48			

Cyclic Prefix (CP): A Cyclic Prefix (CP) is sent and usually the CP has the same length as the guard interval. The CP consists of the end of the symbol placed in the beginning of the new symbol, as can be seen in Figure 2.2.

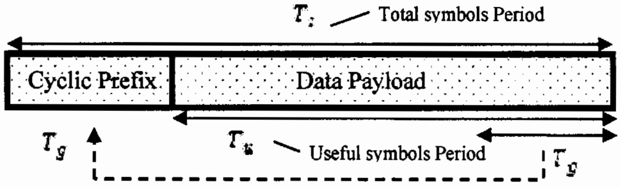


Figure 2.2 - Insertion of Cyclic Prefix

The task of the CP is to settle the echoes from multipath propagation before the actual data can be processed. A negative aspect with the use of CP is the extra overhead and therefore the bandwidth efficiency is affected. However, the channel bandwidth can be used in an efficient way for data transmission since the OFDM spectrum fades fast outside the actual window containing the carriers, as shown in Figure 2.3. It is also important to keep the CP length defined by the Base Station (BS) during initialization because the change of it would force all other MSs to resynchronize.

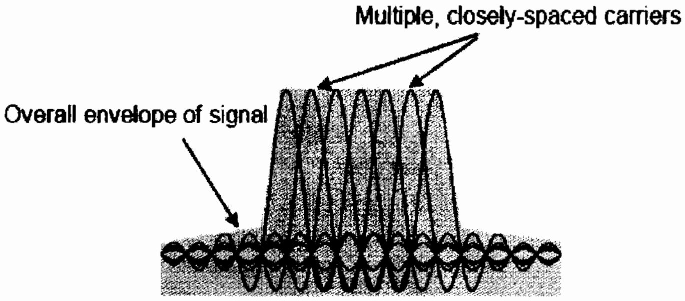


Figure 2.3 - OFDM Spectrum

The selection of FFT size is matter of balance between problems caused by multi path propagation. The FFT size is increased the sub-carrier spacing is decreased and this the total symbol length will increase [9].

2.1.2 OFDMA Symbol Structure and Sub-Channelization

The OFDMA symbol structure consists of three types of subcarriers are used in OFDMA symbols. Data sub-carriers handle the transmission of data, pilot sub-carriers are used for the estimation and synchronization use, and null sub-carriers have no transmission. They are intended for guard bands and Direct Current (DC) carriers. The OFDM symbol structure is shown in Figure 2.4.

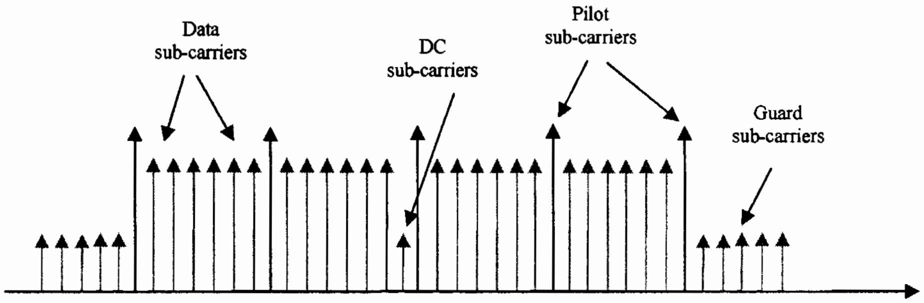


Figure 2.4 - OFDMA Sub-carrier Structure

The definitions sub-carrier and sub-channel may be defined as clarified in the “a subset of data or pilot sub-carriers is a sub-channel and the OFDM symbol consists of several sub-channels". Sub-channelization defines the smallest time-frequency resource unit to be a slot. One slot is the same as 48 data tones, (in other words sub-carriers). Sub-channelization is supported in both link directions. Sub-carrier permutation of sub-channelization can be done in two ways in Mobile WiMAX, with diversity or contiguous permutation. In most of the cases, the diversity permutations are better suited for mobile environment while the contiguous permutations are more applicable for environment with fixed, portable, or low-mobility devices. The choice between these two can be made either to increase throughput or to give more flexibility considering the movement of the user.

Diversity Permutation: The diversity permutation, also known as distributed permutation [10], arranges sub-carriers in a pseudo-random way to create a sub-channel. This enables frequency diversity and averages the inter-cell interference. The available permutations are Downlink Full Usage of Sub-channels (DL FUSC), Downlink Partial Usage of Sub-channels (DL PUSC) and UL PUSC. The 802.16e-2005 defines also optional permutations, such as optional FUSC (OFUSC), Tiled Use of Sub-channel 1 and 2 (TUSC1/2).

Contiguous Permutation: The adjacent, or the contiguous permutation, creates a sub-channel by grouping a block of contiguous sub-carriers. The available modes for contiguous permutation are the Adaptive Modulation and Coding for both DL and UL (DL AMC and UL AMC). The optional AMC allows modulation and coding adjustments to be performed based on current channel conditions. The
Table 2.2 below describes the main differences between the two permutation types.

Table 2.2 - Comparison of Permutation Modes

	Contiguous sub-carrier permutation (Amc)	Diversity sub-carrier permutation (PUSC,FUSC)
Benefits	Sub-channelization gain; Frequency selective loading gain	Sub-channelization gain; Frequency diversity; Inter-cell Interference averaging
Scheduling	Advanced frequency scheduler to explore frequency selectivity gain	Simple scheduler; Rely on frequency diversity to achieve robust transmission
channel condition	Stationary channel	Fast-changing channel
Favorable Smart antenna technology	Beam forming	MIMO

2.1.3 Time Division Duplex Frame Structure

Mobile WiMAX used to support only Time Division Duplex (TDD) but Full and Half –Duplex Frequency Division Duplex (FDD) support has been added too. FDD requires a pair channel while TDD can share one for both [4].An OFDM frame begins with a preamble and continues with both DL & UL sub-frame, which can have the length ratio varying from 3:1 to 1:1.They are a parted by Transmit/ Receive and Receive/Transmit Gaps (TTG/RTG).The TTG follows the DL sub-frame and RTG the UL. These are used for collision avoidance. Figure 2.5 demonstrates the structure of an OFDMA TDD frame. There are additional and optional fields as well that can be used in the sub-frames. The mandatory and optional fields are discussed in sub-subsections after the figure [2], [9].

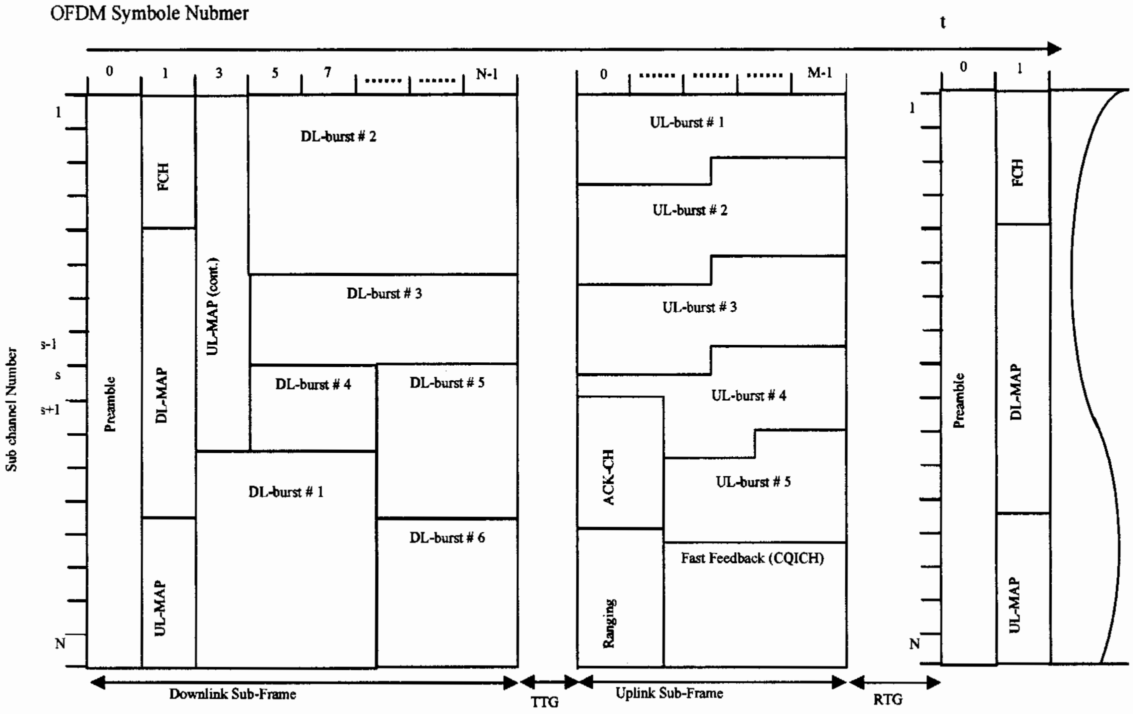


Figure 2.5 - OFDMA Frame Structure in TDD

Preamble: TTG and RTG the preamble is the first symbol in an OFDMA (TDD) frame. It can consist of one or two symbol depending on the type of preamble. There is a preamble before both the DL & UL sub–frames. An optional scheme for preamble is supported as well, where short preambles, called midambles can be used in UL after 8, 16 and 32 symbols.

Frame Control Header (FCH): The preamble is followed by a Frame Control Header (FCH), which contains frame configuration information about the length of MAP message following the FCH, modulation and coding scheme, and the available sub-carriers.

DL/UL Mapping (MAP) messages: After the FCH, the DL sub –frame contains broadcast DL-MAP and UL-MAP message. The actual data payload from different users is carried with in DL bursts that can have varying size or type depending on the application of a user. The UL sub– frame contains a field for ranging purpose. This field is reserved for the MSs to do periodic closed loop time. The UL bursts have the same functionally as the bursts in DL direction. UL also has two optional fields that can be used to enhance the performance of Mobile WiMAX,

2.1.4 Other Advanced PHY Layer Features

To achieve performance improvements in coverage and capacity Mobile WiMAX has received some new features compared to the traditional WiMAX.

Adaptive Modulation and Coding (AMC): Modulation techniques required for the DL direction in Mobile WiMAX are Quadrature Phase Shift Keying (QPSK), 16-point Quadrature Amplitude Modulation (16QAM), and 64QAM. The last one is optional in the UL direction. Coding is achieved with Convolutional Coding (CC) or Convolutional Turbo Coding (CTC) with variable code rate and repetition coding. Optional coding methods are Block Turbo Code (BTC) and Low Density Parity check Code (LDPC). Table 2.3 describes the supported modulation and coding methods.

Table 2.3 - Supported Modulations and Codes

		DL	UL
Modulation		QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM
Code Rate	CC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, 5/6
	CTC	1/2, 2/3, 3/4, 5/6	1/2, 2/3, 5/6
	Repetition	X2, X4, X6	X2, X4, X6

The modulation and the coding have a direct impact on the achievable data rate, hence, one reaches higher rates with the 64QAM, but the channel is weaker to disturbances, and vice versa for the QPSK. Since there are several possibilities to choose the modulation and the coding, the range of data rates in Mobile WiMAX is rather versatile.

Fast Feedback Channel (CQICH): Channel Quality Indicator Channel (CQICH) is an optional channel used for delivering information about the channel condition for Mobile Station (MS) to the scheduler of the BS [4].

Hybrid Automatic Repeat Request (HARQ): Automatic respect request (ARQ) methods are intended for situations the sent packet has not been received properly e.g. due to bit errors, and a transmission is required. HARQ is an optional part of the MOBILE WIMAX MAC. While using HARQ, several MAC Protocol Data Unit (PDU) can be combining to a HARQ Packet. The HARQ packet is formed by adding a Cyclic Redundancy Check (CRC) field to the MAC PDUs. The construction of HARQ encoder packer in shown in Figure 2.6. The parity field contains the information for possible error detection and correction.

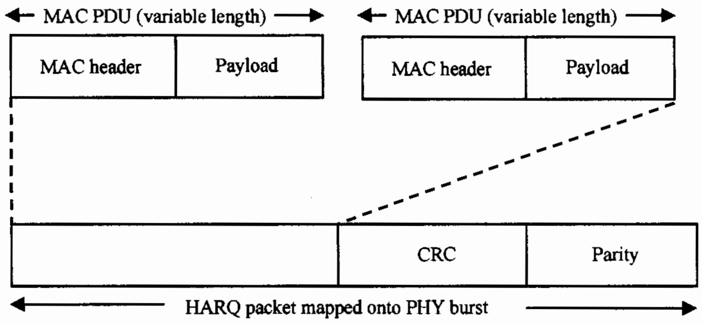

MAC PDU (variable length)
MAC PDU (variable length)
MAC header
Payload
MAC header
Payload
CRC
Parity
HARQ packet mapped onto PHY burst

Figure 2.6 - Construction of HARQ Encoder Packet

HARQ is fundamentally a protocol with a stop and wait nature with support for several HARQ channels per connection. UL sub-frame includes an option for dedicated acknowledgement channel UL-ACK to be used with Hybrid Automatic Repeat Request Acknowledgment /Negative Acknowledgment (HARQ

ACK/NACK) signaling from MS to the BS.

2.2 Mobile WiMAX Medium Access Control (MAC) Layer

The DL in WiMAX runs on a PMP networking basis, which means the principle of a single BS transmitting to one or several users. On a certain frequency channel and antenna sector all SSs, fixed or mobile, receive the same transmission from the BS, unless it is clearly defined in DL-MAP that a certain sub-frame is for a certain Subscriber Station (SS). The Connection Identifiers (CIDs) in received PDUs are inspected by the receiver SSs and only those addressed to them are held. The UL is shared on a demand basis and the resources are given according to the services needed. Naturally, the BS determines whether the SS has the right to access them or not. Unlike in PMP, the Mesh BS cannot transmit without agreeing with other nodes, hence up to the nodes in the extended neighborhood. With distributed scheduling, all nodes broadcast periodically according agreed schedules their current schedules, with possible proposed changes to them, to all neighbors in a two-hop distance. The nodes must ensure that the transmission does not result in collisions with any other data or control traffic from members of normal or extended neighborhoods, in both DL and UL. Another Mesh networking scheduling method is called centralized scheduling, which is based on the Mesh BS that collects resource requests from neighboring SSs within determined distance of hops. It decides permissions for DL and UL traffic, and informs the Mesh SSs within the hop range about the granted resources [2], [3].

2.2.1 Data / control plane

Addressing and Connections: In PMP, every air interface in a MS is given a unique MAC address; just like regular Ethernet network adapters. The address is used with initial ranging process and, as a part of authentication process. A connection between BS and MS is identified with a CID. The MS contacts the

BS, two management connection pairs (DL and UL) are created. These connections form three different Quality of Service (QoS) levels available for management traffic. The first connection, called basic, is intended for exchanging short and time-urgent messages, while the other, called primary, can be used for longer and more delay-tolerant management traffic between the MS and BS MACs. The optional, third connection is called secondary management connection, which is used for delay-tolerant, standards-based messages. A broadcast connection for delivery of some management messages is also available. CIDs for above management connections are defined in ranging or registration response messages RNG-RSP and REG-RSP, respectively. Transmission requests are dependent on management CIDs because the allowable bandwidth can vary for different connections even while still having the same service type. Traffic from several higher level sessions with common service requirement parameters can be combined to a single connection. The Mesh networking also MAC addresses, just like the PMP does above. After successful authentication the node receives a Node Identifier. The nodes create link Identifier between every neighboring node they are linked to. The Link IDs are used with distributed scheduling in order to identify requests and grants of resources. In Mesh networking the traffic is broadcast to all nodes, which can determine the granted schedule by investigating the Node ID of the transmitter and Link ID in a Mesh Mode Schedule with Distributed Scheduling (MSH-DSCH) message [2], [3].

MAC Protocol Data Unit (PDU) formats: The structure of a MAC PDU is demonstrated in Figure 2.7. The PDU begins with a generic MAC header field that has a fixed length. The second field is the payload which may also be empty. The payload can, but does not have to, consist of sub-headers or MAC Service Data Units (SDU) and/or fragments thereof. The length of the payload can vary, so the MAC PDU cannot be explicitly determined in bytes. The final field is used for a CRC, which is required for OFDM and OFDMA PHY layers, while for some

802.16-2004 PHY layers it is optional.

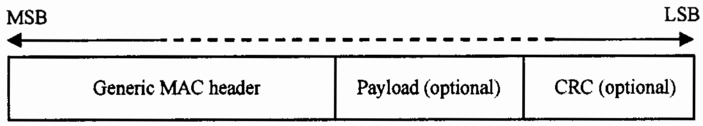


Figure 2.7 - MAC PDU Format

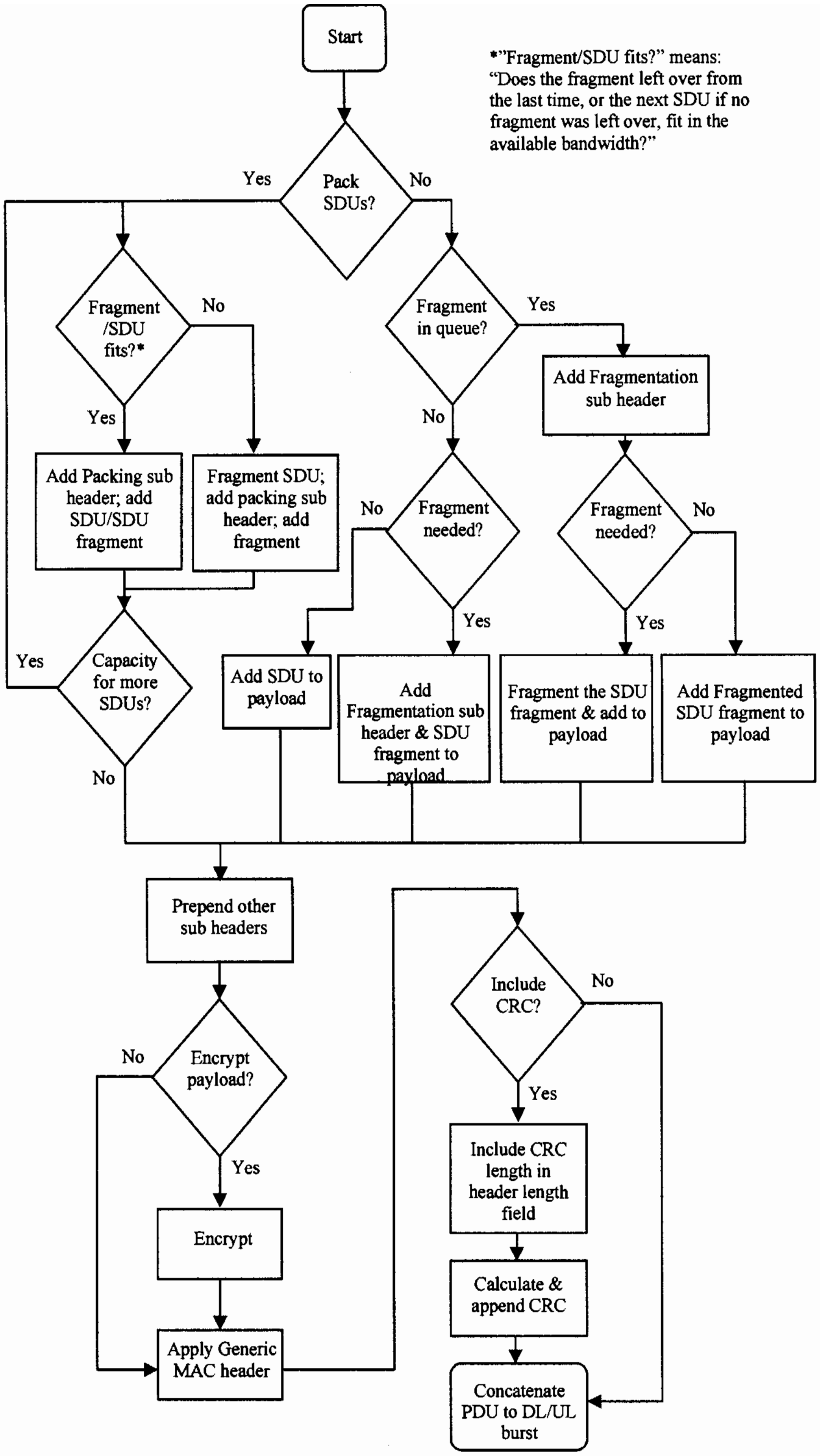
MAC Management Messages: In this sub-section some important messages are sent for the MAC layer is presented. The messages are transmitted in the payload part of the PDU.

Downlink/Uplink map (DL/UL-MAP) messages: An intended for definition of access to the downlink/uplink information.

Ranging Request/Response (RNG-REQ/RSP) messages: A request-response pair during the initial network entry process. The RNGREQ is sent by the MS during the initialization and later in a periodic way. The ranging process determines the delay in the network with request for power and/or downlink burst profile changes. RNG-RSP message is a response to the previous RNG-REQ message. The RNGRSP can also be sent asynchronously in order to apply adjustments according to measured values from other received data or MAC messages. Every PDU has a unique CID that allows the receiving MAC to resolve the MAC SDU from one or more received PDUs and to deliver the SDU to a respective MAC. Hence, the MS may receive RNG-RSP message anytime, not just upon request.

Registration Request/Response (REG-REQ/RSP) messages: Are used during the initialization phase. The MS request registration by sending the REG-REQ message to the BS and the BS responses with REG-RSP. The messages include information about more detailed properties of the connection to be created.

Construction and Transmission of MAC PDUs: The flow process for MAC PDU [3] construction is show in Figure 2.8.


Start
Pack SDUs?
Yes
No
Fragment /SDU fits?*
No
Yes
Add Packing sub header; add SDU/SDU fragment
Fragment SDU; add packing sub header; add fragment
Capacity for more SDUs?
Yes
No
Fragment in queue?
Yes
No
Add Fragmentation sub header
Fragment needed?
No
Yes
Fragment needed?
No
Yes
Add SDU to payload
Add Fragmentation sub header & SDU fragment to payload
Fragment the SDU fragment & add to payload
Add Fragmented SDU fragment to payload
Prepend other sub headers
Encrypt payload?
No
Yes
Encrypt
Apply Generic MAC header
Include CRC?
No
Yes
Include CRC length in header length field
Calculate & append CRC
Concatenate PDU to DL/UL burst

*"Fragment/SDU fits?" means:
"Does the fragment left over from the last time, or the next SDU if no fragment was left over, fit in the available bandwidth?"

Figure 2.8 - Construction of MAC PDU

Concatenation: Is a procedure for combining multiple MAC PDUs into a single transmission, in DL or UL. Every PDU has a unique CID that allows the receiving MAC to resolve the MAC SDU from one or more received PDUs and to deliver the SDU to a respective MAC Service Access Point (SAP). The PDUs for MAC management messages, user data, and bandwidth requests can also be included in the same transmission. Figure 2.9 the situation for UL burst transmission.

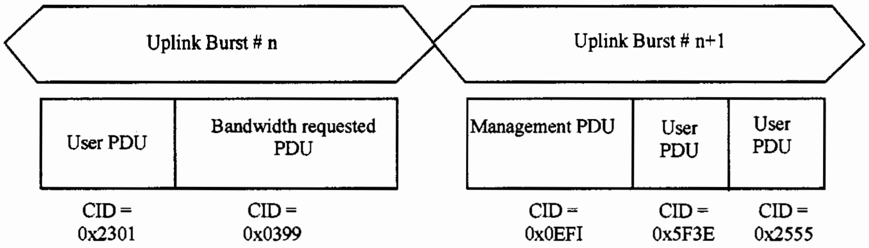


Figure 2.9 - MAC PDU Concatenation Showing CIDs

Fragmentation: Can occur MAC SDU or management message cannot fit into a MAC PDU and have to be divided into several PDUs. The fragmentation and reassembly are needed to better utilize the available bandwidth and they must be supported by the equipment.

Packing: Allows several SDUs to be packed into a single PDU. The decision is made in the transmitting station and the unpacking is made obligatory for all stations.

CRC calculation: Can be required by some connections and in these cases the CRC field is added to respective PDUs containing data for those connections. The CRC will include the generic MAC header and the payload part of the PDU. In case encryption is used, the CRC calculation is performed after it.

Encryption: Is performed to the payload of MAC PDU the connection is mapped to

Security Association (SA). The encryption and data authentication are done in the transmitting end according to the specifications of the SA and the reverse operation of decryption and data authentication at the receiver is based on that same SA. As stated, only the payload is encrypted while the generic MAC header consists of the unencrypted information required for decryption. A PDU mapped to an SA requiring encryption is received unencrypted, it is simply rejected.

Padding: Is intended for filling up the unused parts of an allocated space within a data burst. The space must be in a known state, which can be achieved by setting every unused byte to a stuff byte value (0xFF). In case the size of the unused section is greater than (or exactly) a MAC header length, it can also be formatted as an MAC PDU [2] [3].

2.2.2 Quality of Service (QoS) Support

Mobile WiMAX is suited for supplying various QoS methods for different types of data services and applications. These flows are unidirectional packets with certain QoS parameters and are demonstrating the principle. Figure 2.10 show the QoS.

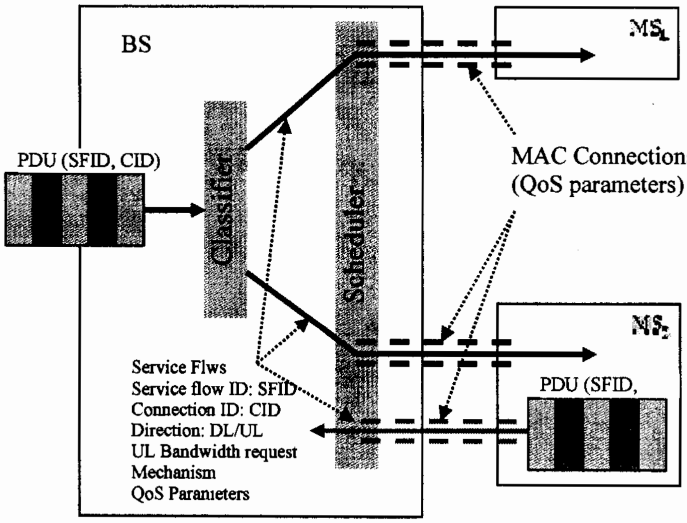


Figure 2.10 - Mobile WiMAX QoS Support

Some type of data service is wanted to be offered, a connection is to be created between BS and the MS this service flow the certain QoS parameters that gives the scheduler a chance to so decisions for transmission priorities even during the transmission. Since the QoS is connection-oriented, it can be effectively controlled during the transmission. This enables an end-to-end QoS even over the air interface, which usually is the main problem in wireless communications. The service flow principle is supported in both DL and UL. The Table 2.4 demonstrates used specifications for different data services and applications.

Table 2.4 - Mobile WiMAX Applications and QoS

QoS Category	**Application**	**QoS Specification**
UGS **Unsolicited Grant Service**	VoIP	• Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance
rtPS **Real-Time Polling Service**	Streaming Audio or Video	• Minimum Reserved Rate • Maximum sustained Rate • Tolerance • Traffic Priority
ertPS **Extended Real-Time Polling Service**	Voice with Activity Detection (VoIP)	• Minimum Reserved Rate • Maximum sustained Rate • Maximum Latency • Jitter Tolerance • Traffic Priority
nrtPS **Non Real-Time Polling service**	File Transfer Protocol (FTP)	• Minimum Reserved Rate • Maximum sustained Rate • Traffic Priority
BE **Best Effort Service**	Data Transfer; Web Browsing, etc	• Maximum sustained Rate • Traffic Priority

2.2.3 MAC Scheduling Service

A mobile user creates special requirements for the transmission because of the continuous change in the used transmission medium. Scheduling for DL and UL, Dynamic resource Allocation, QoS oriented scheduling, and frequency selective scheduling. The scheduling type and related QoS specifications are needed for the BS to be able to predict the needs of the MS regarding throughout and latency of the UL traffic. The Unsolicited Grant Service (UGS) focuses on UL traffic with real time requirements with fixed packet length sent on a periodic basis .The size of the grants is defined based on the maximum sustained traffic rate of the service flow. The Extended Real-Time Polling Service (ert PS) is a combination of the two previous services UGS and Real-Time Polling Service (rtPS). Similar to UGS there is a maximum sustained traffic rate which defines the default size of the allocation. The rtPS offers polls that are sent on uni-cast and on a regular basis .The intervals between polls are not constant but, any way they are kept short enough to provide sufficient service for the MS .The Best Effort (BE) service is intended for traffic without strict requirements for latency and QoS in general.

2.2.4 Bandwidth Allocation and Request Mechanisms

In order to transmit anything MS must request bandwidth for the transmission from the BS .The BS offering grants to the MS for bandwidth allocation according the request sent earlier. The requests are associated in the MS with certain connections by their CIDs but the grants are associated with the basic CIDs of the MS. The MS can simply settle to the decision of BS and drop the SDU or to request again. As told in the previous paragraph, the bandwidth requests are always linked to CIDs and the grant are addressed to certain MSs, which is the case for polling as well. In single BS polling the basic CID of the MS is used and with multi brad cast polling the UL-MAP includes a special CID dedicated to multi broadcast [4].

2.2.5 Mobility Management

The main issues for mobile application in general are the inadequate power resources with challenges in handoffs. The Mobile WiMAX has two modes to allow power saving possible, the Sleep Mode and the Idle Mode. The Mobile WiMAX is also said [4] to support seamless (connection not broken while changing the BS) handoffs, up to the speed of 100 km/h.

2.2.6 Security

Mobile and wireless application are demanded more security compared to traditional fixed and wired connection. The mobile WiMAX supports mutual device authenticities with a flexible key management control.

Key Management Protocol: The security issues or mobile WiMAX are defined as a sub layer in MAC layer. The used protocol, and the basis for WiMAX security, is privacy and key management protocol with versions 1 and 2 (PKMv1/2). The (Fixed) WiMAX supports only the first version while the Mobile WiMAX supports both.

Device/User Authentication and Authorization: A mobile WiMAX device is turned on it tries to connect to a BS. However a reliable connection between the user and the BS has to be ensured. The RSA based solution is dependent on a unique X.509 certificate, which is issued by the ms manufacturer. The ms is requested an Authorization Key (AK) it sends the digital certificate to the BS which confirm the certificate The Extensible Authentication Protocol (EAP) based solution uses an exclusive credential provided by the operator with Subscriber Identity Module (SIM) the used type is EAP. Authentication and key agreement (AKA) or with x.509EAP TTLS Tunneled TLS (TTLS) [4], [11], [12], [13].

Traffic Encryption: The mobile WiMAX MAC layer uses AES-CCM CTR with CBC-MAC where CTR comes from counter mode Encryption and CBC-MAC from cipher Block chaining message Authentication cod. The TEK is generated in the Bs and is a random number created with the TEK encryption algorithm with the KEK as the encryption key.

Fast Handoff Support: The fast hand offs supported by the mobile WiMAX set requirements also for the privacy of the information exchanged during the change of BSs. The mobile WiMAX offers a possibility to use a pre-authentication, which is simply authentication performed before with a target Bs. In order to make the handoff faster. Another presented weakness in Mobile WiMAX security is related to the access network. They point out that the 802.16e-2005 (or 802.16-2004) [14] specification does not provide any security measures within the access network, but the specification only assumes the access service network to be trusted.

2.3 Fractional Frequency Reuse

To take advantage of the most of the channel bandwidth the mobile WiMAX supports fractional frequency reuse. The used reuse pattern is one 1x1.The Co-Channel Interference (CCI) can be mitigated by just arranging the used sub-channels properly. The sub-channel arrangement is made possible by segmentation and a permutation zone. The permutation zone is described as a number of contiguous OFDMA symbols in DL or UL that use the same permutation. The Figure 2.11 shows the frame structure with multiple zones.

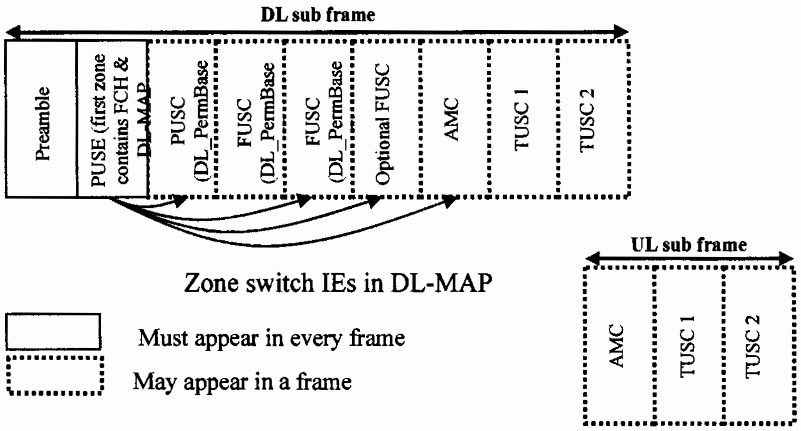


Figure 2.11 - Multi-Zone Frame Structure

The partly used sub-channels must be different than the ones used in the neighboring BS. Although this method gives users at cell edge better chances to maintain the connection with BS, the accessible band with is limited and there for the data rates are affected. The Figure 2.12 is show the principle of fractional frequency reuse. Hence near the BS all sub-channel groups F1, F2, and F3 can be used simultaneously while they are used separately at the cell edges.

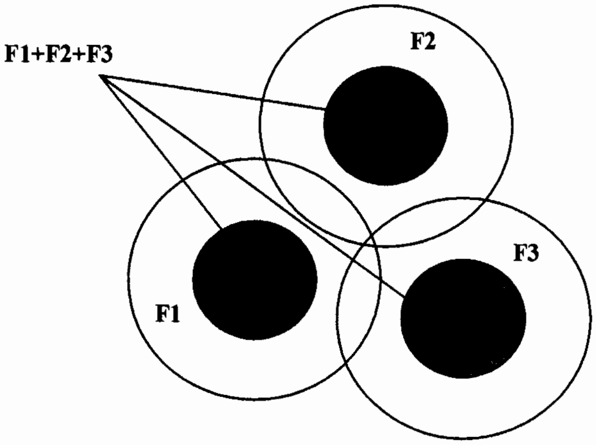


Figure 2.12 - Fractional Frequency Reuse

2.4 Wireless Local Area Network (802.11x)

Currently the WLAN, usually denoting the IEEE 802.11 family, is the solution to be used creating a wireless network inside companies, homes, or other public building. The 802.11a is still in use on some locations where the back hall connection to the access point (name for a BS) cannot be created with wired connection and the clients subsequently use 802.11b or 802.11g for communication with access point. The 802.11 technologies are well suited for communications with short distance to the access. The coverage indoor is only a couple of tens of meters and in perfect conditions outdoors the signal can travel a few hundred meters. There are also other amendments in the 802.11 family that are focused on providing a certain service with some of the transmission amendments. There have also been attempts to increase the mobile use of 802.11 technologies. The 802.11 or also known as fast roaming or fast Basic service set transition is focused on providing hand offs for a moving MS [15], [16].

Chapter 3

MOBILITY

Today the use and rapid increase of mobile is very remarkable mostly owing to new technologies providing sufficient data rate able to compete with traditional wired connections used at homes. The users want to have access to the same services as they are uses to no matter where they happen to be. This creates a fact that the e-mails, instant messaging, multimedia, streaming and web browsing are coming to mobile phones, PDAS, and laptops. However, the development of networks supporting mobility sets several requirements for a device planned to be used "on the go". The first, and maybe the most important, requirement is the ability of a device to change the serving BS according to the movements of the user. This has to be performed without disturbances in the connection and maintaining the confidentiality between the MS and both, old and new, BSs. A very likely usage scenario could be a user in a public transportation vehicle or in a normal car which means that the handoffs and communicating in general need to be supported even in a vehicle moving with a rather high speed. The second obstacle a mobile device has to face is the limited power resources. Therefore the mobility of a user has been the major problem with traditional WiMAX functionality, since it supported only nomadic access. Nomadic access the user was able to change the location of the subscriber station, but without the support for handoffs. The new 802.16e-2005 will to solve these problems and truly make WiMAX go mobile. In the following sections we go through the building blocks of mobility in WiMAX by starting with description of the network architecture behind Mobile WiMAX. Previously there has been only discussion about the connection between the MS and BS.

3.1 Structure of Network

The key property of Mobile WiMAX network is the all-IP (both IPv4 and IPv6) platform which leaves out the traditional circuit switched alternatives. This allows financial savings since there is no need to maintain both types of core networks. The 802.16e-2005 standard defines only the air interface while the implementation of the network connecting the BSs and providing the access to the Internet is left to service providers. The main element of a Mobile WiMAX shown in Figure 3.1 below describes the basic structure of the Mobile WiMAX network. The MSs are connected via air to BSs. The BSs connect via routers to an access gateway which again is connected to a Connectivity Service Network (CSN). The CSN has the functionalities of a home agent and authentication with the access to the Internet.

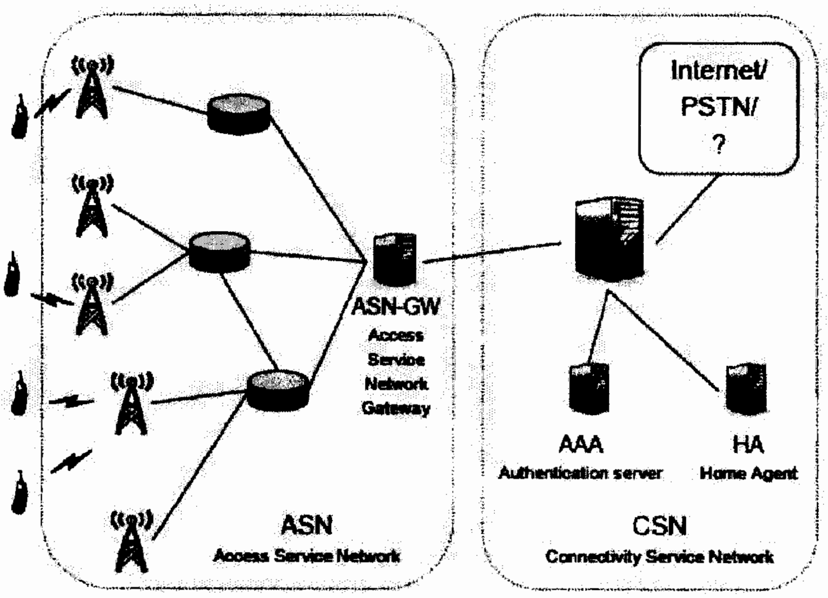


Figure 3.1 - Mobile WiMAX Network Structure

3.1.1 Access to Service Network

The ASN provide all the needed network components to offer radio access to a

WiMAX subscriber [17]. It has the task of providing the WiMAX-L2 connectivity to a WiMAX-MS. It also transfers the authentication, authorization and user accounting information to the home network service provider. Network discovery and selection of a preferred Network Service Provider (NSP) to the user are taken care of in the ASN. The ASN has to deal with relay functionality to enable L3 connectivity to a WiMAX MS, hence providing an IP address. The effective usage of radio resources are also handled with the ASN. The requirements and tasks above are intended for WiMAX in general, but the mobile applications have yet other demands. Hence, ASN/CSN anchored mobility must be supported. The ASN anchored mobility is described as the functionalities needed to allow an MS to change a BS, hence handoffs, as long as the foreign agent is not changed. On the other hand, the CSN anchored mobility allows the change of anchor point within the ASN, but the CSN anchor point is the same. The Mobile WiMAX ASN must also support paging and tunneling between the ASN and the CSN.

3.1.2 Connectivity to Service Network

The general task of the CSN is to provide IP connectivity services to the WiMAX subscriber(s). [17] The CSN is given some other function, which is not defined as required properties, but however, they usually are present. The CSN can allocate the MS IP address and other endpoint parameters, The CSN usually is the one providing the internet access for the users and the AAA proxy or server may be located in the CSN too. It should also implement the policy and admission control (allow/deny certain services) according to the subscription profiles of the users. The support for tunneling between the ASN and the CSN with the billing and inter-operator settlement may be available. Inter-CSN tunneling will allow roaming in the networks of other service providers, while inter-ASN mobility allows MS handoffs between different ASN, but within the same CSN. The CSN provides also WiMAX services such as different IP multimedia services or location services.

3.1.3 Network Reference Model (NRM)

The NRM defines operational entities and reference points over which the interoperability is achieved between network elements the previously described elements, MS, ASN, and CSN create the basis for the NRM. These are connected by reference points R1-R5. The network entities mentioned above form a group of functional entities that can be realized in a single physical functional entity or may be divided to several different physical entities. Hence, the functionalities of the ASN can be constructed within one device, or divided to several. The choice belongs to the operator, but the NWG has defined profiles A, B, and C, in order to assist in the network implementation. The network reference model is shown in Figure 3.2.

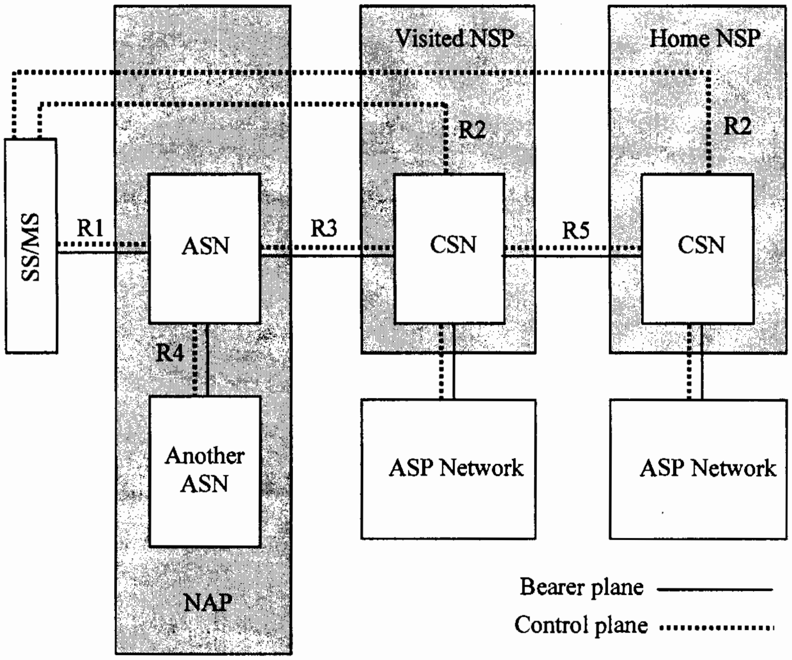


Figure 3.2 - Network Reference Model

Reference points: The reference points R1-R5 shown in Figure 3.2 are defined as follows. The R1 is indicating the protocols and procedures used between the MS and the ASN. The R2 is intended for protocols and procedures between the MS and the CSN, which is associated with authentication, authorization of services, and management of IP host configuration. Since the actual physical connection chain to CSN goes through ASN, the R2 is considered as logical link. The authentication in R2 is operated with the home NSP CSN, while the other can also be operated in the visited NSP CSN. The R3 includes the control plane protocols between the ASN and the CSN. It supports AAA, policy enforcement, and mobility management capabilities. The R4 consists of protocols used within the ASN. It can be used to allow MS mobility management between different ASNs and ASN-GWs. The R5 includes the protocols needed for communication between the visited and home CSN.

ASN Reference Model: The Figure 3.3 describes the reference model for ASN. As mentioned in the previous sub-subsection the ASN shares the R1 reference point with the MS, the R3 with the CSN, and R4 with other ASNs. The ASN must have at least one BS and one ASN-GW. The BS and ASN-GW are connected with logical links referenced as R6. The reference point R8 is intended for communication between BSs to assure fast and seamless handoffs.

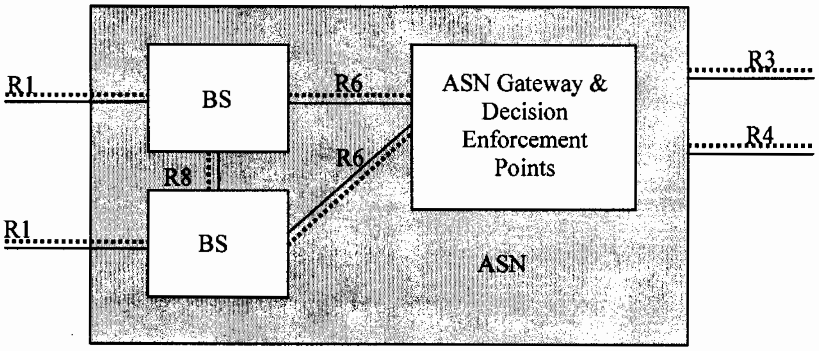


Figure: 3.3 - ASN Reference Model Containing a Single ASN-GW

The ASN-GW can optionally be decomposed to two groups of functions, the Decision Point (DP) and Enforcement Point (EP), which are connected via reference point R7, as shown in Figure 3.4.

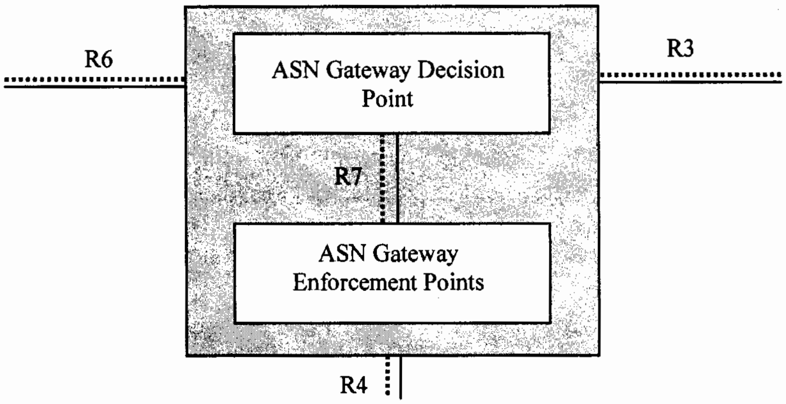


Figure: 3.4 - ASN-GW Decomposition Reference Diagram

ASN Profiles: The NWG has created three profiles for manufacturers and operators to guide them in creating a working Mobile WiMAX network. Here only basic functions are described and the more detailed view can be found at [18]. The Profile A has the handoff control at the ASN-GW. Also the Radio Resource Controller (RRC) is located at the ASNGW, which allows Radio Resource Management (RRM) with multiple BSs. The RRM can be understood as methods trying to increase reliability and efficiency of wireless transmission.

A BS contains a Radio Resource Agents (RRA) that maintains a database of radio resource indicators. Finally, the R4 and R6 physical connections are used for ASN anchored mobility within the BS. The Profile B does not make any assumptions on the physical location of different ASN entities and they can be freely distributed or grouped within the ASN. The requirement, however, is that the Profile B ASN can still communicate through R3 and R4 with other ASNs regardless of their profile types. The last, the Profile C, is similar to the profile A, but here the handoff control and the RRC are located at the BS. RRC and RRA in the BS allow RRM within that BS and the ASN-GW is equipped with an RRC relay for delivering RRM messages from BS to BS via R6.

3.1.4 Interworking with Other Technologies

Since the access network in Mobile WiMAX scenarios is based on IP, it is simple to attach other access network with different technologies to the Mobile WiMAX. The NWG specifies scenarios for 3GPP, 3GPP2, and DSL interworking with Mobile WiMAX. The intention is to combine different technologies to a working solution with common AAA servers. This way the operators with several networks can achieve financial savings since certain services can be shared.

Chapter 4

Handoff/Handover in Mobile WiMAX

Now a days, Mobile Communication become more popular as compare to landline network. The key feature is its mobility of mobile communication as the length or area covered by each cell is limited. So to keep the service continues, it is necessary to introduce Handoff/Handover strategies from one cell to another cell, Handoff/Handover is the process of changing the channel (frequency, time slot, spreading code or combination of them) associated with the current connection while a call is in process. Handoff/Handover initiated mainly due to two reasons, Fist by crossing the boundary of the cell during a cell second by decline the quality of signal strength. A special requirement for a mobile device is the ability to change the serving BS there exists another BS with, better link quality in the reach of the MS. The handoff, in some sources referred as handover, is a procedure with an intention to switch the network connection access point of the MS without data loss or disturbing the existing connections. First, for a handoff to be even possible, one needs to have at least two BSs, the currently serving and the handoff target(s), and an MS within reach of both BSs. The handoff usually is understood as a change of serving BS, but it does not necessarily mean that the BS must be changed. In some cases the handoff can occur also within the same BS, though within different channels. This handoff type is called intra-cell handoff, while the other option is called inter-cell handoff. Handoffs between different technologies are also possible. The horizontal handoff was defined to be a handoff within a single technology network, while the vertical handoff changes the network. The reasons for handoff can be various and here are listed only some of them:

- Signal strength is not enough for maintaining proper connection at the edge of the cell.
- BS capacity is full and more traffic is pending.
- Disturbing co-channel interference from neighboring cell.
- Behavior of MS changes, in a case of fast-moving MS suddenly stopping; a large cell size can be adjusted to a smaller one with better capacity.
- Faster or cheaper network is available (vertical handoffs are supported).

The handoff has roughly two major types, a hard and a soft handoff, with different variants of these depending on the used technology.

The hard handoff is performed, the connection to the serving BS is broken before creating the new connection with the target BS. With soft handoff the connection is transferred to the new BS and after successfully continuing communications the old BS can be released. The hard handoff can be very efficient regarding the channel usage, since only one channel is occupied simultaneously. This makes the equipment also cheaper because it does not have to support two or more channels in parallel. However, it can cause unrecoverable damage to the connection in case the handoff fails. The benefit of soft handoff is the reliability since the connection is broken only after finding a working connection. The drawback of soft handoffs is the required computational capacity in the equipment, which consumes money and power. The use of several channels per user decreases the overall capacity of the BS. Usually, the handoff process follows a common pattern. The BS maintains a list of neighbors that can be used in a case a served MS needing to perform handoff. The connection quality is constantly monitored and at some point the decision for a handoff is made. The criteria for the decision may be listed in handoff reasons above. Before performing handoff an appropriate candidate must be chosen and then the handoff procedure is continued based on the current application and technology. The exact procedures vary depending on used technology and usually within the technology several alternatives are available as well. In WiMAX scenarios the technology has to be 802. 16e-2005 since the 802.16-2004 does not support handoffs at all. There must be way to measure connection quality; since the transmission medium is constantly in change. To be able to perform handoffs, the technology must define a scheme for decision making to initiate them. A procedure for discovering competing BSs is also needed. The handoff should also be as fast as possible, at least fast enough to keep current IP connections alive. Data traffic is not so sensitive to larger delays but real-time voice or video (or both simultaneously) requires a swift change of the serving BS.

4.1 WiMAX Handoff Types

The 802.16e-2005 specification has a support for three handoff methods: the Hard Handoff (HHO), the Fast Base Station Switching (FBSS), and the Macro Diversity Handover (MDHO). The first one is required while the others are optional ones. The WiMAX forum [1] has been working on the HHO designing enhanced techniques to achieve handoffs (layer 2) in less than 50 milliseconds. The Table 4.1 presents the greatest difference between the traditional WiMAX and the new mobile version. As can be seen, the traditional WiMAX does not support handoffs at all.

Table 4.1 Comparison in 802.16-2004 and 802. 16e-2005

Access	Location/speed	Handoff	802.16-2004	802.16e-2005
Fixed Access	Single/Stationary	No	Yes	Yes
Nomadic Access	Multiple/Stationary	Yes	Yes	yes
Portability	Multiple/Walking Speed	Hard Hand off	No	Yes
Simple mobility	Multiple/Low Vehicular Speed	Hard Handoff	No	Yes
Full Mobility	Multiple/High Vehicular Speed	Soft Handoff	No	Yes

4.1.1 Hard Handoff (HHO)

The hard handoff is a procedure to change the serving BS using a "brake-before-make" -way, in other words the connection to the old BS is broken before a new BS is connected. This way the excess signaling traffic can be avoided during the handoff, but the time before the connection is again in normal operation can be longer. [19]

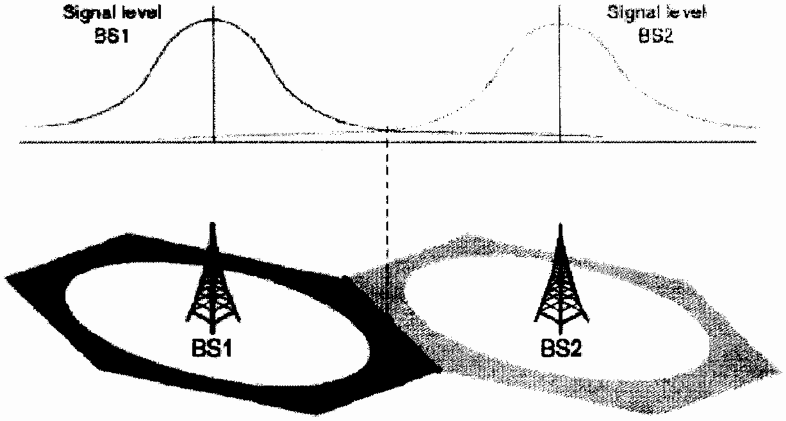


Figure: 4.1 - Hard Handoff Realizations

While connected to a BS, the MS listens to the link-layer messages in case a new BS's periodically broadcasted neighbor advertisement message (MOB_NBR-ADV) is received. These messages are used for identification of networks and distributing the properties they have. The information received can give facts about the signal quality from a neighboring BS. A better BS is not found, the MS can store the information for possible future handoffs. Figure 4.1 above demonstrates the situation a moving user reaches a point where the signal level is better with another BS. A decision criteria hysteresis needs to be included to avoid constant handoffs back and forth between BSs.

4.1.2 Macro Diversity Handover (MDHO)

The MDHO is an optional handoff scheme for the Mobile WiMAX and therefore needs to be supported by both the MS and the BS. The MS keeps a list of BSs capable to the MDHO on its coverage area show in Figure 4.2. This group is called a diversity set, or in some sources an active set. There is always one BS in the diversity set that is defined as an anchor BS. The normal functionality is a special case of MDHO there is only one BS in the diversity set. There might be also BSs that can be reached with the MS, but the signal is too weak for real traffic. These BSs are kept outside the diversity set and named as neighbor BSs. Naturally, while moving towards a neighbor BS, at some moment the signal is strong enough and the BS can be included in the diversity set, or the other way round. The measured factor is long-term CINR which is compared to the defined limits for adding/dropping a BS from the diversity set. The MS has two ways to monitor DL control information and broadcast messages. Either it listens to only the anchor BS for burst allocation information of other (non-anchor) BSs in the diversity set or it listens to all the BSs in the diversity set. While monitoring all the diversity set BSs, a DL/UL-MAP message from any BS may include information for the other BSs. The procedure of MDHO is started by the MS it decides to receive and/or transmit from multiple BSs at the same time interval. For DL traffic, two or more BSs transmit the data to the MS and the diversity combining is performed in the MS. For the UL traffic, the transmission from the MS is received by the diversity set BSs and selection diversity is performed.

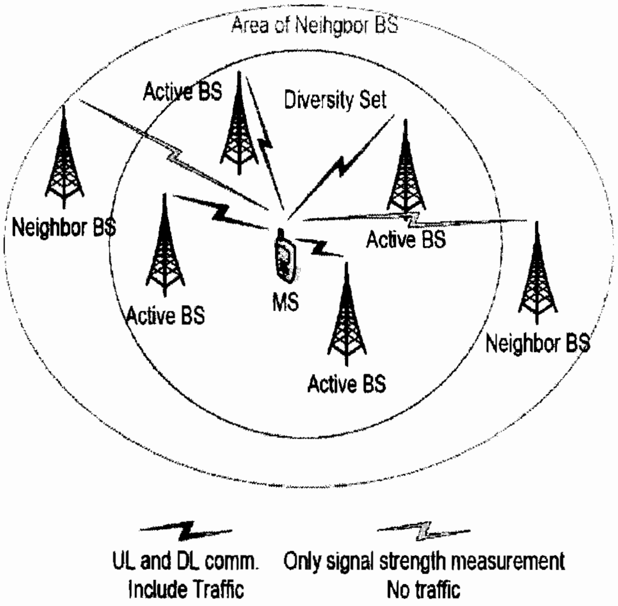


Figure: 4.2 - Macro Diversity Handover

The MDHO requires several terms to be fulfilled before it can be used. First of all, the involving BSs communicate through the RRAs at each station and they are synchronized on a common time source, since the frames sent by the BSs at a certain time frame have to be received at the MS within the prefix interval. The BSs frame structures have to be synchronized and the frequency assignment has to be the same. The same set of CIDs has to be used by all the BSs that form connections with the MS. Furthermore, all the BSs should send the same MAC/PHY PDUs to the MS. Finally, the BSs involved in MDHO must share MAC context. By MAC context is meant everything a BS and an MS usually share from encryption information to information exchanged during network entry. [2]

4.1.3 Fast Base Station Switching (FBSS)

The FBSS is based on a similar principle as the MDHO above. Again both the MS and the BSs have to support the FBSS. A diversity set is kept in the MS and the BS but the MS communicates only with one BS in the diversity set show in Figure 4.3. The currently serving BS is named as an anchor BS. In FBSS the communication, including the signaling traffic focuses on only one BS at a moment but the anchor BS can be changed for every frame separately. Naturally, the changing is possible only there are multiple BSs in the diversity set. The adding/dropping of members of the diversity set is similar to the one with MDHO above.

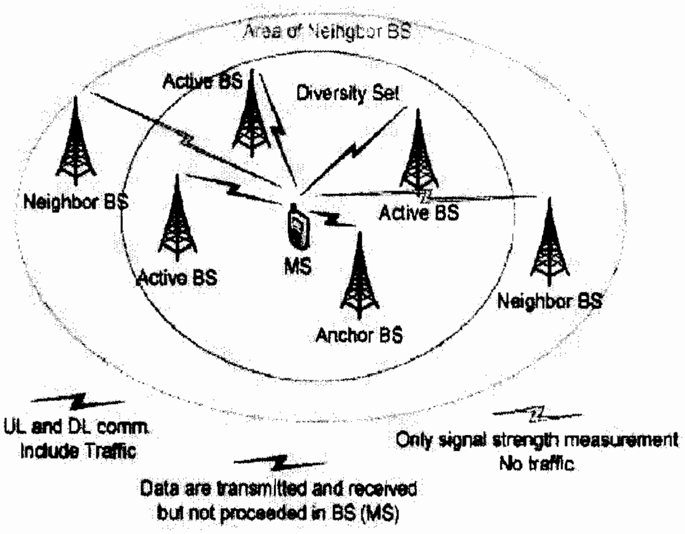


Figure: 4.3 - Fast Base Station Switching

In fact, all the BSs in the diversity set receive the data addressed to the MS, but only one of them transmits the data over the air interface while the others eventually drop the received packets. The operation of FBSS is based on the decisions of MS regarding the used (anchor) BS and these decisions are transmitted on the CQICH channel or by MS/BS initiated request message. Again, the decision of MS overrules the ones of BS. The requirements of FBSS are the same as earlier with MDHO without the demand for same set of CIDs and MAC/PHY PDUs. [2]

The HHO is best suitable for low mobility scenarios while the MDHO/FBSS can provide better performance for users moving with greater speeds. However, this does not mean that the MDHO/FBSS would be less suitable for low mobility. The HHO is an efficient method that does not require multiple channels during the handoff, unlike the two other soft handoff methods. However, in a case of failed handoff the connection can be completely broken. This can be avoided with MDHO/FBSS, which on the other hand demand more capacity in terms of bandwidth efficiency (at least two parallel channels reserved during the handoff). Complex methods require also more computing power, which again makes the equipment more expensive and tend to consume more battery power as well. The soft handoff methods can improve link quality while the MS is operating with a weak signal to the BS specially the MDHO can perform well because of several combined transmissions from different BSs. The probability that all the diversity set BSs would have an unusable signal is rather low. The FBSS cannot take advantage of several simultaneous transmissions, but it can choose the best BS on a frame-by-frame basis. For HHO the situation can be very demanding and it could be forced to handoff back and forth between two (or more) BSs.

4.2 Purpose WiMAX Handoff Method

The handoff process in Mobile WiMAX is described in the following sub-subsections. The Mobile WiMAX specification [2] defines the procedures during the handoff, but the making of handoff decision is left outside the scope of it.

Generally, the decision for a handoff can be determined based on various properties and values. As described in [20], the decision attribute is a combination of network conditions, system performance, application types, power requirements, MS conditions, user preferences, security, and cost. The network conditions and system performance can be improved by balancing the load of heavily occupied BSs to less active BSs, assuming possible within other requirements. Different applications in the mobile device can set requirements to the currently serving BS and it might be that it does not support all the needed technologies. A new BS can provide sufficient service with better power saving or security properties than the currently serving BS, it can be useful for the MS to perform a handoff to the new one. The costs and user preference can define that the network of the own service provider is used from several available networks. The MS conditions are measured constantly and, a certain level of degradation is noticed in some of the defined parameters, the handoff decision can be initiated. These parameters may include signal strength, BS coverage area, data rate, service cost, reliability, security, battery power, and network latency [20]. In Figure 4.4, a combination of network entry and handoff processes is presented. It can be seen that the two procedures are very similar to each other.

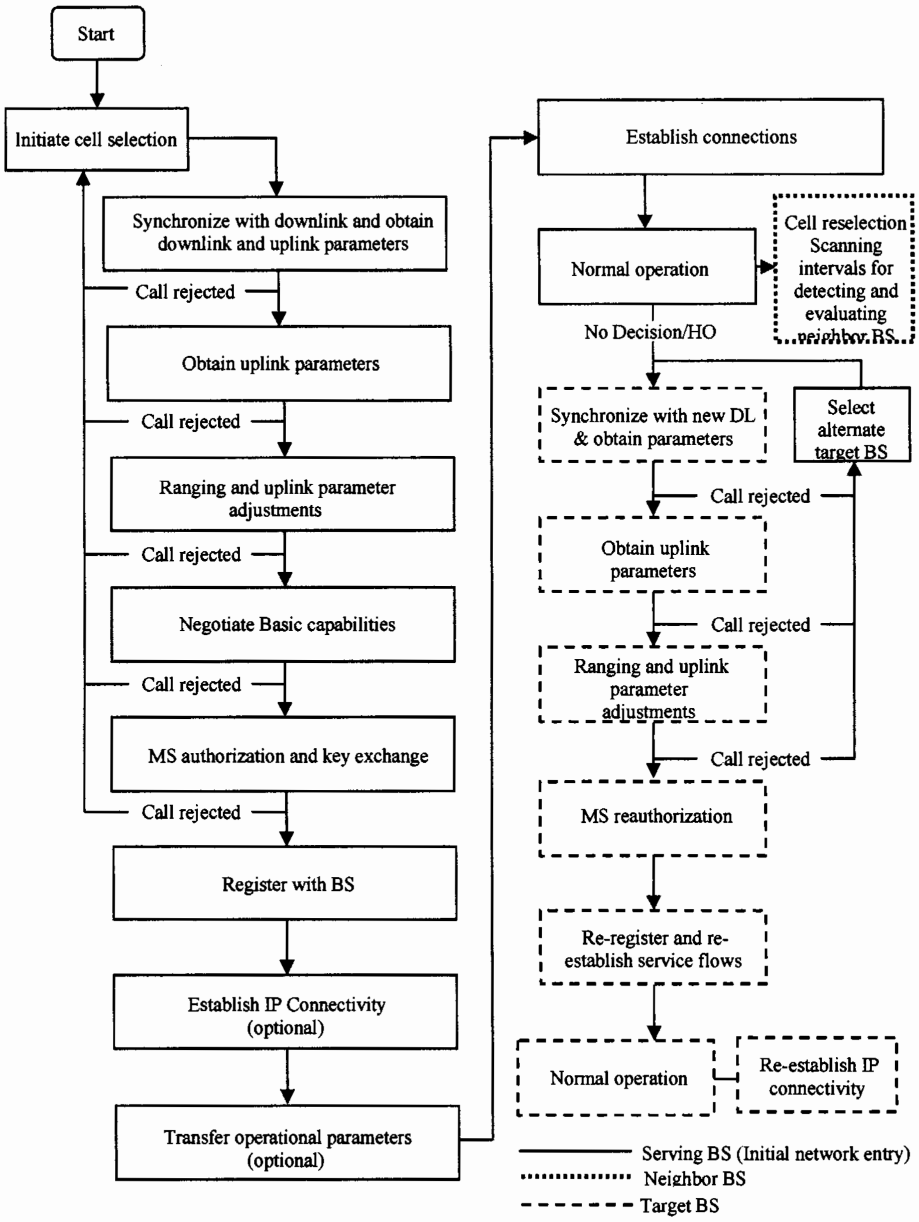

Start
Initiate cell selection
Synchronize with downlink and obtain downlink and uplink parameters
Call rejected
Obtain uplink parameters
Call rejected
Ranging and uplink parameter adjustments
Call rejected
Negotiate Basic capabilities
Call rejected
MS authorization and key exchange
Call rejected
Register with BS
Establish IP Connectivity (optional)
Transfer operational parameters (optional)
Establish connections
Normal operation
Cell reselection Scanning intervals for detecting and evaluating neighbor BS
No Decision/HO
Synchronize with new DL & obtain parameters
Select alternate target BS
Call rejected
Obtain uplink parameters
Call rejected
Ranging and uplink parameter adjustments
Call rejected
MS reauthorization
Re-register and re-establish service flows
Normal operation
Re-establish IP connectivity
Serving BS (Initial network entry)
Neighbor BS
Target BS

Figure: 4.4 - Network Entry and Handoff

4.2.1 Reselection of Cell

The cell reselection is a process with intention to find a potential BS for handoff. The MS has several possibilities to use while evaluating the possible change of the serving BS. It can exploit the information in neighbor advertisement messages (MOB_NBR-ADV). The MOB_NBRADV message is sent periodically by the BS and the intention is to identify the network and to give the MS information about neighbor B S(s) for possible handoff or initial network entry. The BS stores the MAC addresses and indexes of neighbor BS as mapping tables and transmits them in the MOB_NBR-ADV message. The message includes also several other fields and is described in greater detail in [2]. The MS can send a request for scanning interval or sleep-intervals to be used for scanning and/or ranging the neighboring BS. This process is just a survey about handoff alternatives and the connection is not yet broken with the serving BS. The Figure 4.5 describes the performed procedures during cell selection, including ranging. The process begins with synchronization to the first BS and DL/UL parameters (DL and UL-MAP, DCD, and UCD messages) are acquired. The air interface parameters are received the channel measurements can be launched by sending a ranging request message (RNG-REQ). The BS responds with a ranging response message (RNGRSP). The messaging during the handoff is shown in Figure 4.6, as a case of MS initiated handoff. Shortly described, the process begins with a MOB_MSHO-REQ message sent by the MS to the serving BS. The BS gathers information about neighboring BSs and informs MS with MOB_HO-RSP. The MS confirms the target BS and initiates the actual process of handoff with MOB_HO-IND sent to the serving BS. Then the MS synchronizes with the target BS and retrieves the basic connection parameters (DL_MAP, UL-MAP, DCD, and UCD messages). After successfully resolving the mentioned messages, the MS requests ranging (RNG-REQ) and target BS responds with RNG-RSP. With successful response the network re-entry is performed and the old serving BS released.

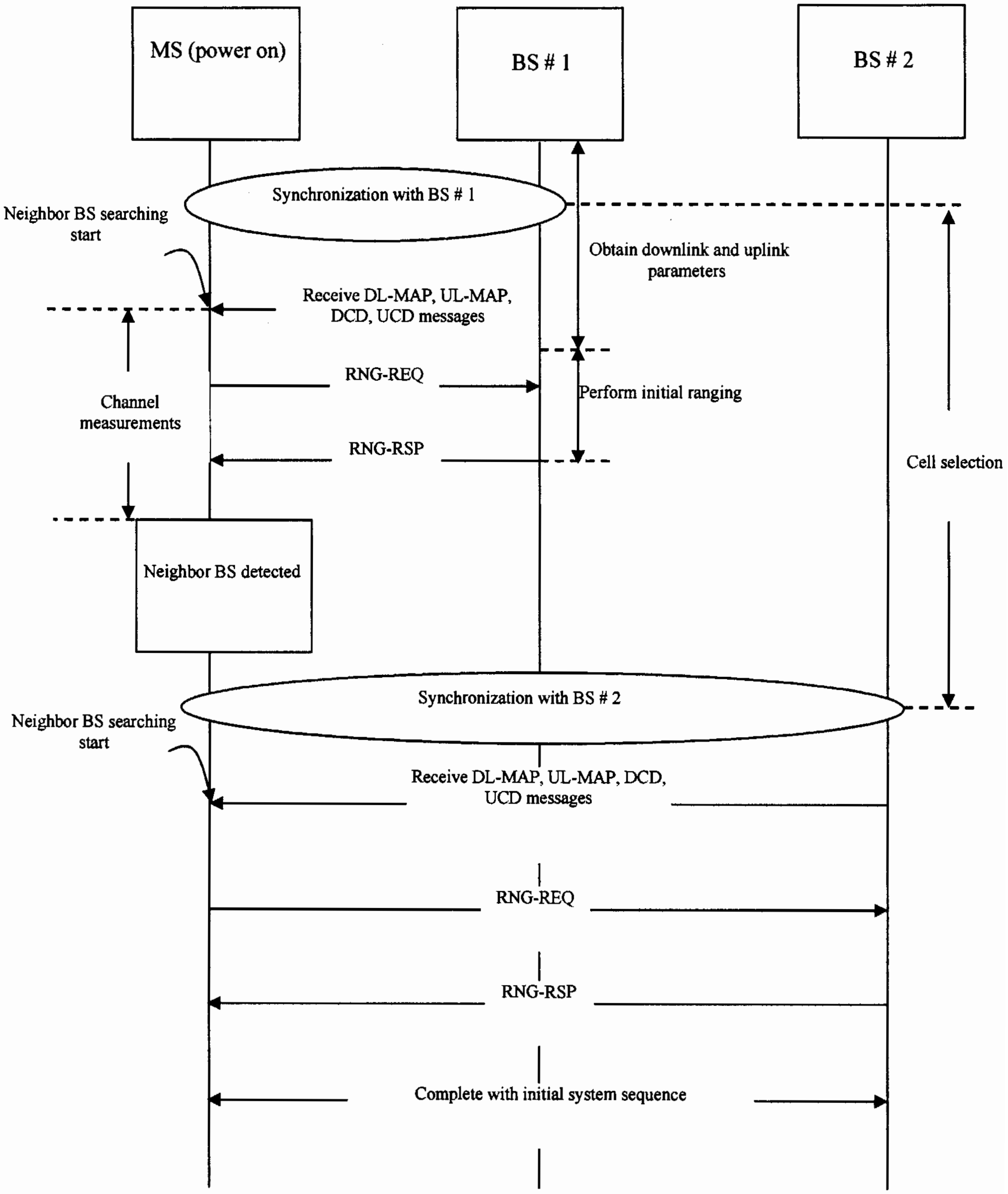

MS (power on)
BS # 1
BS # 2
Synchronization with BS # 1
Neighbor BS searching start
Obtain downlink and uplink parameters
Receive DL-MAP, UL-MAP, DCD, UCD messages
RNG-REQ
Perform initial ranging
Channel measurements
RNG-RSP
Cell selection
Neighbor BS detected
Synchronization with BS # 2
Neighbor BS searching start
Receive DL-MAP, UL-MAP, DCD, UCD messages
RNG-REQ
RNG-RSP
Complete with initial system sequence

Figure: 4.5 - Cell Selection with Ranging

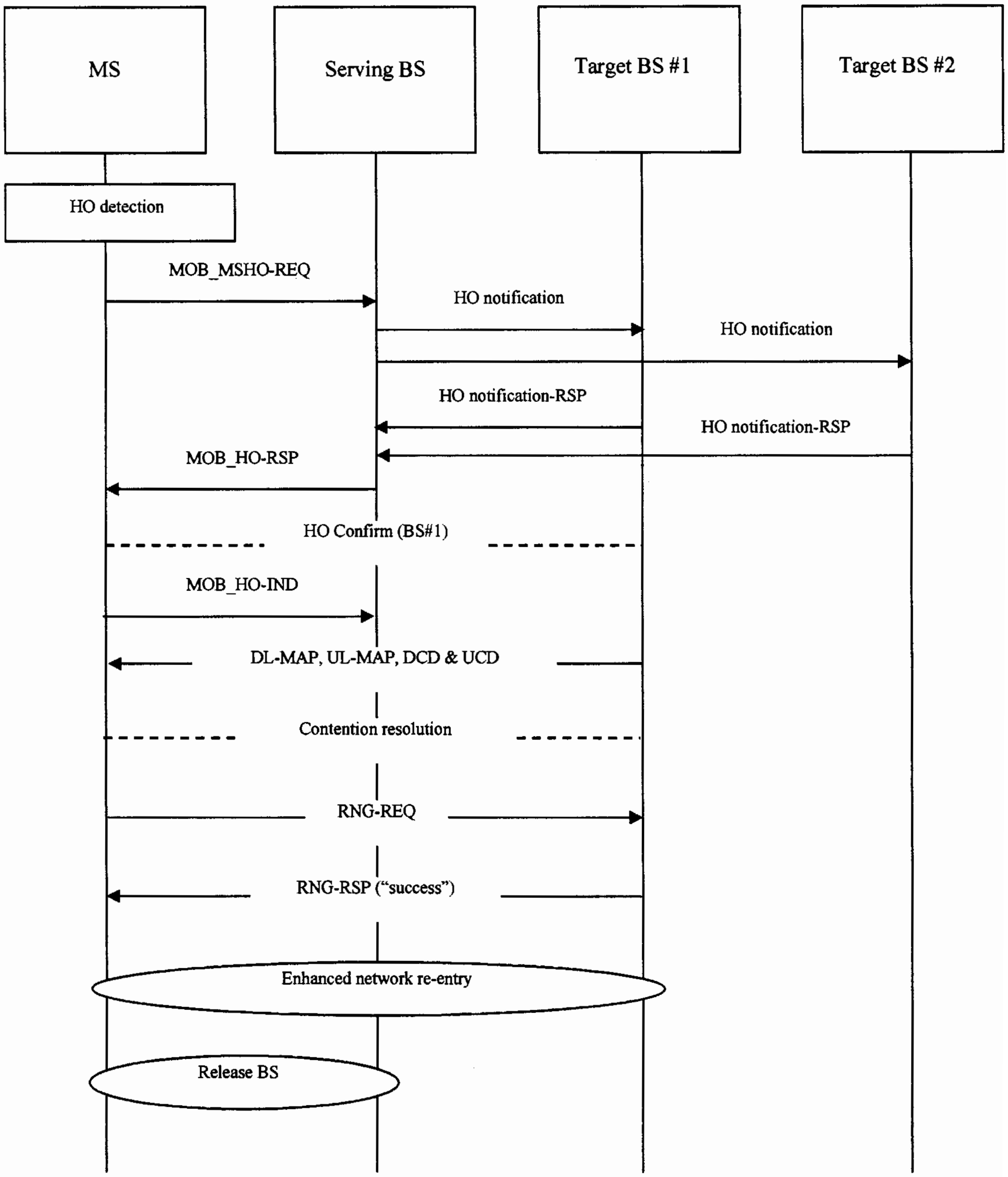


Figure: 4.6 - Messaging during a MS Initiated Handoff

4.2.2 Initiating and Deciding the Handoff

The actual handoff begins a decision is made that the MS changes the serving BS. The decision can be made at the MS, the BS, or on the network. The following step is sending a notification message, not obligatory but recommended, by either the MS (MOB_MSHOREQ) or the BS (MOB_BSHO-REQ). The notification message is sent; a response (MOB_MSHO-RSP or MOB_MSHO-RSP) is required. In a case both send notification messages, the one sent by the MS has a priority over the one sent by the BS. Both notifications may include one or more possible target BS, which have been scanned earlier. There is also a possibility for the serving BS to communicate through the backbone with the possible target BS. The serving BS has only a possibility to force the MS to handoff, not to define the target BS. The MS can choose or neglect recommended options for the target BS without restrictions. The and off decision is confirmed with a MOB_HOIND message. The MOB_HO-IND is sent by the MS and it tells the BS whether the MS is really proceeding with the handoff or not. The message can include also other information related to BS selection:

- 0b00: HO (serving BS release, HO cancel, or HO reject)
- 0b01: MDHO/FBSS anchor update (confirm, cancel, or reject)
- 0b10:MDHO/FBSS diversity set update (confirm, cancel, or reject)
- 0b 11: Reserved

4.2.3 Synchronizing the Target BS

After the handoff is initialized the MS synchronizes with target BS DL and UL transmissions by obtaining the required parameters. The MS has received a neighbor advertisement earlier; the synchronization procedure can be faster. The advertisement needs to include target BS Identity (BSID), physical frequency, DCD, and UCD. A handoff notification was sent by the serving BS and received by the target BS (via backbone connection), non-contention-based initial ranging opportunities can be assigned.

4.2.4 Range

After the synchronization of the DL/UL parameters the MS starts the ranging phase. The two possibilities available are initial or handoff ranging. The ranging is a phase that consists of several processes between the MS and the target BS in order to communicate the properties of the transmission link.

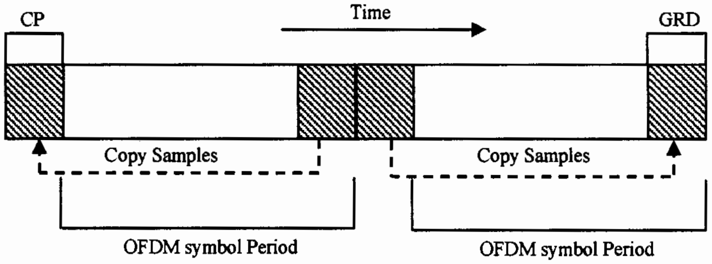


Figure 4.7 - Handoff Ranging Transmission for OFDMA

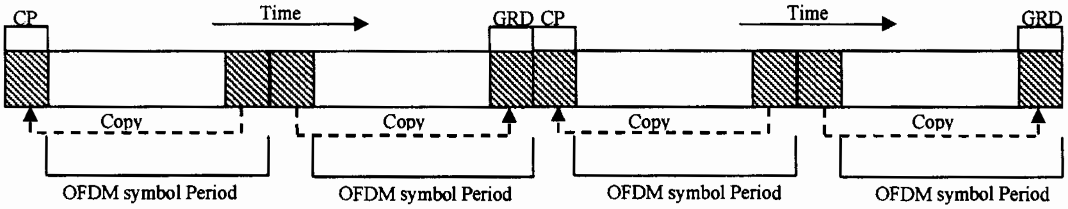


Figure: 4.8 - Handoff Ranging Transmission for OFDMA (using two consecutive initial ranging codes) [2]

Figures 4.7 and 4.8 show the structure of ranging code to be used during initial or handoff ranging, with single and two consecutive ranging codes. Periodic ranging and bandwidth requests, used during normal operation, use similar structure, but they last only for one or two OFDM symbol periods while initial/handoff ranging has the codes in pairs two or four periods. The initial ranging begins by the MS choosing a ranging slot for a ranging code (using CDMA) to be sent to the target BS. The ranging codes are created as Pseudo-Random Binary Sequences (PRBS) with the generator described show in Figure 4.9, which is implementing the polynomial 1 + x^1 + x^4 + x^7 + x^{15} The seed used is b14...b0 = 0,0,1,0,1,0,1,1,s0,s1,s2, s3,s4,s5,s6, where s6 is the LSB of the seed and s0. ..s6 = UL_PermBase (an integer value of 7 LSBs of the Permutation Base parameter transmitted within the UCD) with s6 as the MSB of it.

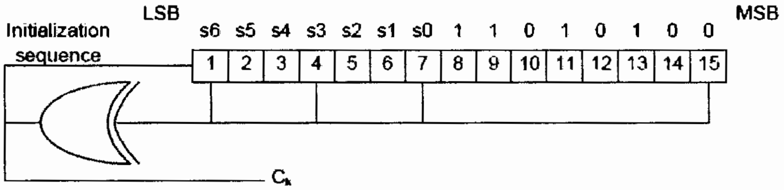


Figure 4.9 - PRBS Generator for Ranging Code Generation

As a reaction to the MS ranging the BS broadcasts a ranging response message marked with the sent slot and code for the MS to identify the correct response. The response is broadcast since the BS cannot know which MS sent the ranging code. The response message includes also all the needed adjustments (such as power, time, or frequency corrections) with status notification. The status is "continue"; the MS will repeat sending the ranging code, generated according to the description above. With "success" status the BS allocates bandwidth for the MS and the ranging is over. The difference with handoff ranging is that the sent CDMA code is selected from a special handoff-ranging domain. The target BS is informed in advance about the coming handoff; it can directly allocate the needed bandwidth. Another possibility for shortening the handoff duration is to use target BS information acquired earlier during scanning interval. This information can decrease the amount of needed RNG-REQ/RSP interactions, but it has to be recent enough to qualify accurate.

4.2.5 Re-entry of Network

The network re-entry is performed in a similar way as the initial network entry, a MS is turned on. The process of re-entry during handoff can, however, be enhanced and therefore made faster. Figure 3.8 (initial network entry and handoff) already described the phases of network (reentry) and the handoff process so far has included the ranging phase. The next step is to negotiate the basic capabilities regarding modulation/demodulation. The reauthorization of MS and key exchange is performed and the MS registers with the target BS, which is intended for agreement of ARQ or CRC capabilities. Now, the MS has re-entered the network of the target BS and the service flows can be reestablished with proceeding to the normal operation. Finally, the old serving BS can be released. The target BS can acquire information from the serving BS via backbone connect ion, or even from other network entities. With this information, the basic capabilities negotiation, registration, privacy key management, authentication and/or encryption key establishment phases can be skipped for enhancement of the network re-entry and therefore the entire handoff process. [2] [6]

4.2.6 Cancellation of Handoff

The MS can cancel the handoff process anytime after the sending of MOB_MSHO/BSHO_REQ message, as long as the above mentioned Resource_Retain_Timer has not expired. The cancellation is done by sending a message (MOB_HO-IND) containing a handoff cancels option.

4.2.7 MS Context Termination

After the handshake with the target BS is completed the connection to the serving BS has to be broken. The termination message (MOB_HO-IND) with a code indicating BS release is sent to the serving BS. Upon receiving the message, the serving BS starts a Resource_Retain_Timer. This timer defines all context (information in queues, counters, timers, etc.) related to the MS is retained. However, in a case the target BS sends a backbone message of successful MS network attachment with it, the timer can be bypassed and the MAC context and PDUs related to the MS removed from the old serving BS.

4.2.8 Dropping of Call during Handoff

There can be a situation during the handoff process the MS has stopped communicating with the serving BS before the normal cell selection or termination of MS context have been completed. This situation is called a drop and the MS can detect it by failed demodulation of DL, or by exceeding the limit for consecutive RNG-REQ re-tries. On the other hand, the BS can notice a drop the limit for inviting ranging request messages is exceeded. The MS detects a drop while trying to establish a connection with a target BS; it can attempt network re-entry with its preferred target BS as through cell reselection. It can resume communicating with the serving BS by sending a handoff cancellation message.

Chapter 5

Simulations and Results

In dissertation, my goal is to achieve handoff during moving object in WiMAX and to test the properties of Mobile WiMAX in practice. I used Network Simulator [21] (version 2.29 with additional WiMAX and Mobility packets from a NIST project [22]).The main issue is handoffs between BSs; they are demonstrating the HHO method. The add-on description [23] defines as the main supported features the PHY layer of Wireless MANOFDM with only TDD, messages for network entry management without support for authentication, 802.16e-2005 extensions for scanning, handoff, fragmentation and reassembly of frames.

The circumstances consisted of three BSs evenly aligned on a line in a way that the coverage areas of two neighboring BSs had some overlap. Certain constant values like the cell size, the transmit power of BSs, the route of MS, were selected for the simulation and the handoff times were tried to make faster by adjusting the properties of the WiMAX module in the NS-2. In conclusion, the tests were also run with speeds 1-40 m/s (3.6-144 km/h) with 1 m/s steps. The assumed traffic was constant bit rate with data rate of 1.2 Mbit/s.

5.1 Scenario

The all-in-one package of the NS-2 did not include support for Mobile WiMAX and therefore additional components were required. In WiMAX and the Mobility module, from NIST were mount to achieve model of mobile set-up. In the modules was very similar to the designed simulation scheme. The essential idea is shown in

Figure 5.1. There is a MS traveling through the coverage areas of three 802.16e-2005 BSs (BS0, BS1, and BS2).

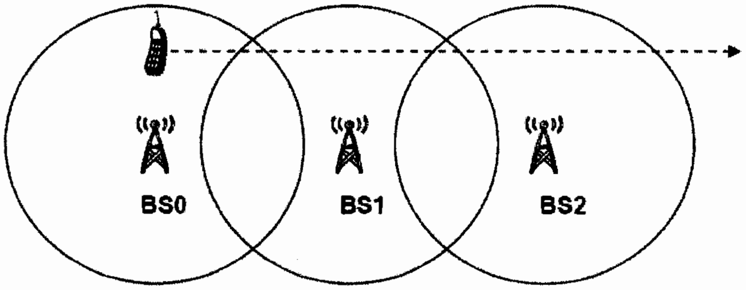


Figure 5.1 - Simulation Scenario

The BSs are aligned on a straight line so that they have 750 meters between each other and their coverage areas have a radius of 500m. At the start of the simulation the distance between the MS and the BS0 is 310 meters. The MS begins moving, as shown in Figure 5.1, while keeping the shortest distance to the BS in mentioned 310 meters. This value was selected in random and, naturally, it could be anything else too. However, the MS has to be in the reach of the BS coverage. The reasonable maximum distance is the crossing point of the edges of the cells, approximately 330 meters from the center line.

5.2 Components

The simulation scenario was based on the Mobility and WiMAX packets from NIST, especially the Neighbor Discovery (ND) and Media Independent Handover (MIH) modules were the key elements used in the simulation.

5.2.1 Neighbor Discovery –module

The Neighbor Discovery (ND) module is designed to provide movement detection for layer 3. Its assignment is to create IP addresses a network is changed. The module is a part of the MIH packet is intended to support multiple interface types, such as Ethernet, WLAN, UMTS, and, in this case, Mobile WiMAX. The ND agent uses broadcast or uni-cast messages according the technology in use. The ND agent is located in all nodes, but the configuration in NS-2 has to be done according the type of the node in the network. Ethernet or UMTS networks do not have a capability to send broadcast messages in NS-2 whereas WLAN has. The ND agent can be configured to send uni-cast messages according a pre-configured list of targets. The functionality of the ND agent depends on the role of the node in the network, in other words, whether the node is a router or a host. The router functionality consists of sending unwanted Router Advertisements (RA) periodically to the hosts. In case a router receives a Router unwanted messages from a host, it sends an RA, assuming the time from previous sending is between the values of parameters. A router receives an RA, it is discarded. The hosts can ask for an RA with router surplus messages. RA is received the included prefix information is compared to the existing tables and possibly new values are added. An expiration timer is attached to an RA message; Dump the prefix information in case a new one is not received. [24], [25]

5.2.2 Media Independent Handover –module

The Media Independent Handover (MIH) module was developed to control handoffs with various technologies. The functionality is based on MIH Function (MIHF). It works on layer 3 and can communicate between local and remote interfaces. The remote interfaces can be contacted via another MIHF. This is show in Figure 5.2.

5.3 Parameters

The aim with simulations was to find parameters that affect the most in the handoff performance. The values measured were the number of sent, received, and dropped packets with times for both handoffs. The time of handoff was determined to be the time difference between the last received packet from the old BS and the first received packet from the new BS. The two handoffs had never exactly the same length in time and usually the difference varied from a few milliseconds to a few tens of milliseconds.

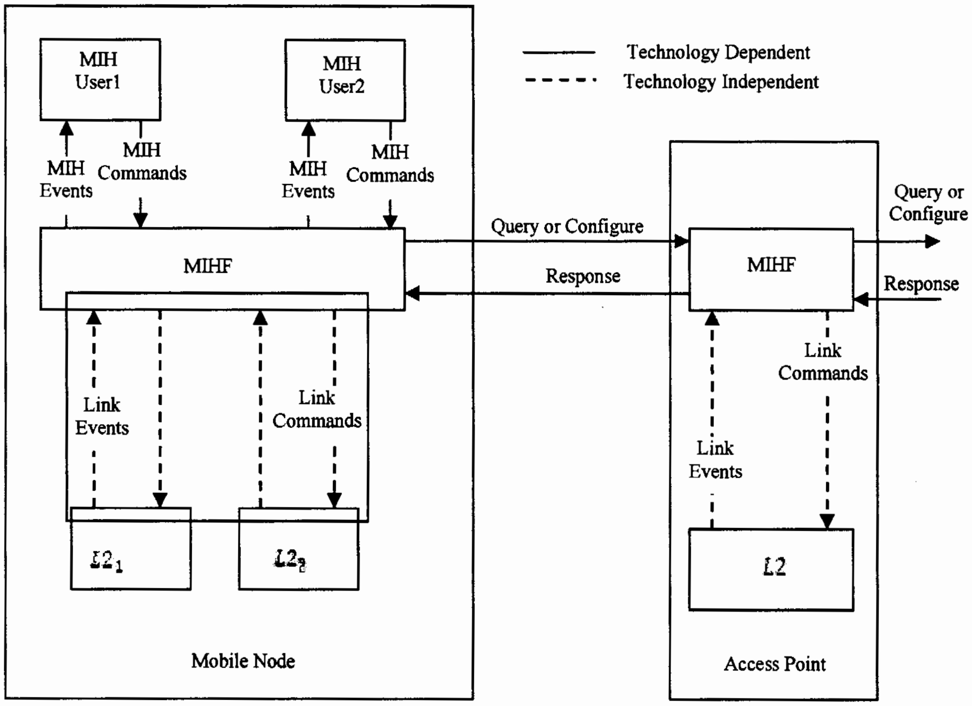


Figure: 5.2 - MIH Design Overview

5.3.1 Constant Parameters

Various parameters were set as constant in order to keep the simulation simple. The BS coverage area and transmit power as well as operating frequency were unchanged, and they were the same for all three BSs. The velocity was kept in 10 m/s and only after all the adjustments different speeds were tried. With lower speeds the length of simulation time had to be adjusted to allow two handoffs. The topology of simulation was the same for all simulations. This included the locations of BSs and the route of the MS. The data was sent with constant bit rate so that the packet size was 1500 bytes and a packet was sent with 10 ms interval. These result in the data rate of 1.2 Mbit/s, which is rather moderate compared to the announced theoretical maximum rates (Table 2.6). However, the selected rate is already nearly sufficient to provide a MPEG-1 video stream, which needs a data rate up to 1.5 Mbit/s, [26].

5.3.2 Adjusted Parameters

Since the results of simulator was deterministic with the unchanged parameters, it was enough to run the simulation only once per change of a parameter. Certain preset values from file were used as a basis and were changed while trying to find the shortest handoff times. A parameter is not separately defined in the code; they use default values described in the WiMAX module files. The adjustments displayed that some of the parameters did not have an influence at all to the handoff latency, but there were others that had an impact on the latency. The Link Going Down -factor was one of the parameters with rather significant influence. It determined the detection sensitivity of a failing link. It was important to detect the link failure, on one hand, early enough before the connection is broken, or on the other hand, late enough, to avoid unnecessary handoffs. Several timer and timeout parameters had also their impact on the handoff latency. This was quite understandable since they usually define some time to wait before some function is performed. The function is somehow related to the handoff process, it can delay the process even significantly. The adjustment of parameters was completed; the amount of sent packets during one simulation was also received. These are the combined values of all three BSs. The reported packet drop was five packets. This was explained by examining the simulation data, which showed, that the first drop comes already before any packets are sent. The timestamp of the first drop was at 24.14ms, while the first data packet was sent at 38.23ms and received at 39.16ms.

Another interesting point was found out, the time difference between transmission and reception time stamps were compared. The MS communicated with the first BS, the difference was just below 1ms, while with the second BS it is already 21ms and with the last BS it doubled to 41ms. It seemed that the simulator is circulating the packets through the first BS although each BS is defined to have direct link of their own to the presumed access network. Nevertheless, the handoff times were not influenced by this. With the adjusted parameters the handoff times were 32.06ms for the first handoff and 33.75ms for the second one. During the adjustments, either handoff latency value was occasionally even below 30 ms, but in such cases the other was significantly larger. There might be even better values for the parameters, since some of them had a rather unpredictable influence on the handoff times. As mentioned earlier, the main goal was to find the parameters that are the most sensitive in influencing the handoff duration.

5.4 Velocity of MS

The adjustments of NS-2 and WiMAX-module parameters were performed; the influence of velocity of the MS was also investigated. In the previous section the speed of the MS was set to constant 10 m/s (36 km/h). In these simulations the simulation parameters were untouched and only the speed of the MS was changed. The simulations were done with MS speeds between 1 and 40 m/s with 1 m/s step. The 40 m/s equals to 144 km/h. For the slowest speeds the overall length of the simulation time had to be increased in order to allow two handoffs. Higher speeds 50, 60, 75, and 100 m/s were also simulated. The handoff times varied in the region of 40 ms and stayed nicely below the 50 ms limit until the MS reached the velocity of 20 m/s, apart from few exceptions that exceeded the limit by only few milliseconds. After this, the times show a more or less steady growth up to 150 ms region with the 40 m/s MS speed. The handoff times (for 1-40 m/s) are drawn in Figures 5.3 and 5.4 below. The higher speeds (50, 60, 75, and 100 m/s) showed also a steady increase while the velocity grew. The handoff time with 100 m/s, according to the simulations, was just below 0.2 seconds. The simulator seemed to handle the speed and there were no traffic problems between the MS and the BS, but in real life the situation would hardly be the same, or even possible to achieve.

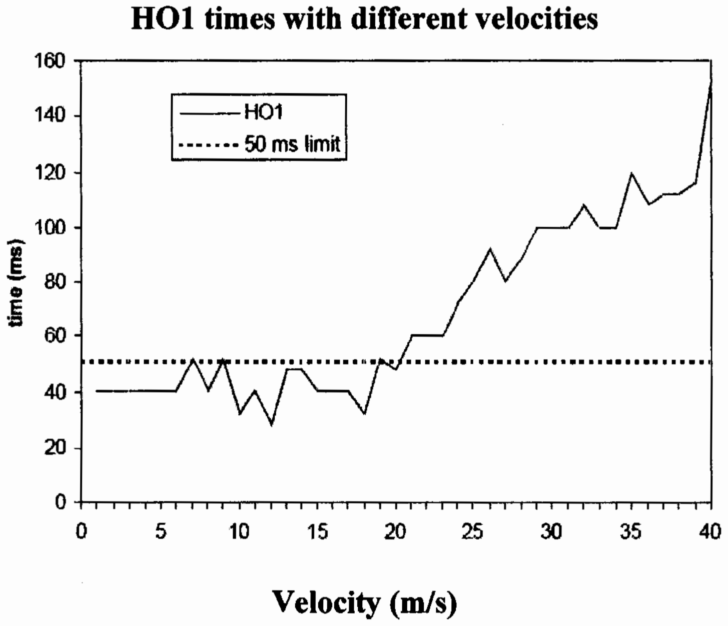


Figure 5.3 - Handoff Times for the First Handoff

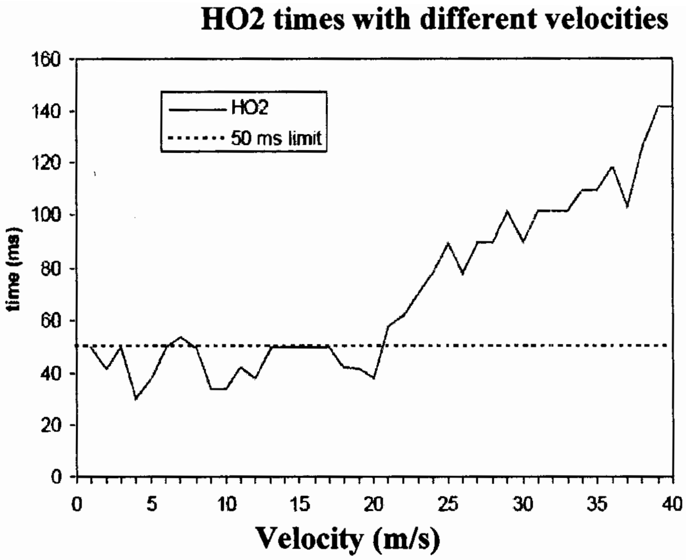


Figure 5.4 - Handoff Times for the Second Handoff

5.5 Signal Strength

The decision is based on an average measurement of the received signal. In Figure 5.5, the handoff would occur at 20m/s. The effect of the threshold depends on its relative value as compared to the signal strengths of the two BSs at the point at which they are equal. The MS hand off only the current signal is suitably weak (less than threshold) and the other is the stronger of the two. The threshold is higher than this value, 80dbm as shown in Figure 5.5, the handoff occurs at 20m/s. The threshold is lower than this value 58dbm as show in Figure 5.5; the MS would delay handoff until the current signal level crosses the threshold at 23m/s. In the case of 38dbm, the delay may be so long that the MS drifts also far into the new cell. This reduces the value of the communication link from BS_1 and may result in a dropped call. In addition, this results in additional interference to co-channel users. Create overlapping cell coverage areas. A threshold is not used alone in actual practice because its effectiveness depends on previous knowledge of the crossover signal strength between the current and candidate BSs. This system allows a user to hand off only the new BS is stronger (by a Hysteresis margin, h in Figure 5.5) than the current one. The handoff would occur at 25.5m/s. This technique prevents the so-called ping-pong effect, the repeated handoff between two BSs caused by rapid fluctuations in the received signal strengths from both BSs. The first handoff, however, may be unnecessary the serving BS is sufficiently strong. This scheme handovers a MS over to a new BS only the current signal level drops below a threshold and the target BS is stronger than the current one by a given hysteresis margin. In Figure 5.5, the handoff would occur at 25.5m/s. the threshold is 38dbm.

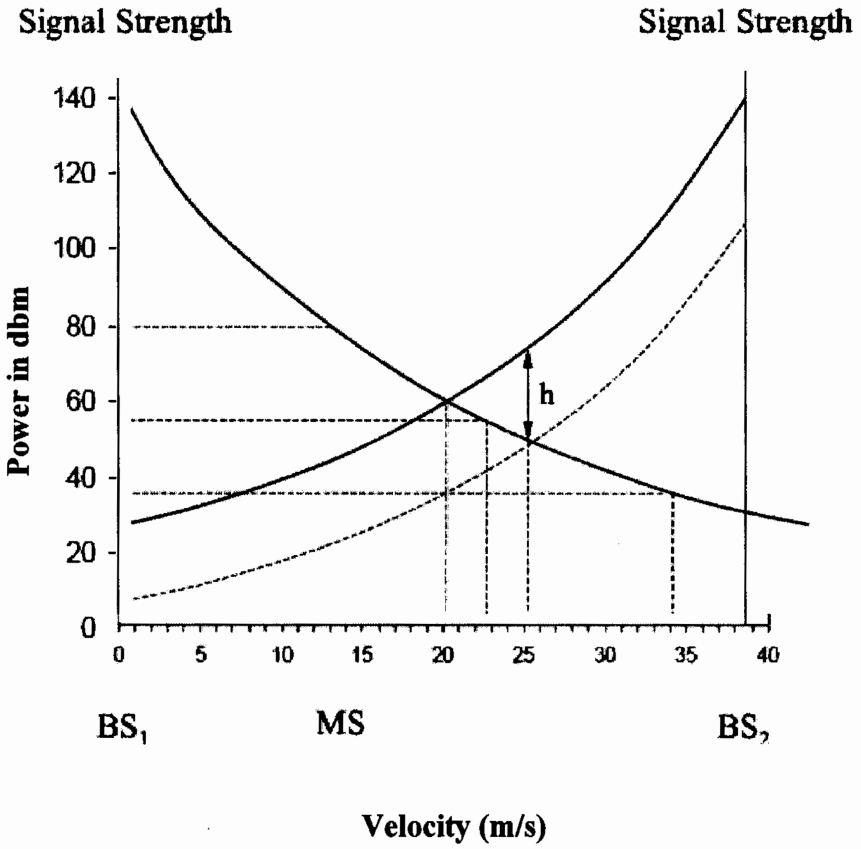


Figure 5.5 - Signal Strength between two Adjacent BSs Handoff.

5.6 Cell Size

The first step in designing a wireless system is to develop a link budget. Link budget is the loss and gain sum of signal strength as it travels through different paths between transmitter and receiver. The link budget determines the maximum cell radius of each base station for a given level of reliability and is comprised of two types of components: system related components and non-system related components. These components are important factors measuring the complexity and speed in deploying at higher frequency bands. Other factors like interference from other surrounding networks will also impact network performance and quality of service. The physical surroundings of a cell site play a very important role in determining the cell coverage area. A cell site coverage area can decrease from 7km in a mostly flat area with light tree densities to 3 km in hilly areas. RF planning remains the fundamental limiting factor in system performance in WiMAX. The cell size for several carrier frequencies from 450MHz to 3.5GHz is estimated for WiMAX systems using path loss propagation models for flat rural, hilly rural and urban environment. The simulation results to obtain the same cell radius of 3km with 2.5 GHz frequency band a 4dbm link budget are needed. WiMAX systems operate at 450MHz frequency, due to large cell size. The radio improvement characteristic valid to fixed and mobile WiMAX is sub-channelization. The improvement features that are only valid to mobile WiMAX are convolutional turbo coding, repetition coding (3dbm gain), and Hybrid Automatic Repeat Request (HARQ). Applying smart antennas or MIMO configuration in the different topologies will enhance the cell site coverage area. Cell preparation option and WiMAX technology features also allow interference and noise handling so that WiMAX can provide sufficient coverage. The cell size depends upon using the frequency of system. By making the cell size small, the soft handoff increases and our some information is loosed. The greater advantage of making cell size small is that the transmitting power saves and receiving data rate is high and our MSC will be burdened and the load on the network increases. On the other hand, the cell size is large there will be decreased number of handoffs but transmitting power is consuming high. Receiving data rate is low and load on the network is minimized.

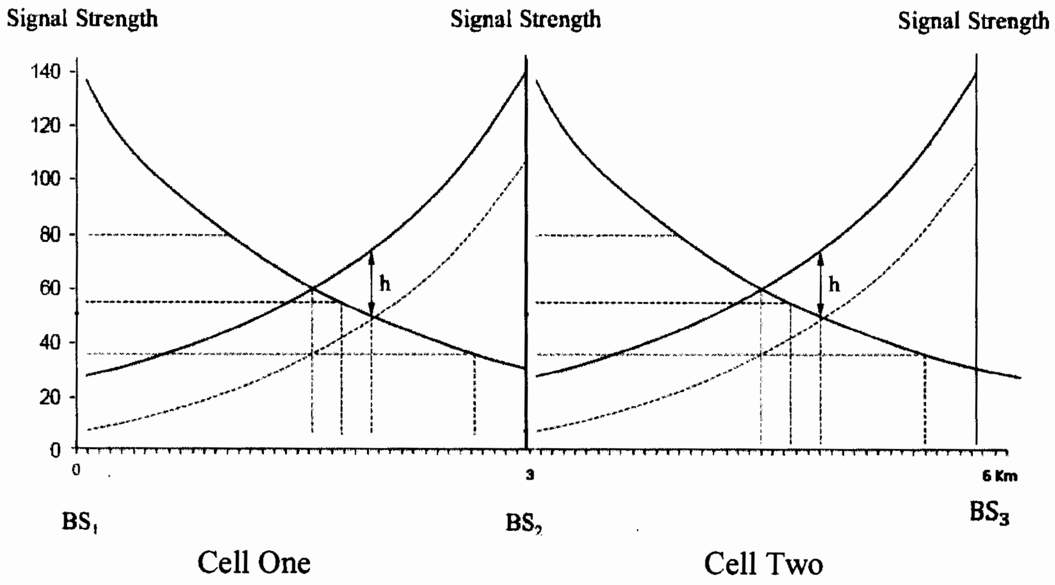


Figure 5.6 -Handoff between three adjacent BSs due to small cell size

REFERENCES

[1] WiMAX Forum, "Fixed, Nomadic, Portable and Mobile Applications for 802.16-2004 and 802.16e WiMAX Networks", November 2005.

[2] LAN/MAN Standards Committee, "IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," IEEE STD 802.16e-2005—Approved 7th December 2005.

[3] LAN/MAN Standards Committee, "IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Broadband Wireless Access Systems," IEEE STD 802.16-2004—Approved 1st October 2004.

[4] WiMAX Forum, "Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation," vol. 2.8, August 2006.

[5] J. H. Stott, "The how and why of COFDM (Coded Orthogonal Frequency Division Multiplexing) EBU Technical Review," 1998.

[6] Qualcomm, "Mobile WiMAX: Hype and Realities".

[8] J. Shandle, "All about OFDMA," 5th June 2008.

[9] J. Andrews, A. Ghosh, and R. Muhammad, "Nuts and Bolts of WiMAX - Parts I-VIII," 2nd April 2008.

[10] H. Yaghoobi, "Scalable OFDMA Physical Layer in IEEE 802.16 Wireless MAN," Intel Technology Journal, vol. 8, no. 3, 2004.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Network Working Group, "Extensible Authentication Protocol (EAP)," RFC3748. June 2004.

[12] R. Housley, W. Polk, W. Ford, and D. Solo, Network Working Group, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC3280," April 2002.

[13] RSA Laboratories, "RSA Cryptography Standard," PKCS #1 vol. 2.1, 14th June 2002.

[14] T. Shon and W. Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Vol. 4658, pp. 88-97, 24th August 2007.

[15] S. McCann and D. Stephenson, IEEE 802.11u Task Group, "Interworking with External Networks," January 2008.

[16] S. Churchill, IEEE 802.11p Task Group, "Intelligent Transportation Gets 802.11p," July 2004.

[17] H. Zheng, S. Maheshwari, Y. Saifullah, A. Boariu, IEEE 802.16 Broadband Wireless Access Working Group "Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points)," Part I, 14th January 2008.

[18] H. Zheng, S. Maheshwari, Y. Saifullah, A. Boariu, IEEE 802.16 Broadband Wireless Access Working Group "Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points)," Part II, 14th January 2008.

[19] Conniq.com, "Handoff mechanism in Mobile WiMAX", 2005-2008.

[20] Y. Nkansah-Gyekye and J. Agbinya, "Vertical Handoff Decision Algorithm for UMTS-WLAN," Vol. 27, no.30, pp. 37, August. 2007

[21] K. Fall and K. Varadhan, the VINT Project, "The Network Simulator - NS-2.29", 2007.

[22] The Project of National Institute of Standards and Technology (NIST), "Seamless and Secure Mobility", January 2007.

[23] R. Rouil, "The Network Simulator NS-2 NIST add-on - IEEE 802.16 model (MAC+PHY)", July 2007.

[24] NIST, “The Network Simulator NS-2 NIST add-on - IEEE 802.21 model (base on P802.21/D03.00)”, January 2007.

[25] NIST, the Network Simulator NS-2 NIST add-on – “Neighbor Discover”, January 2007.

[26] L. Chiariglione, International Organization for Standardization, “Short MPEG-1 description. Parts I-V”.