國立交通大學

資訊科學與工程研究所

碩士論文

IEEE 802.16e 基本的換手機制仿真器

An Implementation of IEEE 802.16e General Handover Emulator

研 究 生：陳思敏

指導教授：簡榮宏　教授

中華民國　九十五　年六月

IEEE 802.16e 基本的換手機制仿真器
An Implementation of IEEE 802.16e General Handover Emulator

研 究 生：陳思敏　　Student：Szu-Min Chen

指導教授：簡榮宏　　Advisor：Rong-Hong Jan

國 立 交 通 大 學

資 訊 科 學 與 工 程 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Computer Science and Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年六月

IEEE 802.16e 基本的換手機制仿真器

研究生：陳思敏　　指導教授：簡榮宏 博士

國立交通大學資訊科學與工程研究所

摘　要

近年來無線網路相關技術迅速發展普及，無線網路涵蓋範圍從數公尺一直擴充到英哩。目前最新提出的 WiMAX 技術宣稱能提供每秒 75 Mbits 頻寬，並擁有 31 英哩的涵蓋範圍，其中 IEEE 802.16e 為具有行動技術之最新標準。本篇論文根據最新的標準實作 IEEE 802.16e 基本換手機制仿真器，此仿真器可以作為將來相關研究與產品開發的平台，亦可以作為 WiMAX 學習教材。此外，本篇論文也提到在實作中的經驗與遭遇的相關問題，這些經驗與問題對將來 IEEE 802.16e 實際建構時，有所助益。

An Implementation of IEEE 802.16e General Handover Emulator

Student：Szu-Min Chen Advisor：Dr. Rong-Hong Jan

INSTITUTE OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL CHIAO TUNG UNIVERSITY

Abstract

Recently wireless technologies are fast growing and widespread, the coverage of wireless networks extends from meters to miles. The up-to-date WiMAX technology claims to provide a bandwidth of 75 Mbps and coverage over 31 miles. In this thesis, we design and implement an IEEE 802.16e emulator with the general handover mechanism. The proposed emulator will be a good platform for further research, application development and even teaching tools. The experiences and the problems we encountered during implementation will be helpful for the one who wants to construct a real WiMAX network system.

Acknowledgements

I would like to show the greatest gratefulness to my advisor, Prof. Rong-Hong Jan, for his patience and guidance in the whole process of this thesis. I would also like to thank the members in the Computer Network Laboratory and my friends for their assistance and support.

Last, thanks to my family for their endless love and accompanying.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Many different wireless access protocols have been designed nowaday. These protocols can be divided into several groups by the access range and available bandwidth. Personal Area Network (PAN) [1], takes Bluetooth as example, is about 10 meters in distance and a bandwidth of 1 Mbps; Local Area Network (LAN) [2], takes 802.11a and 802.11g as examples, are about 100 meters and 54 Mbps; Wide Area Network (WAN) is expected to provide about 1000 meters and bigger bandwidth. An up-to-date technology, WiMAX technology [3], promises to transfer data at about 75 Mbps over 31 miles.

To accomplish WiMAX technology standard, IEEE standard 802.16d [4] [5] and IEEE standard 802.16e [6] are finalized in 2004 and 2005, respectively. IEEE standard 802.16d defines the PHY and MAC layers for Subscriber Station (SS) and Base Station (BS) to setup essential management connections and data connections. IEEE standard 802.16e is an amendment for IEEE standard 802.16d in both PHY layer and MAC layer to provide further capabilities of security, mobility and power saving without modifying the network entry process defined by IEEE 802.16d.

To achieve mobility, the most two important problems in MAC layer

are the process of handover and managing security information. However, in this paper we only discuss the process of handover. IEEE standard 802.16e defines four different MAC layer handover mechanisms, every one of these four mechanisms has special characteristics. However, some researches focus on supporting mobility for WiMAX before IEEE standard 802.16e shows up. [7] proposes a handover scheme for IEEE standard 802.16d without adding any new management frame. In the proposed method, they obtain the functionalities required by connection handoff by eliminating unnecessary steps in the initialization process. They also find that it is possible to reuse existing messages to serve the place of Handover Request (HO-REQ) and Handover Response (HO-RSP) messages.

There are also researches about handover scheme defined in IEEE standard 802.16e. [8] mentions a problem of handover delay to real-time downlink services and proposes a fast handover scheme to reduce the handover delay. The proposed scheme is reached by sending the data "during handover procedure" instead of "after handover procedure". They define a new message named Fast_DL_MAP_IE, which contains the Mobile Station (MS) MAC address and resource allocation information for downlink data. If there is an emergent downlink data for MS during handover procedure, MS can receive the real-time traffic from Target BS using Fast_DL_MAP_IE. They claim that MS can receive data from Target BS without synchronization. [9] also proposes a handover scheme that Serving BS is in charge of monitoring the uplink signal strength or SINR to decide and initiate handover procedure. MS doesn't need to do scan until handover procedure is initiated. Since data connections will be interrupted during Scan procedure, the proposed scheme provides better channel utilization. When handover procedure is initiated, MS will do scan and report the results to Serving BS. Serving BS will also send handover

notification to neighbor BSs and get some responses. The responses from neighbor BSs include the signal strength estimation of the relevant MS. Serving BS then will be able to decide the handover direction according the results. But the disadvantage of the proposed scheme is that all MS must be active and have uplink traffic all the time. However, MS may go to sleep mode while it needs to perform handover.

Both IEEE standard 802.16d and IEEE standard 802.16e are modern technologies and there is no ready tool to simulate them, thus we try to implement the process of general handover mechanism defined by IEEE standard 802.16e based on an IEEE standard 802.16d emulator implemented by National Central University (called NCU Emulator in the rest of this paper) [10]. Our goal is to add mobility modules to NCU Emulator and construct an emulation environment which supports handover mechanism defined in IEEE standard 802.16e.

We implement the MAC layer general handover process, a most essential and simplest handover mechanism, defined in IEEE standard 802.16e specification. Both MAC layer and network layer to complete the handover procedure are also implemented. The details of MAC layer is well defined in the specification, however, the part of network layer is not. In this thesis, we present the details of network management during handover procedure. To demonstrate our handover mechanism, we put a simple echo application on SS to produce and receive data continuously, and we also execute an echo server somewhere in Internet. After the MAC layer handover process is completed, we tunnel the data through backbone network to new BS to continue the data connections. In chapter 3 we will show the architecture of protocol stacks and data flows, and we will also indicate the problems during implementation.

The proposed emulator can be a platform of testing for the development of applications based on IEEE standard 802.16e. As long as the application functions well on the emulator, it is easy to be ported to fit in with the real IEEE standard 802.16e environment. In addition, the emulator can also be a good teaching material about the procedure of IEEE standard 802.16d and IEEE standard 802.16e. Beginners can learn the protocol of IEEE standard 802.16e quickly through the GUI interface or tracing source codes.

Though IEEE standard 802.16e amends the PHY and MAC layer for IEEE standard 802.16d to provide mobility support, there are still many issues to be discussed, for example, the decision of handover. The further research of these issues, whether it is in MAC layer or network layer, can be based on the proposed emulator.

The remainder of this thesis is organized as follows. In chapter 2, we will shortly introduce the four handover mechanisms described in IEEE standard 802.16e. In chapter 3, the details of our constructions/implementation will be described, including the architecture, topology and problems during implementation. Finally, we will give some conclusion and future works in chapter 4.

Chapter 2

The Handover Mechanisms in IEEE 802.16e

IEEE standard 802.16e is finalized in December 2005. This standard enhances the PHY and MAC layers for 802.16 to support mobility, power saving and security. In this chapter, we will introduce four MAC-layer handover methods described in IEEE 802.16e: General HandOver (General HO), Network Assisted HandOver (Network Assisted HO), Macro-Diversity HandOver (MDHO) and Fast BS Switch (FBSS). The procedure of handover includes several steps, which listed below:

1. Cell Reselection: Both mobile station (MS) and base station (BS) need to find if there is a neighbor BS which can provide stronger signal strength or better QoS services.

2. Handover decision and initiation: BS or MS has to inform its' intends of handover, decide the Target BS, and begin the handover procedure.

3. Ranging to Target BS: In the handover procedure, the Serving BS would release MS, and MS has to do ranging with Target BS. The ranging process is to perform precise synchronization and power control.

4. Network Re-entry: After ranging, the MS has to negotiate with Target BS about capabilities, re-authentication, re-registration, re-establish IP connections . . . etc.

5. Releasing context of MS: Serving BS will discard any context of MS after Target BS reporting that the handover is done.

Note that during the network re-entry process, MS and BSs have to negotiate in both MAC layer and network layer for further connection setup. In MAC layer MS and Target BS have to negotiate their capabilities such as encryption algorithms and QoS requirements. However, MS's information could be sent from Serving BS to Target BS through backbone network after MS sends the ranging request (RNG_REQ) to Target BS if the ranging request includes Serving BS ID. In spite of MS's information of MS's capabilities (negotiate capabilities), Target BS has to arrange the security-related information (re-authentication) while network re-entry process as well. IEEE 802.16e standard defines a protocol, which named PKM, for MS and BSs to do key exchange in a secure way. In this step there will be a lot of time spent on keys generation and exchange.

The five steps listed above must be performed to complete the handover procedure. All of the four handover methods will finish these steps but in different manners, thus they have different handover delay, packet loss rate and implement complexity.

2.1 Cell Reselection

Fig. 2.1 illustrates two different ways for MS to get neighbor BSs' information. First, Serving BS will periodically broadcast Neighbor Advertisement, the

frame MOB-NBR-ADV in Fig. 2.1, and MS can get neighbor BSs' information through this frame. Second, MS can also do scan occasionally or periodically after having Serving BS's approval.

While scanning, Serving BS has to stop communicating with MS and buffer the data during scanning interval. MS will then try to listen if there are some other BSs broadcasting Downlink Map (DL-Map)/ Uplink Map (UL-Map) or Downlink Channel Descriptor (DCD)/ Uplink Channel Descriptor (UCD) and record the carrier-to-interference plus noise ratio (CINR) for each neighbor BS. These CINR values will be reported to Serving BS with Scan Report (SCN-REP) frame after scan.

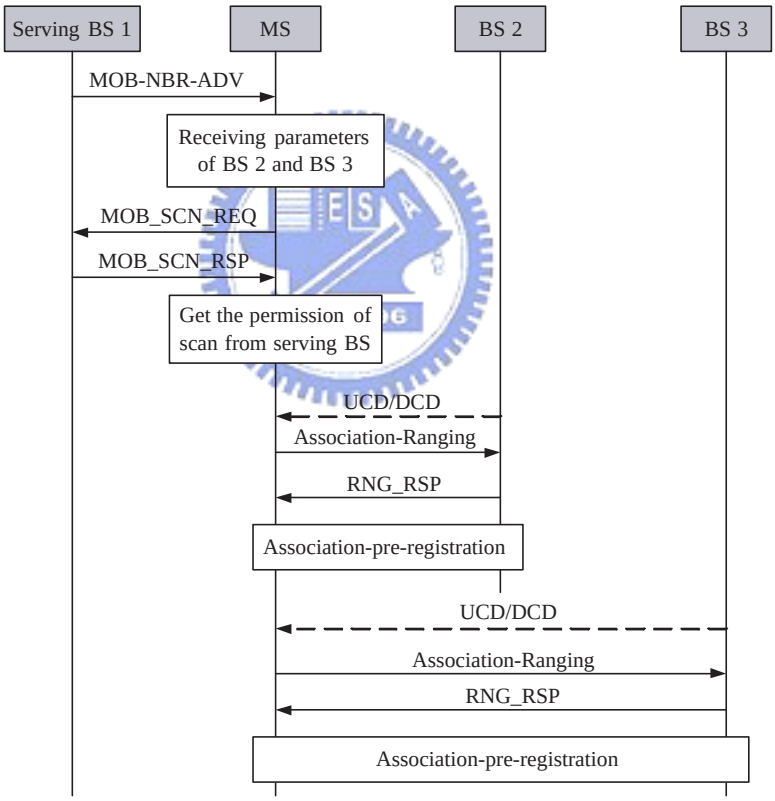


Figure 2.1: MAC management flow for MS doing Cell Reselection.

MS can also do association with neighbor BSs during scanning interval. Association is an option for MS to do initial ranging with neighbor BSs. The ranging results will be recorded in MS's local association table. After ranging, MS will get more precise synchronization and power control parameters, and the results can be used to accelerate the handover procedure later.

2.2 General Handover

General handover is the fundamental method for BS and MS to perform handover. Fig. 2.2 illustrates the procedure of general handover. Fig. 2.2(a) is the handover procedure initiated by Serving BS, and Fig. 2.2(b) describes the handover procedure initiated by MS.

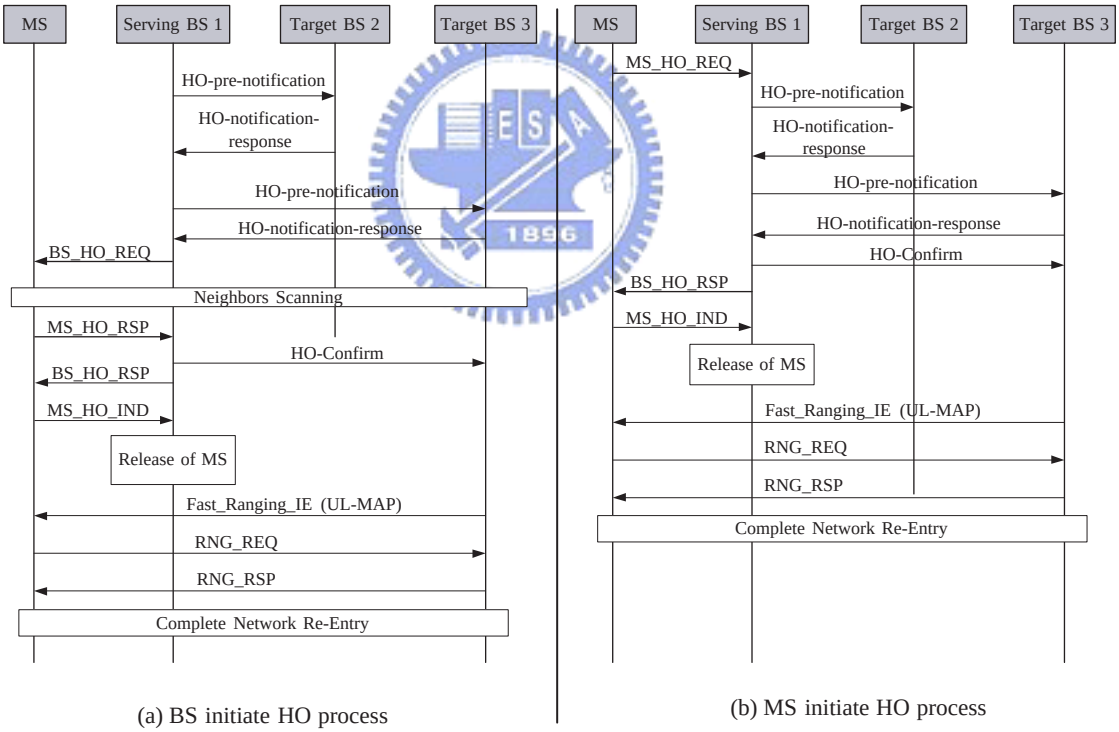


Figure 2.2: General Handover: initiated (a) by BS and (b) by MS

Now we will explain the procedure revealed in Fig. 2.2(a). When Serving BS is aware of the necessary to handover, Serving BS sends handover pre-notification (HO-pre-notification) to neighbor BSs with the MS's information. Neighbor BSs will then send a handover pre-notification response (HO-notification-response) notifying Serving BS whether it can offer the MS sufficient bandwidth and QoS level. MS and BS have to negotiate by sending handover request/ handover response to decide the Target BS. Serving BS decides the recommended BSs for MS to handover according to these responses and sends Handover Request (BS-HO-REQ) to MS. MS will then do a short scan to get signal strengths of neighbor BSs and report the values with Handover Request as a response (MS-HO-RSP) of BSHO-REQ. After receiving the MS-HO-RSP, Serving BS has both data from MAC layer (signal strength) and network layer (the ability to satisfy MS) and is able to decide the Target BS. Serving BS sends Handover Response (BS-HO-RSP) to MS with the information of Target BS decided by Serving BS.

MS can only get the signal strengths of neighbor BSs and compare with the signal strength of Serving BS. When MS is aware of the necessary to handover, the handover procedure is described in Fig. 2.2(b). MS will send Handover Request (MS-HO-REQ) including the information and signal strengths of recommended BSs to Serving BS. Serving BS will then send HO-pre-notification to neighbor BSs and get all HO-pre-notification-responses. Serving BS collects information of MAC layer and network layer. After the decision of the Target BS, Serving BS sends Handover Response (BS-HO-RSP) to MS with the information of Target BS decided by Serving BS.

The rest part of handover after negotiation is described below. Serving BS sends handover confirm (HO-confirm) to the Target BS agreed by both Serving

BS and MS. MS sends HO-IND to confirm the Target BS decision and to inform Serving BS that MS is ready to go. When the time Serving BS receives HO-IND, Serving BS releases MS, which means that all the data communication between Serving BS and MS is suspended.

Target BS becomes aware of the MS's handover in by the HO-pre-notification from Serving BS, and would probably allocate a non-contention ranging opportunity for MS. This information will be put in the UL-MAP broadcasted by Target BS, and MS will be able to send ranging request (RNG-REQ) without contention.

After ranging, re-authentication and re-registration, Target BS will notify Serving BS of the success of handover. The data buffered by Serving BS should be forwarded to Target BS, and many other things should be done to reconstruct the IP connections for MS.

2.3 Network Assisted Handover

Fig. 2.3 reveals the process of Network Assisted Handover. At first, Serving BS sends not only HO-pre-notification but also HO-Confirm to all neighbor BSs.

The HO-REQ sent by Serving BS informs MS that this is a network assisted handover. MS then can send HO-IND right away. After Serving BS release MS, MS has to do scanning and choose the Target BS by its own decision. The rest of the procedure is the same as general handover.

To consider what kind of circumstances would use network assisted handover, we list the differences between general handover and network assisted handover below:

1. Only Serving BS can initiate network assisted handover.

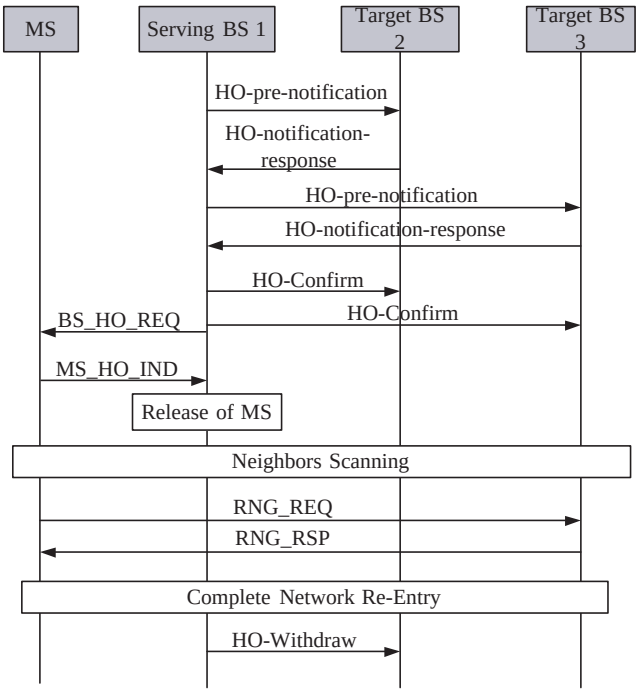


Figure 2.3: The Procedure of Network Assisted Handover

2. Serving BS sends HO-Confirm to all neighbor BSs without negotiation with MS first.

3. MS begins to handover after receiving HO-REQ from Serving BS, and MS doesn't need to negotiate with Serving BS any longer.

4. MS has to decide the Target BS alone.

With the difference list above, we can simply get the picture from the name "Network assisted", which indicates that network information is hidden behind. Imaging that Serving BS is aware of the neighborhood graph and can predict the direction MS is moving toward. There might also be other factors such as load balancing and QoS requirement. Serving BS would probably filter the neighbors after receiving HO-notification-responses from neighbor BSs. Thus the neighbor

BSs in recommended BS list included in HO-REQ are all qualified to take over the duty of serving MS.

On the other hand, MS only needs to decide the Target BS according to signal strength because Serving BS already pick out some capable neighbor BSs. We can say that network assisted handover is triggered by network factors, and general handover is triggered by MAC layer factors.

2.4 Macro-Diversity HandOver and Fast BS Switch

Both Macro-Diversity HandOver (MDHO) and Fast BS Switch (FBSS) are able to provide seamless handover. These two mechanisms are so complicated that they are only optional functions. MS can be informed during capabilities negotiation if Serving BS provides any of these two mechanisms. But before we start to introduce MDHO and FBSS, we must describe the significant data structure named Diversity Set. The members of Diversity Set are BSs participating in the MDHO/FBSS.

Anchor BS is quite the same as Serving BS, it is in charge of handling control messages, negotiation and management with MS during MDHO and FBSS. Anchor BS also has to share all kinds of information of MS and negotiate about the resource allocation with other members in Diversity Set. Both MS and Anchor BS have to maintain the correlated diversity set, including creation and update.

Many restrictions are determined to perform MDHO and FBSS mechanisms:

1. BSs involving in MDHO/FBSS are synchronized based on a common time source.

2. BSs involving in MDHO/FBSS have the same frequency assignment.

3. BSs involving in MDHO shall use the same CID set for connections established with the MS.

4. BSs involving in MDHO/FBSS are required to share or transfer MAC contexts which includes all information MS and BS normally exchange during Network Entry, such as current authentication and encryption keys, registration data, . . . ,etc. So than a MS authenticated/registered with one of the BSs from diversity set is automatically authenticated/registered with other BSs in the same diversity set.

2.4.1 Macro-Diversity HandOver

MDHO is a mechanism for MS to communicate with many BSs at the same time. During MDHO, MS has to send the same PDU to all BSs in diversity set, and every BSs in diversity set has to forward the same data to MS. Before entering the state of MDHO, there are many preparations to do. Fig. 2.4(a) depicts the procedure of starting MDHO.

First, MS and Anchor BS create and confirm the member of diversity set by exchanging Handover Request (HO-REQ), Handover Response (HO-RSP) and Handover Indication (HO-IND) MAC control frames. After the diversity set is determined, Anchor BS has to inform other members and share all MS's information with other members in diversity set. After sending out HO-IND, MS needs to listen to the broadcasted DL-MAP and UL-MAP frames from BS 1 and BS 2. In the MAP frames MS will know exactly when to communicate with each BS.

At the end of Fig. 2.4(a), MS can communicate with both BS 1 and

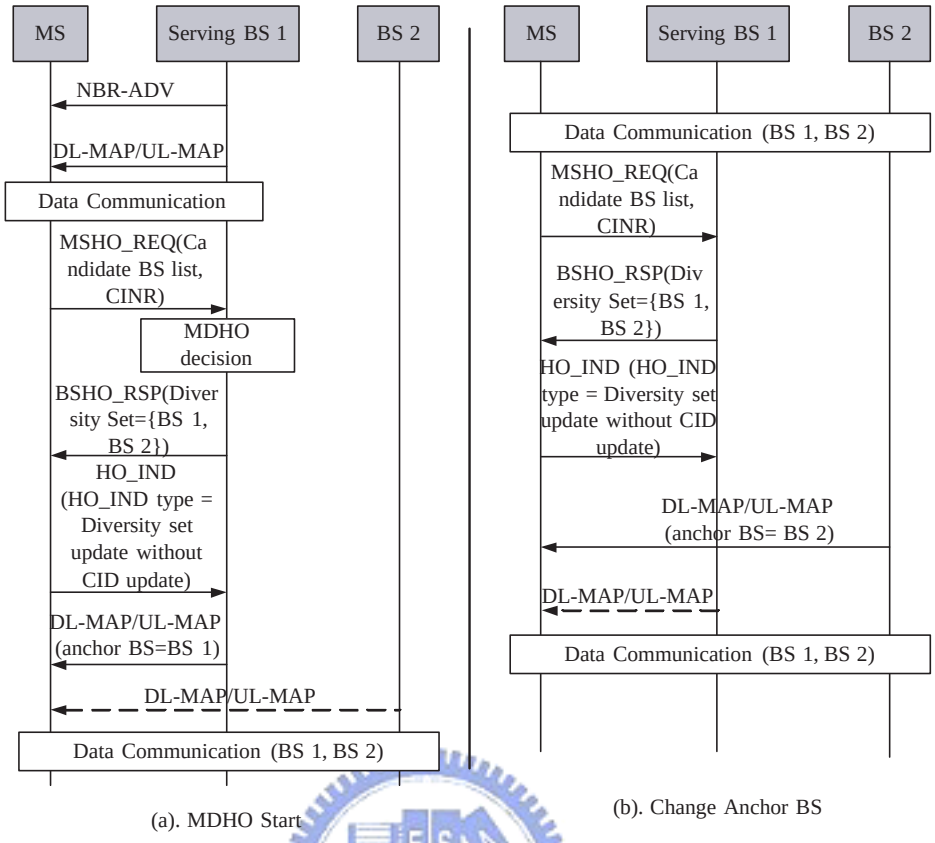


Figure 2.4: The procedure of MDHO: (a) Start MDHO and (b) Change Anchor BS.

BS 2, but Anchor BS is still BS 1. (See Fig. 2.4(b))For updating Anchor BS, MS must send HO-REQ. After HO-IND, MS needs to listen to the UL-MAP/DL-MAP again.

The main factor of diversity set or Anchor BS updating is the CINR evaluated by MS. In the DCD MAC frame, Anchor BS will define two threshold value named H-Add and H-delete. If the CINR value is better than H-Add, the corresponded BS is allowed to be added into diversity set. But if the CINR value is worse than H-delete and the corresponded BS has been in diversity set already, the BS must be dropped immediately.

Fig. 2.5 shows the procedure of updating diversity set. At first MS is performing MDHO with BS1, BS2 and BS3. Then MS might find out that the CINR value with BS 3 is bad after evaluation. Thus MS sends HO-REQ to Serving BS 1 with evaluation result.

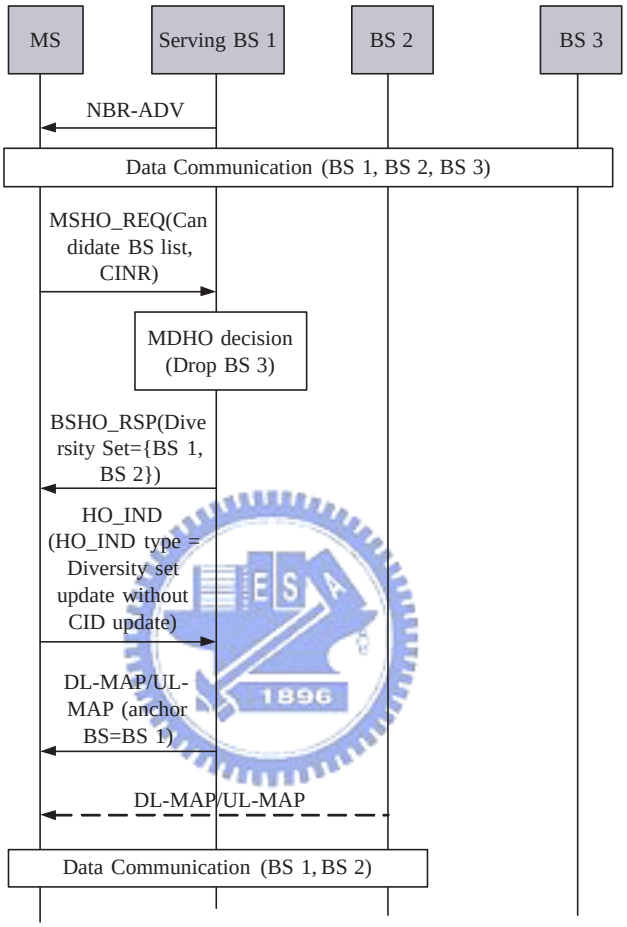


Figure 2.5: The procedure of updating diversity set.

The procedure of diversity set update is exactly the same as diversity set setup and updating Anchor BS. Every variation is negotiated and confirmed by exchanging HO-REQ, HO-RSP and HO-IND.

When the number of BSs in diversity set remains to one, the MDHO can

be seen as the usual communication before MDHO happened and can also be taken as the end of MDHO.

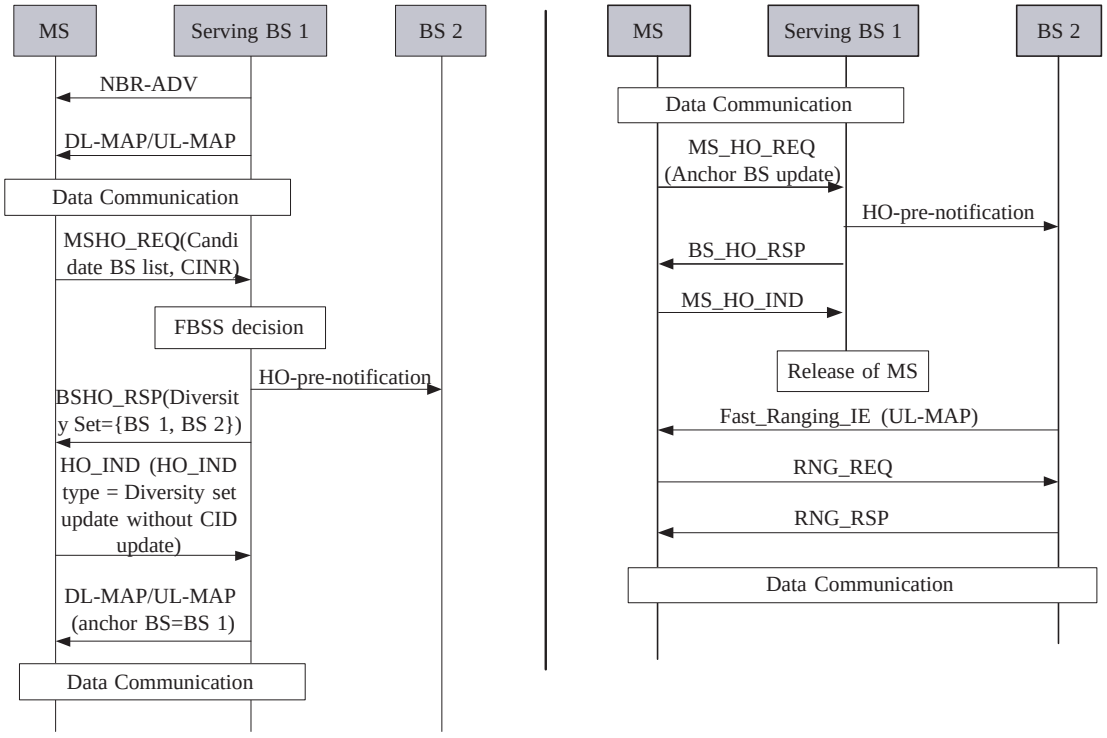
2.4.2 Fast BS Switch

FBSS is a handover mechanism also providing seamless handover, but it is much simpler than MDHO on both aspects of PHY and MAC layers. During FBSS, MS only needs to communicate with one BS, i.e. Anchor BS, and this BS must belong to diversity set. Anchor BS will share MAC context of MS to other BSs in the same diversity set through backbone network automatically. When MS wants to switch Anchor BS to other BS (also called Anchor BS update), none of the Network Re-entry steps is needed.

MS and Anchor BS both need to maintain diversity set as MDHO, and the procedures to update diversity set are totally the same. But to perform FBSS there are two ways, one is to send MAC control frames as other handover procedures described above.

Fig. 2.6 reveals the message flow for FBSS by MAC control frames. As MDHO dose, FBSS needs to construct the diversity set to collect all BSs involved in (See Fig. 2.6(a)). The Anchor BS must belong to diversity set. To change Anchor BS within diversity set, both MS and current Anchor BS can send HO-REQ to inform the decision, shown as Fig. 2.6(b). Worth a special note, they don't need to perform any Network Re-entry step. And this is how FBSS provides seamless handover.

The other way to perform FBSS is to send Anchor Switching Indication through Fast Feedback Channel. Under this mechanism MS will be able to send FBSS related control messages through Fast Feedback Channel without compe-



(a). FBSS Start

(b). Change Anchor BS

Figure 2.6: The message flow for FBSS by MAC control frames: (a) Start FBSS and (b) Change Anchor BS.

tition with other MSs on air. The Fast Feedback Channel shall be allocated by Anchor BS before starting FBSS. There are three methods to notify MS the allocation of Fast Feedback Channel:

1. Pre-allocated by MOB-BSHO-REQ or MOB-BSHO-RSP when a BS is added to the diversity set.

2. Allocated through Anchor Switch Information Element (Anchor-Switch-IE, will be described below) during Anchor switching operation.

3. Allocated by UL-MAP of the new Anchor BS after the switching period.

Fig. 2.7 shows the procedure of FBSS using Fast Feedback Channel. Since FBSS wants to perform seamless handover, the switching time has to be limited. The ASR slots depicted in Fig. 2.7 forces MS to make up switch decision and perform FBSS in the limited time interval. The length of ASR slots is determined by Anchor BS and is broadcasted within DCD MAC control frame.

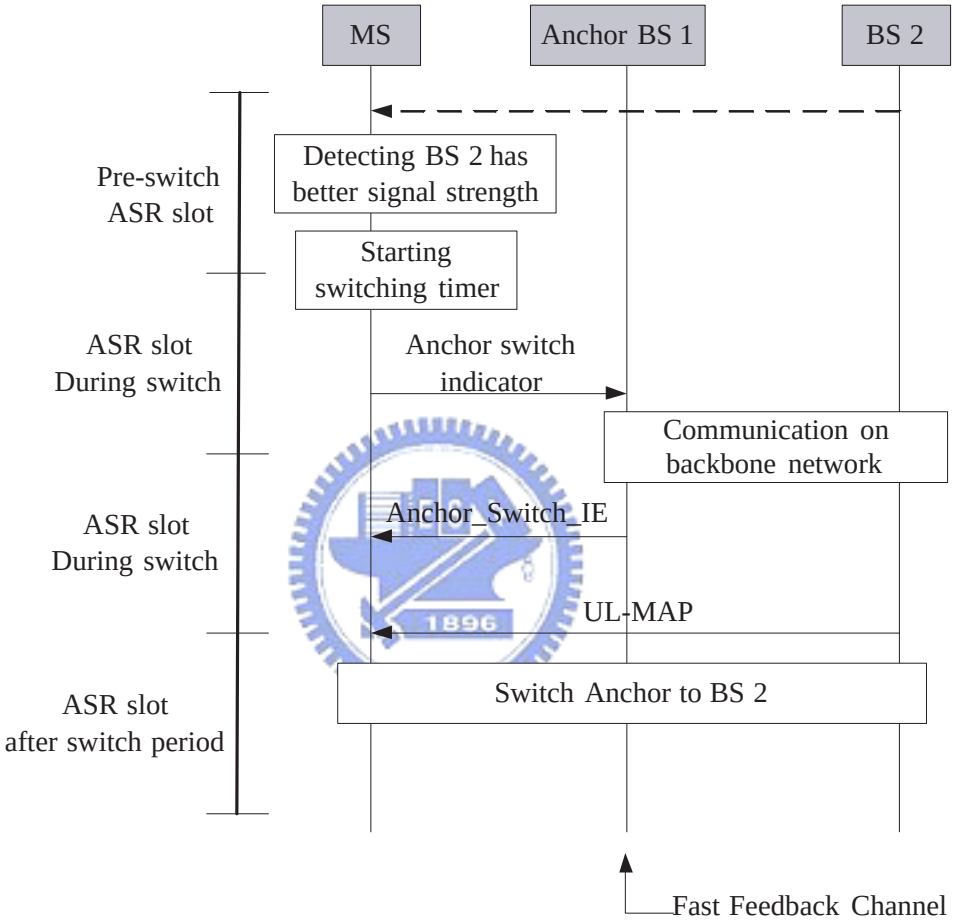


Figure 2.7: The message flow for FBSS by Fast Feedback Channel.

At the first ASR slot MS try to scan other BSs in diversity set, as Fig. 2.7, MS finds out that BS 2 has stronger signal strength and makes a handover decision. After MS makes the handover decision, a switching timer is set up. MS

has to finish BS switching before the switching timer expires.

The second and the third ASR slots are for switching interval. At the beginning of switching interval, MS has to send Anchor Switch Indicator to inform current Anchor BS through Fast Feedback Channel. Current Anchor BS then knows the candidate new Anchor BS and informs the new Anchor BS that BS switching is happening. During switching interval there is a very important message called Anchor-Switch-IE. With Anchor-Switch-IE the current Anchor BS may notify MS about many things:

1. Acknowledgement of MS's switch indication.
2. Cancellation of BS switching.
3. Informing the allocation of Fast Feedback Channel by new Anchor BS.
4. Giving instruction on exact action time to switch.
5. Specifying the new Anchor BS to switch to.

Every item listed above is optional and may be within or without. If the exact switching time is included, MS must obey it. But if the switching time is not told, MS will do BS switching after the expiry of switching timer. Since the new Anchor BS can get all contexts of MS from current Anchor BS, there is no need to perform any part of Network Re-entry.

To compare FBSS with MDHO, the former is simpler and much easier to implement. Although they both need to maintain diversity set and share MS's contexts with all BSs involved in, while MDHO is performing, all BSs have to use the same frequency and CID sets to communicate with MS, and these must be

negotiated carefully. On the other hand, there is no need for FBSS to negotiate about the CID sets, and the MS only sends/receives data from Anchor BS, thus has better channel utilization.

Chapter 3

The Implementation of IEEE 802.16e General Handover Mechanism

In this chapter, we will describe the main steps defined in IEEE standard 802.16e to perform the handover mechanism. With these steps there are the most important functions needed to implement. These functions can be divided into two aspects: MAC layer (defined in specification) and network layer (described but not defined in specification) functions. Then we will give an entire look of the handover process and explain the reasons of our measures during implementation.

3.1 Introduction of IEEE 802.16e General Handover Mechanism

3.1.1 MAC Layer (defined in specification)

MAC layer procedure is performing between MS and BSs. The main steps during handover are described in order below:

1. Cell Reselection: Before doing handover, the MS and BS must know how many other BSs exist nearby. For BS, we construct the neighbor graph

manually and statically before the compile time. For MS, the situation is a little complicate.

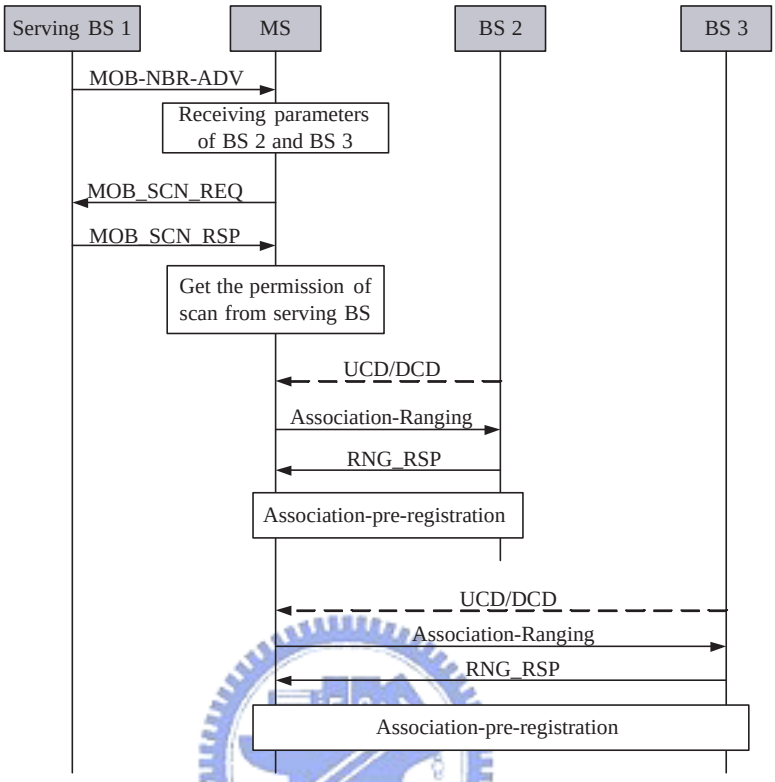


Figure 3.1: The ways MS get aware of Neighbor BSs.

See Fig. 3.1. MS will receive Neighbor Advertisement (NBR-ADV) periodically broadcasted by Serving BS, which MS performed Network Entry procedure with. The NBR-ADV includes the information of neighbor BSs, such as BS MAC address. Besides receiving NBR-ADV, MS can also do some Scan, try to listen to the message broadcasted by neighbor BSs. To perform the Scan, MS has to send a Scan Request (SCN-REQ) to Serving BS. After receiving the Scan Response (SCN-RSP), MS is able to perform the Scan during Scan Interval defined in SCN-RSP. While MS is performing Scan, Serving BS has to stop sending data to MS (buffer the data for MS)

and flush out the buffer after the Scan Interval. During the Scan Interval, MS will try to receive messages broadcasted by neighbor BSs and estimate the signal strength. MS can also do some Association with neighbor BSs. Association is the procedure for MS to send Initial Ranging Request (RNG-REQ) to neighbor BS. The purpose of Association is for MS and neighbor BS to have ranging information (precise synchronization and power control) of each other. After the Association, both MS and neighbor BS will record the result, and these data will be used to fasten the ranging procedure during handover.

2. Handover decision and initiation: After Scan, MS gets the estimation of signal strengths and may send Scan Report (SCN-REP) to Serving BS periodically or by trigger. Both MS and BS may make a decision to handover according to these data collected by MS. To initiate the handover process, both MS and BS can send Handover Request (HO-REQ) to the other. The procedure initiated by MS is a little different from the procedure initiated by BS. We will get down to specifics in the later part of this chapter.

3. Negotiation between MS and BS: When the handover procedure is initiated, the MS and BS have to negotiate to decide a Target BS for MS to handover toward. Both BSHO-REQ and MSHO-REQ will include recommended BS list, while the BSHO-RSP may include only one recommended BS (Target BS). When MS received BSHO-RSP and accept the recommended BS, MS will send a Handover Indication (HO-IND) as agreement. HO-IND also represents that handover shall begin. When HO-IND arrives as agreement, Serving BS must release MS, which means stop sending data to MS.

4. MS performs ranging and network re-entry with Target BS: After sending HO-IND, MS will try to perform ranging and the rest of steps with Target BS to complete the network re-entry.

3.1.2 Network Layer (described but not defined in specification)

Network layer procedure is performing between BSs through backbone network:

1. Cell Reselection: Serving BS has to know the neighbor graph, which is defined and constructed before compile time.

2. Handover Decision and Initiation: When there is a handover decision, Serving BS has to send Handover pre-notification (HO-pre-notification) to all neighbor BSs, which includes the information of the MS yearning for handover, such as MAC address, supports of encryption/decryption algorithms, bandwidth requirement or QoS level requirement. Neighbor BS will send Handover pre-notification Response (HO pre-notification-response) to notify the Serving BS whether the neighbor BS is able to accept the MS.

3. Negotiation between MS and BS: After Serving BS collects all HO pre-notification response from neighbor BSs and get SCN-REP from MS, Serving BS will be able to select the most suitable Target BS from neighbor BSs. Serving BS will then send the BSHO-RSP including the Target BS information to MS. Serving BS will also send Handover Confirm (HO-Confirm) message to notify Target BS that MS is sure to handover toward.

4. MS performs ranging and network re-entry with Target BS: After the network re-entry is complete, Target BS will send a Handover Complete (HO-Complete) message to the origin Serving BS, notifying that the MS is already under control.

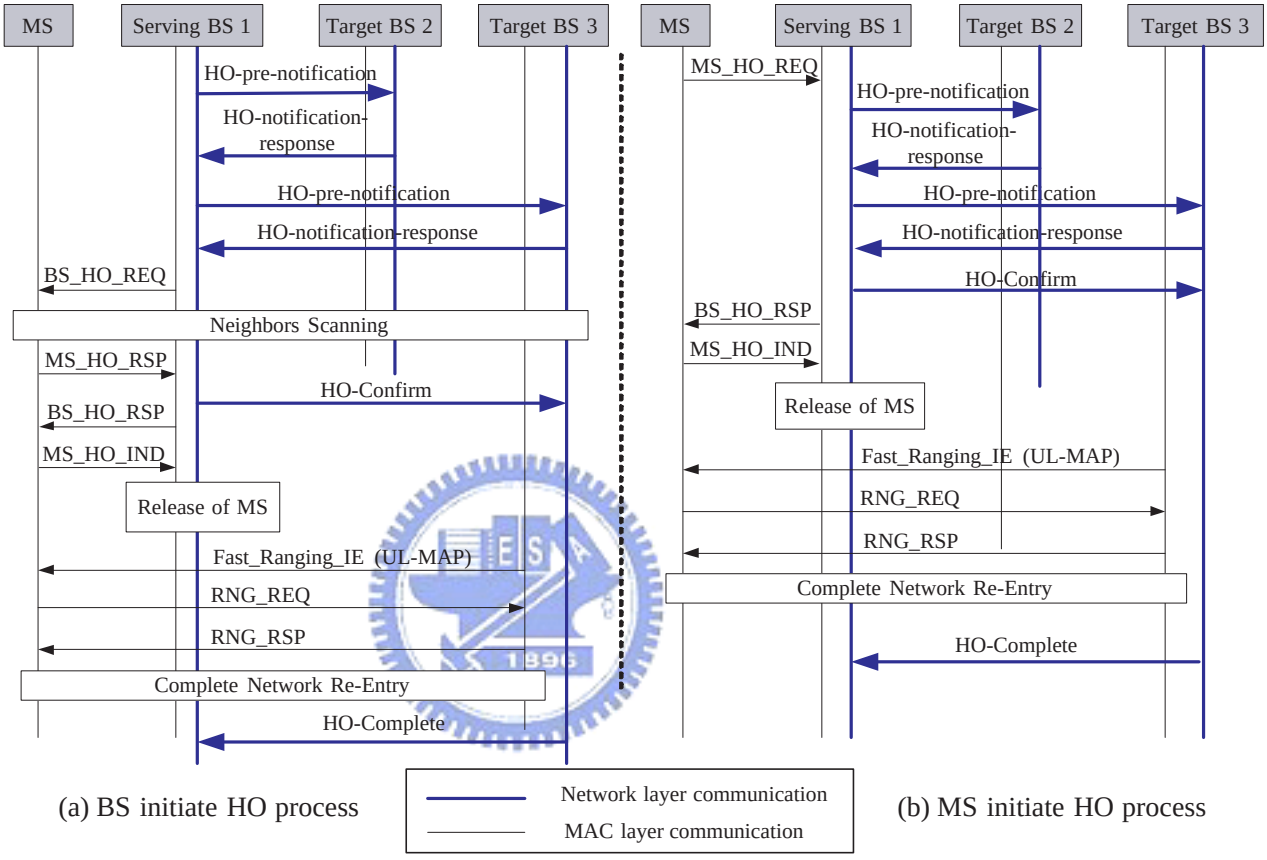


Figure 3.2: The Handover procedure can be initiated (a) by MS or (b) by BS.

Fig. 3.2 reveals the entire handover procedure including both MAC layer and network layer.The MAC layer message exchanges and network layer message exchanges are shown in different colors of lines.

Fig. 3.2(a) is the handover procedure initiated by BS. When Serving BS decides to handover the MS out (maybe it's because the signal strength of MS

is weak, or Serving BS has heavy loading and needs load balance), Serving BS will send HO-pre-notification to all its' neighbor BSs. After collecting HO-pre-notification-responses, Serving BS will send BSHO-REQ to MS including recommended BS list. Then MS might do some Scan very shortly and send MSHO-REQ as response of BSHO-REQ. The MSHO-REQ will also include recommended BSs list with the estimated signal strength of each neighbor BSs. When getting the MSHO-REQ, Serving BS will be able to decide the suitable Target BS and send HO-Confirm to Target BS. Serving BS will also send BSHO-RSP including the information of Target BS to MS. When MS sends HO-IND to Serving BS, the handover procedure begins.

Fig. 3.2(b) is the handover procedure initiated by MS. When MS decides to handover to other neighbor BSs (maybe it's because the signal strength of Serving BS is too weak, or the Serving BS can't afford enough bandwidth, or the Serving BS can't satisfy the QoS requirement of MS), MS will send MSHO-REQ, which includes the recommended BSs list with the estimated signal strength collected by Scan procedure before. When receiving MSHO-REQ, Serving BS will send HO-pre-notification to the neighbor BSs listed in MSHO-REQ, and decide the Target BS after collecting all HO-pre-notification-response. Serving BS then can send HO-Confirm to Target BS and send BSHO-RSP to MS. The rest of the procedure is the same as the handover procedure initiated by BS, which described in the paragraph above.

3.1.3 The Components needed to be Implemented

We give a list of the components needed in Table 3.1. Because of the constraints of the emulator, not all of them are implemented. We implement the

functions to encode/decode MAC and network management frames. The Neighbor Table for BS is constructed before the compile time, while the Neighbor Table for MS is dynamically updated according to the content of NBR-ADV broadcasted by Serving BS.

No.	Title	Detail
1	MAC management frames	NBR-ADV SCN-REQ SCN-RSP SCN-REP BSHO-REQ BSHO-RSP MSHO-REQ MSHO-IND
2	Network management frames	HO-pre-notification HO-pre-notification-response HO-Confirm HO-Complete
3	Association Table	Not implemented. We'll explain this in the next section.
4	Neighbor Table	BS: static. MS: dynamic.
5	MAC Address and IP Address Map	BS: static. MS: static. We'll explain this in the next section.
6	Data Buffering	When scanning and handover, the data must be buffered by Serving BS.
7	Data Tunneling	After handover, data must be tunneled between Target BS and Serving BS.

Table 3.1: The Components needed to be Implemented.

3.2 The Architecture of Implementation

3.2.1 NCU Emulator

NCU Emulator is an emulator of IEEE standard 802.16d. Fig. 3.3 shows the BS interface, Fig. 3.4 reveals the SS interface and Fig. 3.5 describes the Echo interface.

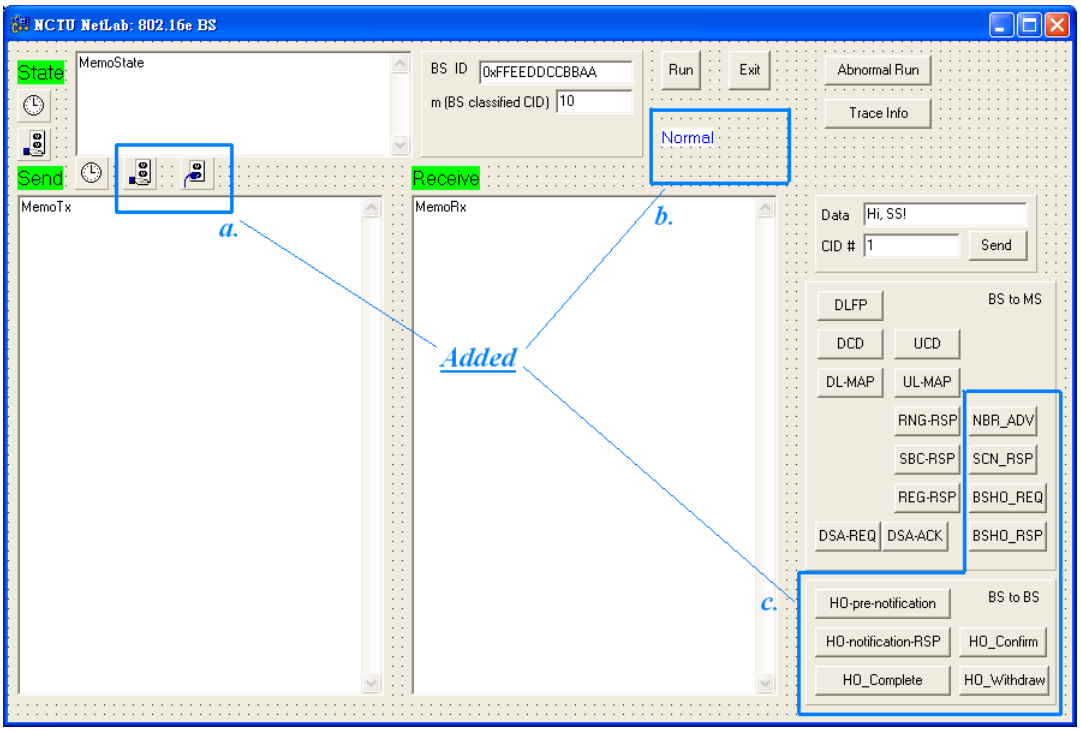


Figure 3.3: The BS Interface of Emulator.

The blue lines drawn in these figures indicate the components we added. The area a. in Fig. 3.3 has two sockets used for the communication between BSs. The area b. in Fig. 3.3 has a label showing if there is a MS handover in/out. The area c. in Fig. 3.3 includes the management frames we added to perform handover.

The area a. in Fig. 3.4 is an Echo button, when the button is pushed, the Echo interface will show up. The area b. in Fig. 3.4 has two buttons. When

push the Scan button, SS will send SCN-REQ to Serving BS. When push the Stay button, the caption of the button will change to "Handover" and trigger the handover event. The area c. in Fig. 3.4 includes the management frames we added to perform the handover procedure.

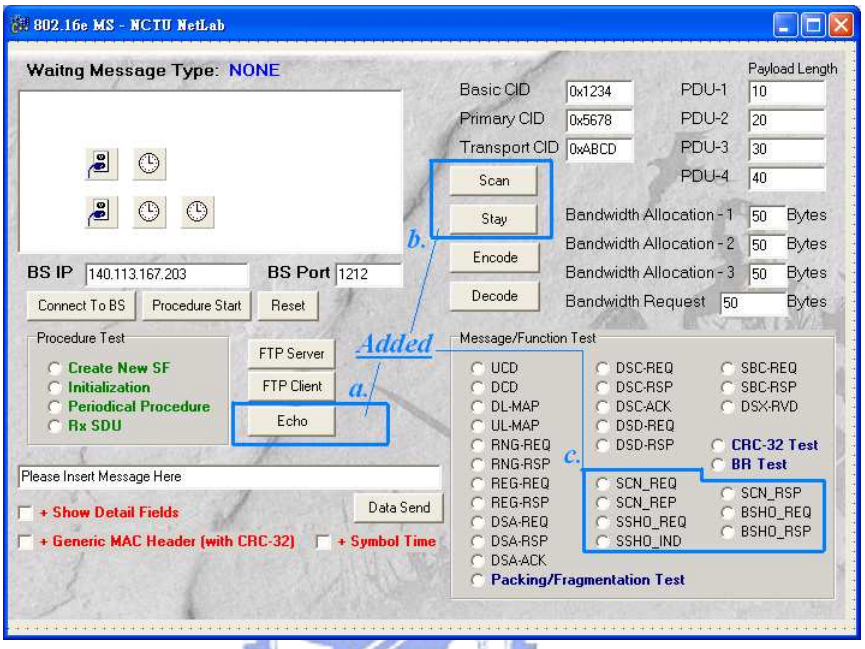


Figure 3.4: The SS Interface of Emulator.

At the beginning of the emulation, we fill in the BS IP address and push the button "Connect To BS", after the connection is setup, push the button "Procedure Start" to start the emulation. When the IEEE standard 802.16d Network Entry procedure is done, push the Echo button to start to send data continuously.

The Echo interface shown in Fig. 3.5 is added to verify the handover procedure, it's whole new to the NCU Emulator. When push the Begin button, the timer will produce data continuously and print out the data in the Sending Listbox. When receiving data, it will be displayed in the Receiving Listbox.

With these GUI interfaces we can see the contents of data transpoted

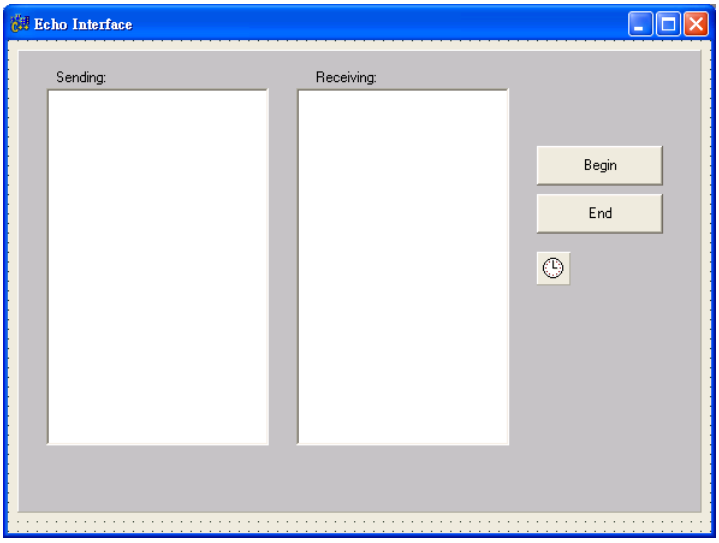


Figure 3.5: The Echo Interface of Emulator

between BS and MS, and we can also observe the progress of all procedures in real time.

3.2.2 Technical Details of Implementation

NCU Emulator is implemented by Borland C++ Builder, which means that the emulation is in Application layer. Fig. 3.6 described the protocol stacks of our emulation.

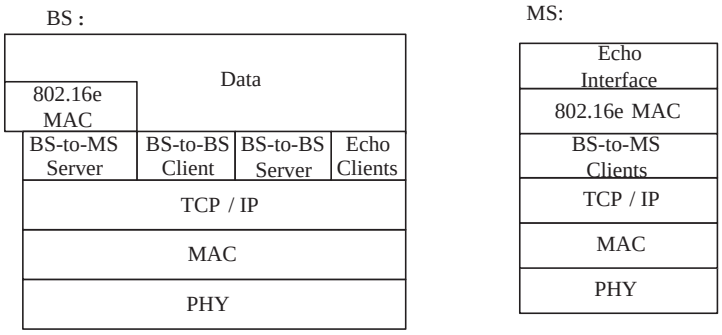


Figure 3.6: The Protocal Stacks of Emulator.

At the beginning of the emulation, Mobile Station (MS) has to setup an IP connection with BS, as revealed in Fig. 3.7. After MS connected with BS, MS is able to receive the IEEE standard 802.16 MAC management frames periodically broadcasted by BS, such as Downlink Channel Descriptor (DCD), Uplink Channel Descriptor (UCD), and Neighbor Advertisement (NBR-ADV).

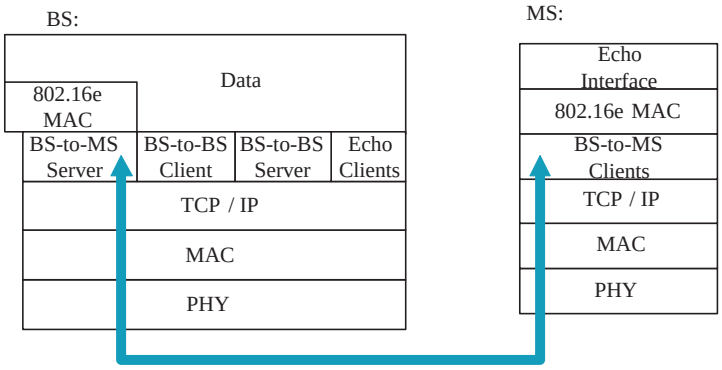


Figure 3.7: MS connects to BS by BS-to-MS Client Socket.

When MS receives either DCD or UCD, MS will start the Network Entry procedure defined in IEEE standard 802.16d. The data flow is described in Fig. 3.8.

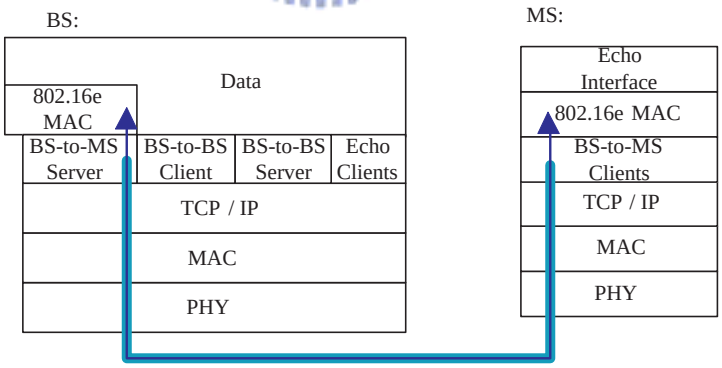


Figure 3.8: MS setup 802.16 connection with BS.

MS will get a Traffic Channel ID (TCID) assigned by Serving BS after Network Entry procedure, so that MS can send data with this TCID. In the meanwhile of emulation procedure, we will start up the Echo Interface and push the Begin button to produce and send continuous data.

When BS receives the data from MS, BS will forward data to Echo server. BS also forwards data echoed by Echo server to MS. What MS sends is what MS gets. To achieve this goal, Serving BS maintains an Echo Client socket for each of the MS. The data flow is shown in Fig. 3.9.

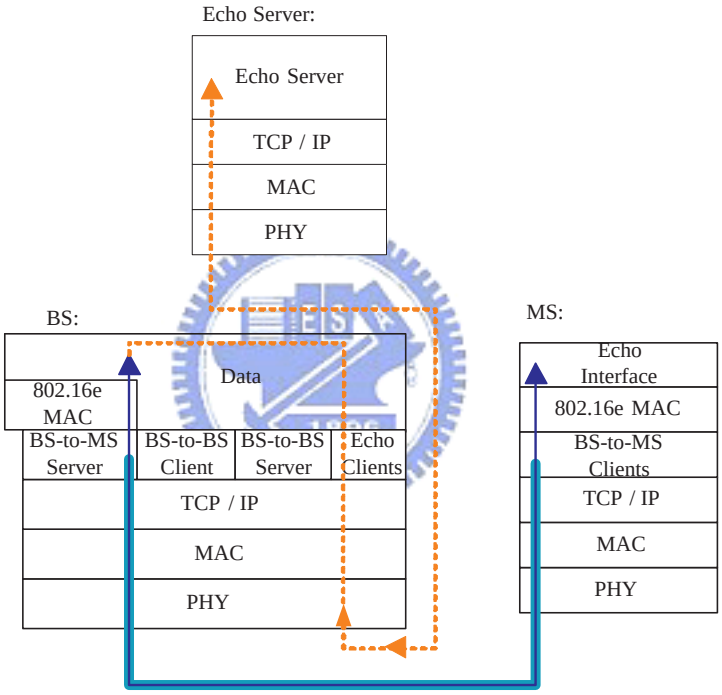


Figure 3.9: BS sends echo data from MS to Echo Server, and sends data echoed by Echo Server to MS.

The handover procedure cannot be triggered before MS complete the Network Entry procedure with Serving BS. We will be able to push the Stay button to trigger handover event at anytime when MS gets ready. During handover pro-

cedure, Serving BS needs to communicate with neighbor BSs, such as HO-pre-notification, HO-Confirm, and Data Tunneling. To carry out the communication through backbone network, we implement one BS-to-BS Client socket and one BS-toBS Server socket in Every BS as revealed in Fig. 3.10. BS-to-BS Client socket sends the network management messages, and BS-to-BS Server socket receives and handles network management messages.

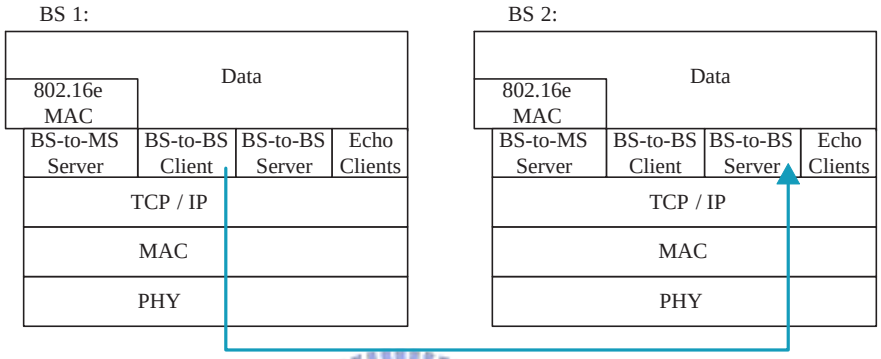


Figure 3.10: If BS 1 wants to communicate with BS 2, BS 1 uses BS-to-BS Client socket to connect to BS 2.

When data delivering has begun before handover, we'll need to perform data tunneling after handover. Fig. 3.11 describes one case of the data tunneling. The BS 1 in Fig. 3.11 is the new Serving BS (Target BS) after handover, and BS 2 in Fig. 3.11 is the origin Serving BS before handover. MS sends data to the new Serving BS, and the data will be tunneled to BS 2, since the data connection to Echo server was set by BS 2.

And when Echo server sends data to BS 2 (as shown in Fig. 3.12), BS 2 will recognize that the data belongs to MS who has already handover to BS 1. Thus BS 2 will tunnel the data to BS 1, and BS 1 will forward the data to MS.

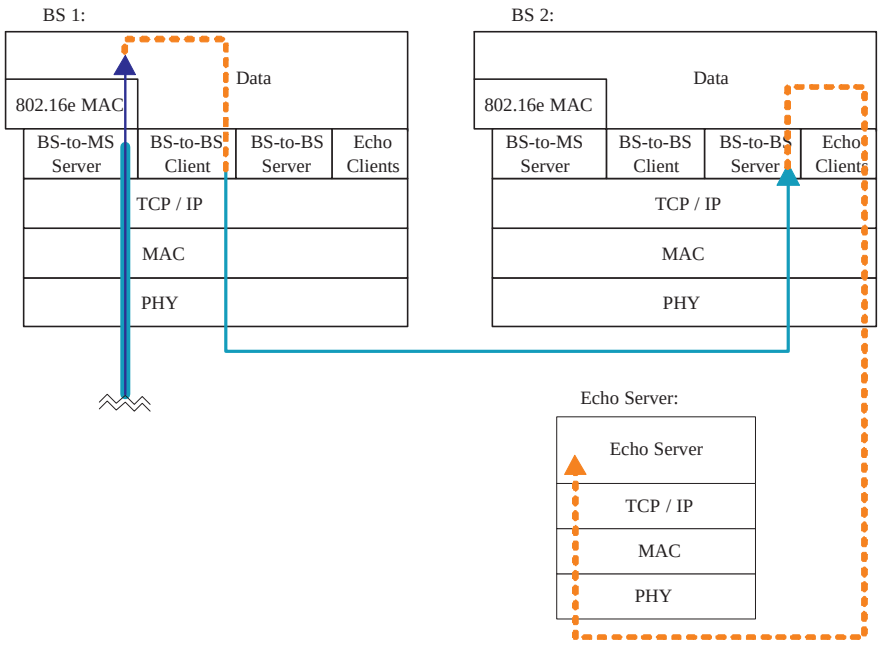


Figure 3.11: Data Tunneling: when BS 1 is Target BS and BS 2 is Serving BS, and BS 1 receives data from MS.

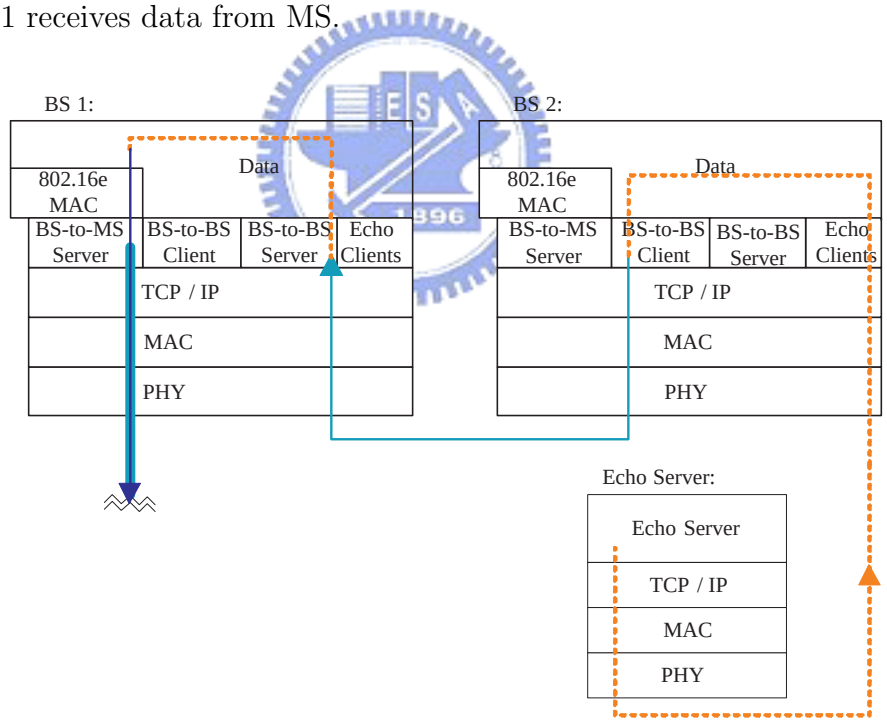


Figure 3.12: Data Tunneling: when BS 1 is Target BS and BS 2 is Serving BS, and BS 2 receives data from Echo Server.

3.2.3 The Problems during Implementation

In this section we will describe the problems and issues during our implementation.

1. Since the emulation is in Application, we need something informal to support the emulation procedure.

   The first thing is the IP Address Map for both BS and MS to know how to connect to neighbor BSs. IP Address Map can get the corresponding ip address from BSs' MAC address, which will be included in NBR-ADV broadcasted by Serving BS.

   The second thing is that NCU Emulator doesn't support real TDMA technology. Thus we can't perform precise synchronization and any function that needs synchronization, such as Scan and Association.

2. For a BS to know the existence of neighbor BSs, we have considered static manner and dynamic manner. The dynamic manner may be achieved by BS periodically broadcast information on a special channel or interface. Every BS will listen to the channel and get information of other BSs. The concept of constructing neighbor graph is vague, and we decided to implement the neighbor graph with static manner, which means to construct the neighbor graph before compile time. The static manner is not only easier but also reasonable. These BSs don't move at all, and the neighbor BSs of one BS would never change.

3. To trigger handover, we need to get signal strength, and even to control the value. When Serving BS's signal strength is weak, MS will try to initiate

handover procedure. But NCU Emulator is in Application layer, thus we implement a function to get CINR value of Serving BS and neighbor BSs. As long as the Stay button on SS Interface is pushed, MS will get the CINR value lower than handover threshold and will begin the Scan procedure. During Scan interval, MS will get the CINR values of neighbor BSs and compare with the CINR value of Serving BS. Becoming aware of the necessary of handover, MS will send MSHO-REQ with the CINR values collected during Scan interval. Though we can't get CINR value actually, the functions to retrieve CINR values can be replaced by any distribution model.

4. Within HO-pre-notification-response there should be a parameter called Service Level Prediction. Serving BS sends HO-pre-notification including information of MS, such as supports of encryption/decryption algorithms, bandwidth requirements and QoS requirements, to neighbor BSs. Neighbor BS should determine if it is able to accept that the MS will handover in. The result of determination should be the value of Service Level Prediction parameters. But we don't implement those requirements from MS, and we don't know how to measure if a BS is able to accept that a MS can handover in.

5. To determine the most suitable neighbor BS as Target BS is also a difficult function. Serving BS can get the information of signal strengths collected by MS and the network information responded by neighbor BSs. Serving BS has to converge these knowledge and rate the performance of each neighbor BSs according to the situation of MS. There will be a lot of factors to bring the result of rating, and the weight of each factors can be different. Weighting these factors depends on the purpose of applications, and it is out of the scope

of our paper. Though we don't discuss the question here, we implement a function to do the selection of Target BS. The function always returns the first neighbor BS in Serving BS's neighbor graph because we only have two BSs in our topology.

6. After handover, MS will regain the data connection. To achieve this, the management of CIDs is a problem. Transport CID is used for recognizing data connection, every connection will assigned a TCID by Serving BS. After handover to a new BS, MS might get a TCID different from the one MS got from original Serving BS. If Serving BS has buffered data for MS during handover and tunneled the data to Target BS after handover, the data contained old TCID will be forward to MS. MS will extract the data and discard the data as soon as MS finds out that the TCID in data is different from the TCID MS owns at this moment. MS will treat the data as someone else's.

   To solve this problem, we send the TCID assigned by Serving BS to Target BS through HO-pre-notification, and the neighbor BS can reserve the same TCID (if not being used) for the MS who possibly will handover in. But if the TCID is used by other MS under Target BS, the Target BS has to be in charge of modifying the TCID in data tunneled by original Serving BS. There can be other ways to solve this problem. But what we should think about is which role does a BS play, a bridge or a router. The role of BS decides the solution of this problem.

7. The estimation of handover delay depends on the definition of "connect". The handover delay is a period of time start from the time MS "disconnect" with Serving BS, and to the time MS "connect" to Target BS.

To consider of the handover procedure defined in IEEE standard 802.16e, Serving BS will release MS after receiving the HO-IND from MS. The release of Serving BS means that Serving BS buffers the data instead of sending it to MS. At this moment, we can say that MS "disconnects" with Serving BS.

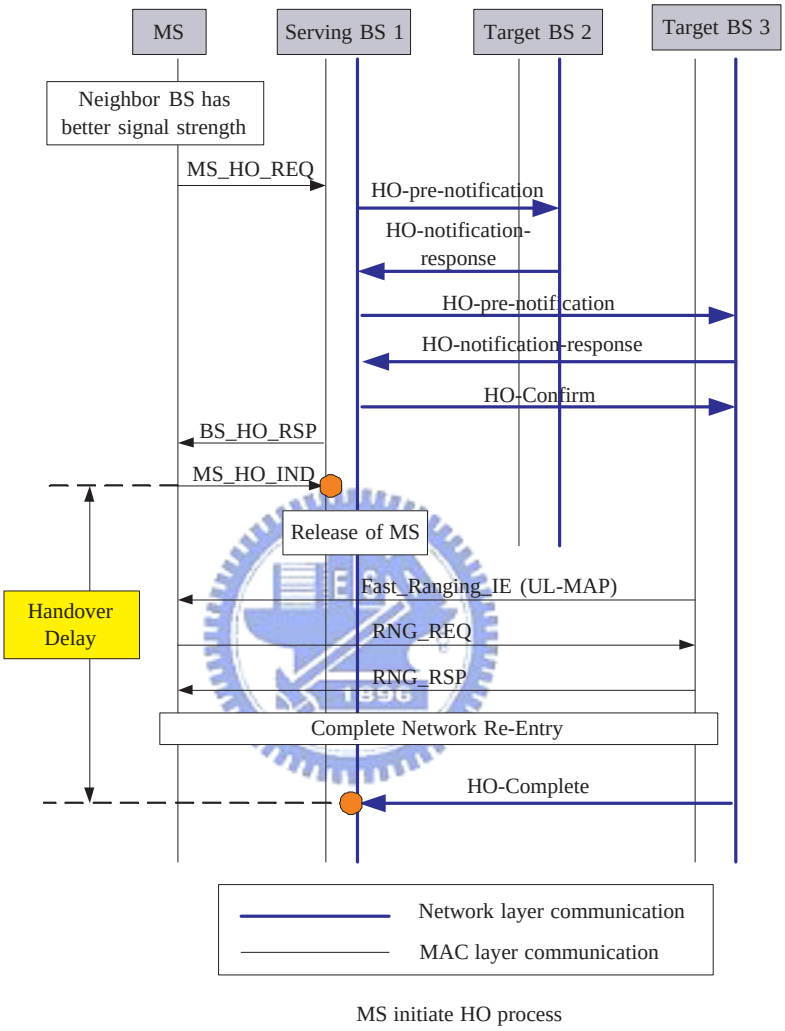


Figure 3.13: The period of handover delay.

After MS completes the Network Re-entry procedure with Target BS, MS is able to send data once again. Target BS will send HO-Complete to the original Serving BS of MS as the notification of the completion of handover.

When Serving BS receives the HO-Complete, the data buffered by Serving BS will be tunneled toward Target BS. Finally, the data will be given to MS. At the time we can say that MS "connects" with Target BS.

As the procedure we described above, the handover delay can be estimated according to two management frames: HO-IND from MAC layer, and HO-Complete from network layer (shown in Fig. 3.13). Since these two messages are received by Serving BS, there won't be a problem of system clock synchronization.

3.3 Emulation Environment

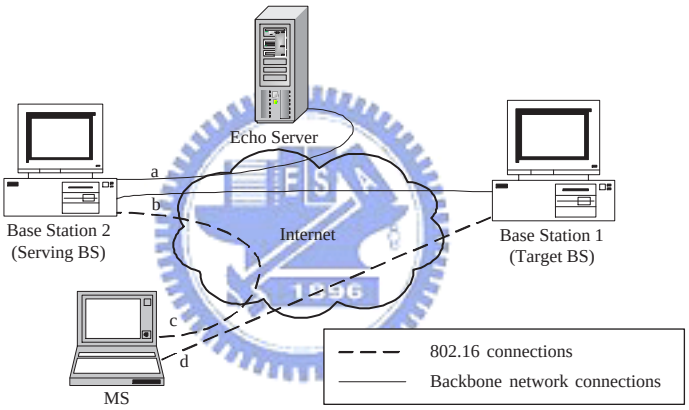


Figure 3.14: The topology of our emulation.

Fig. 3.14 describes the emulation topology. We have one Echo server, two BSs and one MS. When MS connect with BS 2, MS can start the Network Entry procedure defined in IEEE standard 802.16d with BS 2. After the completion of Network Entry procedure, BS 2 becomes the Serving BS of MS (as shown in Fig. 3.15). Then MS is able to send data, and BS 2 will forward data from MS to Echo Server, and forward the echoed data from Echo Server to MS.

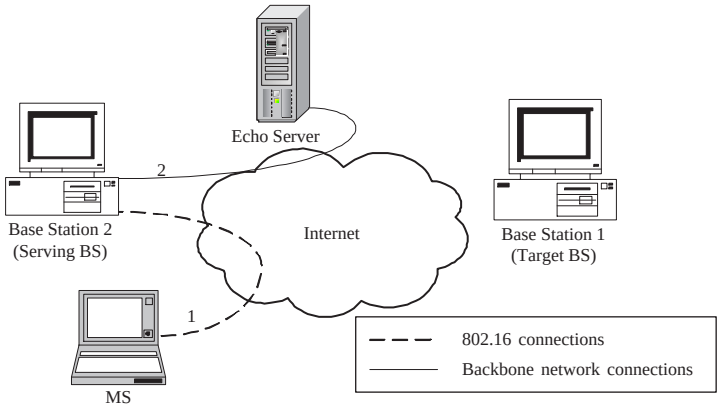


Figure 3.15: After Network Entry procedure: in our topology.

When handover procedure starts, Serving BS will communicate with BS 1, and make the decision that BS 1 is Target BS. MS will agree the decision of Serving BS and then close the connection with BS 2, open a new connection with BS 1. After handover, the data from MS will be tunneled from BS 1 to BS 2, and BS 2 will forward data to Echo Server. The data echoed will be tunneled from BS 2 to BS 1, and BS 1 will forward data to MS. The data flows are revealed in Fig. 3.16.

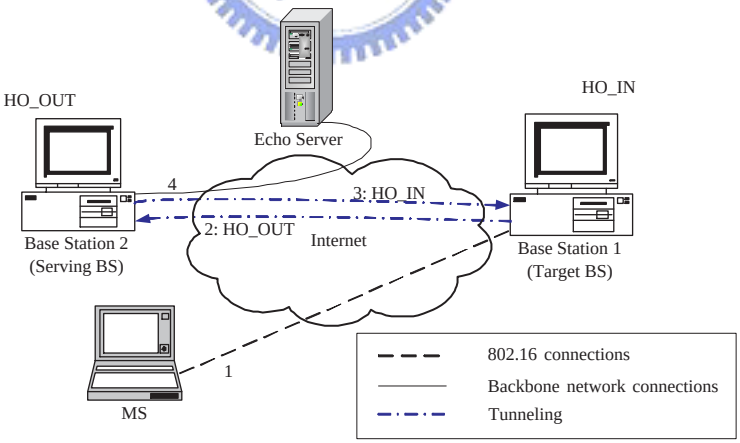


Figure 3.16: After handover: in our topology.

Chapter 4

Scenario of Emulation

In this chapter, we will display the scenario of emulation procedure. We execute an Echo Server on IP address 140.113.23.201, two BSs on IP address 140.113.167.202 (BS 1) and 140.113.167.203 (BS 2), and a MS on IP address 140.113.24.172.

The following pictures describe the preparation of emulation, while Echo Server doesn't do anything (shown in Fig. 4.1); two BSs broadcast many kinds of management frames periodically (described in Fig. 4.2); and MS set up an IP connection to one of the BSs.

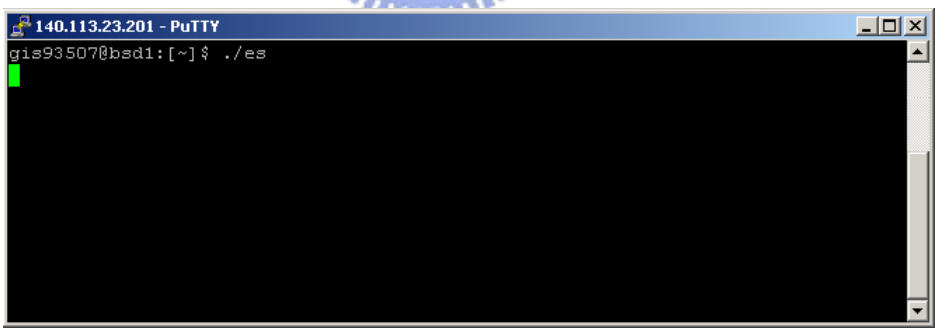


Figure 4.1: Echo Server Interface: at the beginning of emulation.

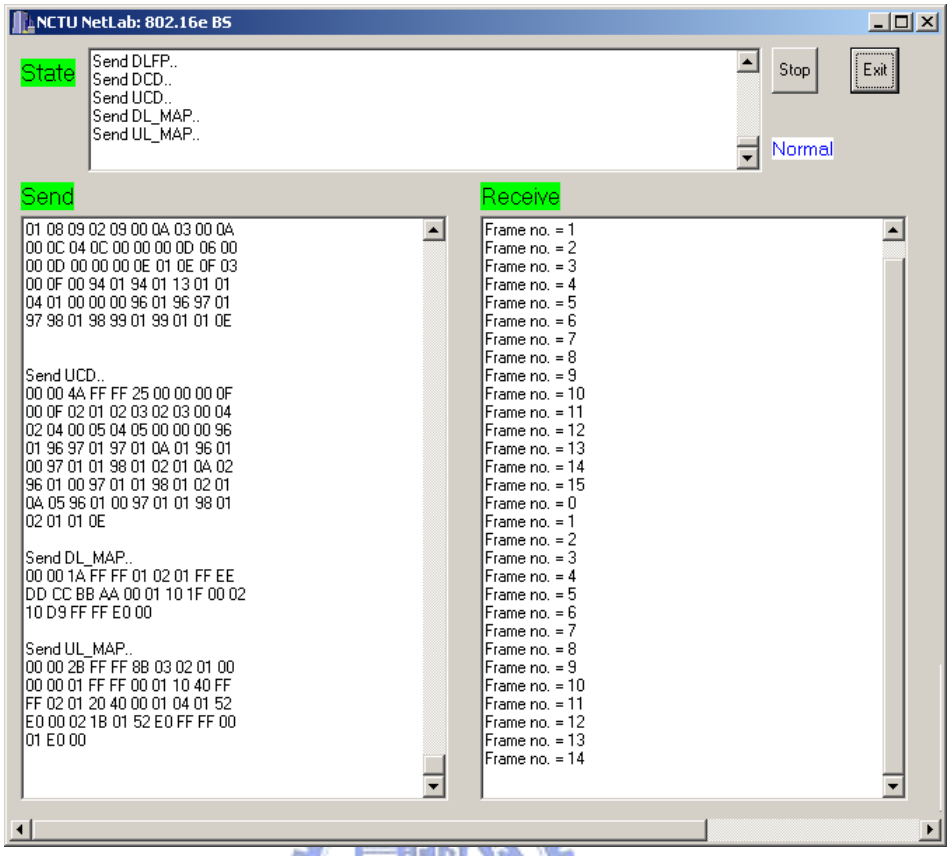


Figure 4.2: Base Station Interface: at the beginning of emulation.

In this scenario, MS connects to 140.113.167.203 at first (revealed in Fig. 4.3). We fill in the BS IP address into the textbox and press the button "Connect To BS" to set up an IP connection with BS 2. Now we can start the IEEE 802.16 emulation. Press the button "Procedure Start" and MS will try to setup IEEE 802.16 connections with BS 2 through the IP connection setup before. At this time, "Waiting Message Type:" shows the type of management frame MS is waiting from BS.

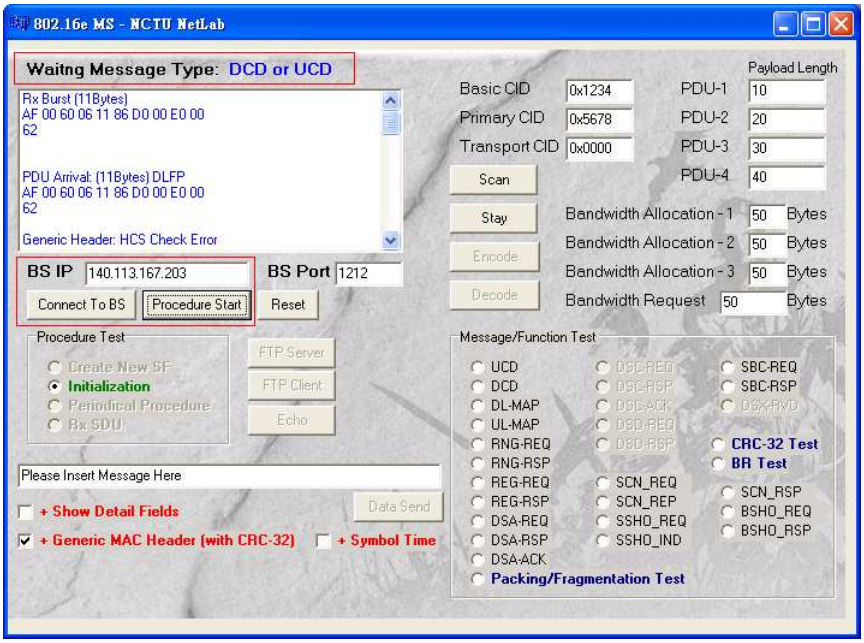


Figure 4.3: Mobile Station Interface: at the beginning of emulation.

When MS receives a DCD or UCD from BS, MS will try to perform ranging and network entry procedure to setup connections. We will be able to observe the entire procedure with these GUI interfaces. In Fig. 4.4, BS displays the content of received message on right side and the content of sent message on left side. BS 2 received a RNG-REQ from MS during frame no. 9, and BS 2 sent a RNG-RSP to MS during frame no. 10. After ranging, BS and MS have to exchange many management frames to negotiate the capabilities of each other, doing authentication and registration. Fig. 4.5 reveals MS interface while performing registration, after MS sends REG-REQ, MS is waiting for REG-RSP from BS. BS and MS will eventually complete the network entry, the "Waiting Message Type" of MS will switch to NONE (described in Fig. 4.6).

Now we can press the Echo button to open the Echo interface and produce data. Fig. 4.7 reveals the Echo interface while producing and receiving data. We

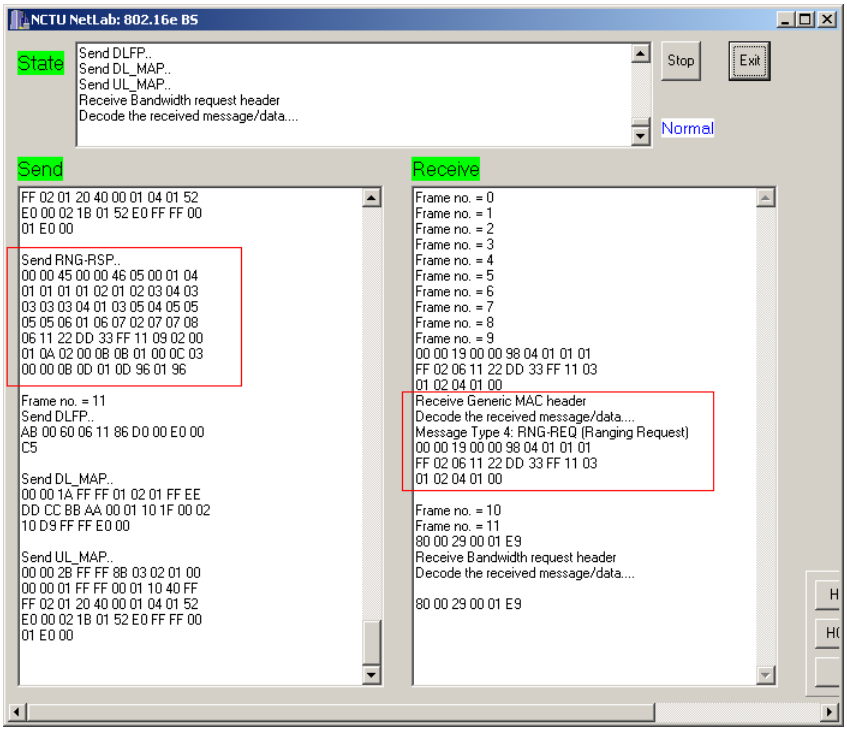


Figure 4.4: Base Station Interface: ranging with Mobile Station.

can also see the data received by Echo Server as described in Fig. 4.8.

When the network entry procedure is completed and data connection is proved to be fine, we can start to emulate the handover procedure. Press the Stay button to trigger the handover event. The caption of Stay button will change to "Handover" as a sign of MS yearning to handover out (shown in Fig. 4.9).

When handover event is triggered, MS will get weak signal strength of BS 2 after receiving NBR-ADV from BS 2. Then MS will try to perform Scan to see if other neighbor BSs can provide better signal strength. Fig. 4.10 reveals the step of MS sending SCN-REQ.

After Scan, MS will discover that BS 1 have better signal strength and send a MSHO-REQ to BS 2. When BS 2 receives MSHO-REQ from MS, the

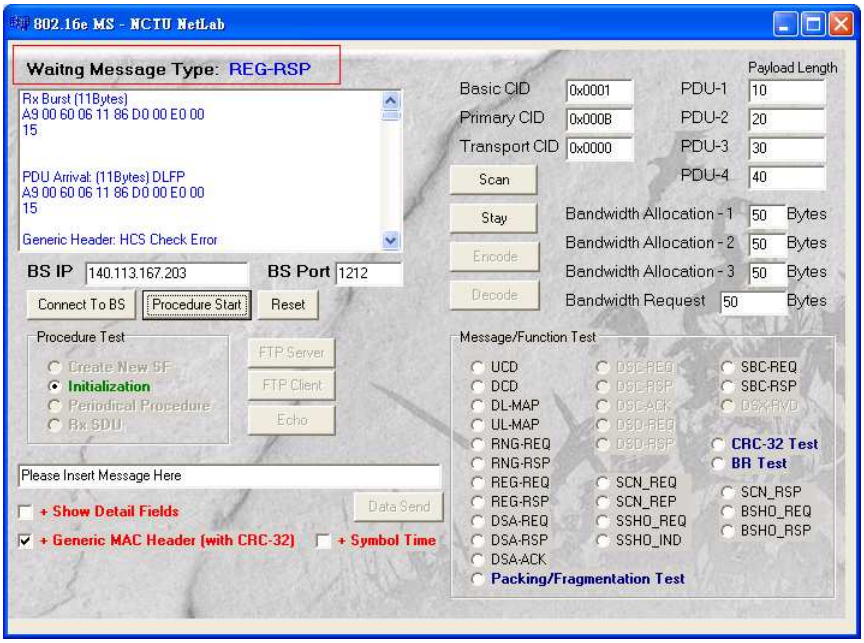


Figure 4.5: Mobile Station Interface: performing registration with Base Station 2.

label on BS interface will display "MS wants to HO OUT". BS 2 will also send HO-pre-notification to BS 1 and wait for HO-pre-notification-response. After all HO-notification-response are collected, BS 2 will send BSHO-RSP to MS including information of BS 1. When BS 2 receives HO-IND from MS, handover begins, and the label on BS interface will display "MS HOing OUT" (described in Fig. 4.11).

When BS 1 receives HO-pre-notification form BS 2, the label on BS interface will display "MS wants to HO IN" and BS 1 will reserve the MS information in a HO-IN table. After receiving RNG-REQ form MS, BS 1 will discover the data of MS in HO-IN table and realizing that MS is handover in, thus the label on BS interface will display "MS HOing IN" (described in Fig. 4.12).

Fig. 4.13 and Fig. 4.14 reveal the BS interfaces after handover procedure is completed. In Fig. 4.13, the label on BS 1's interface display "MS HOed IN".

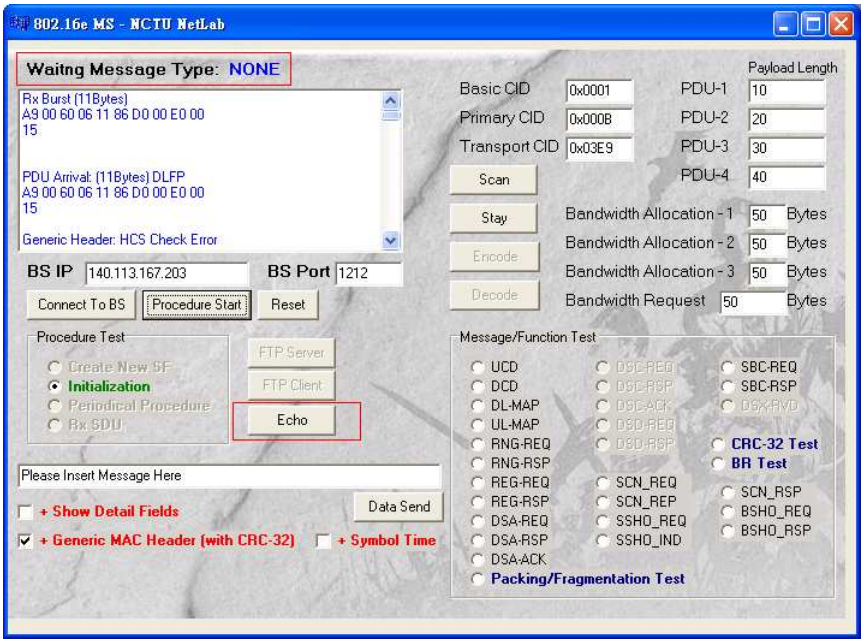


Figure 4.6: Mobile Station Interface: Network Entry procedure complete.

BS 1 will receive data tunneled from BS 2 and forward data to MS. In Fig. 4.14, after receiving HO-Complete from BS 1, the label on BS 2's interface display "MS HOed OUT". BS 2 will tunnel data from Echo Server to MS. Also, BS 2 will receive data tunneled from BS 1 and forward data to Echo Server.

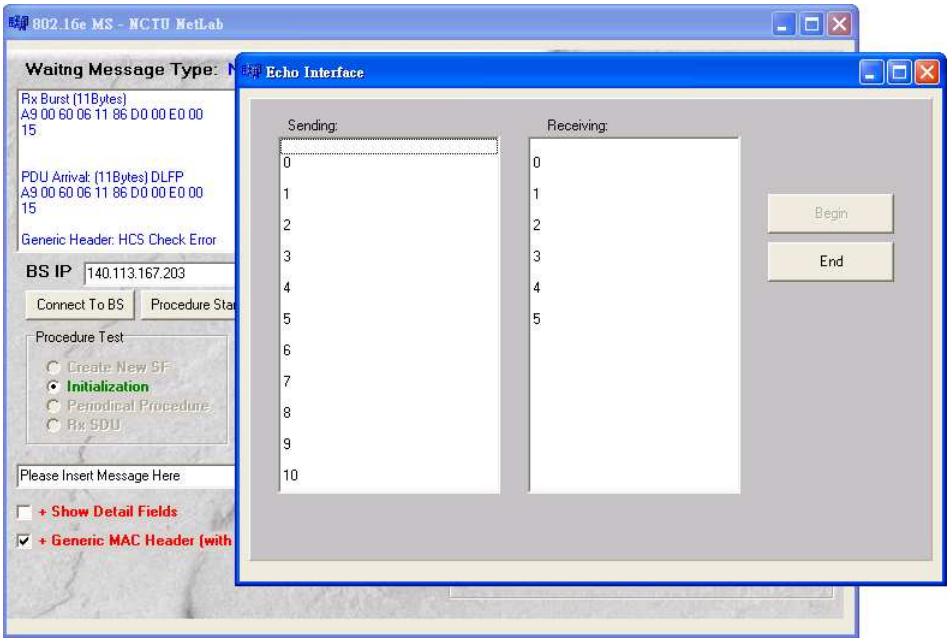


Figure 4.7: Echo Interface: producing and receiving data continuously.

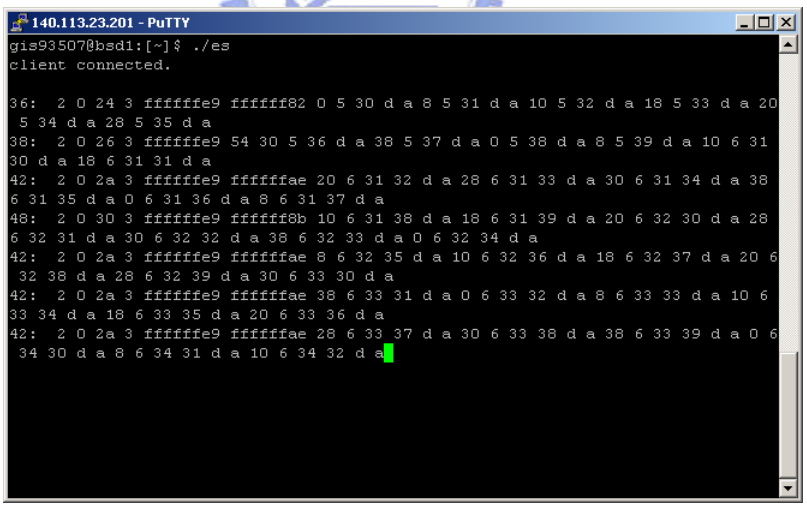


Figure 4.8: Echo Server Interface: receiving and echoing data.

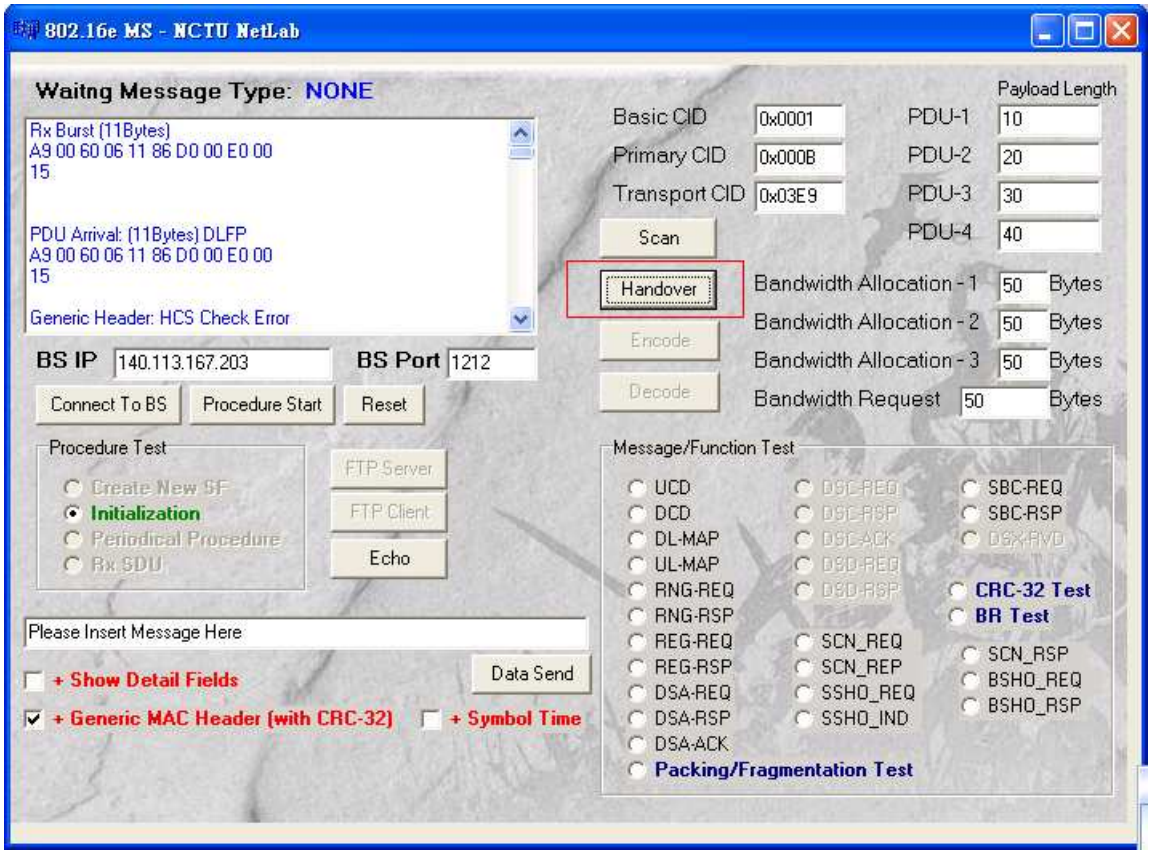


Figure 4.9: Mobile Station Interface: trigger handover event.

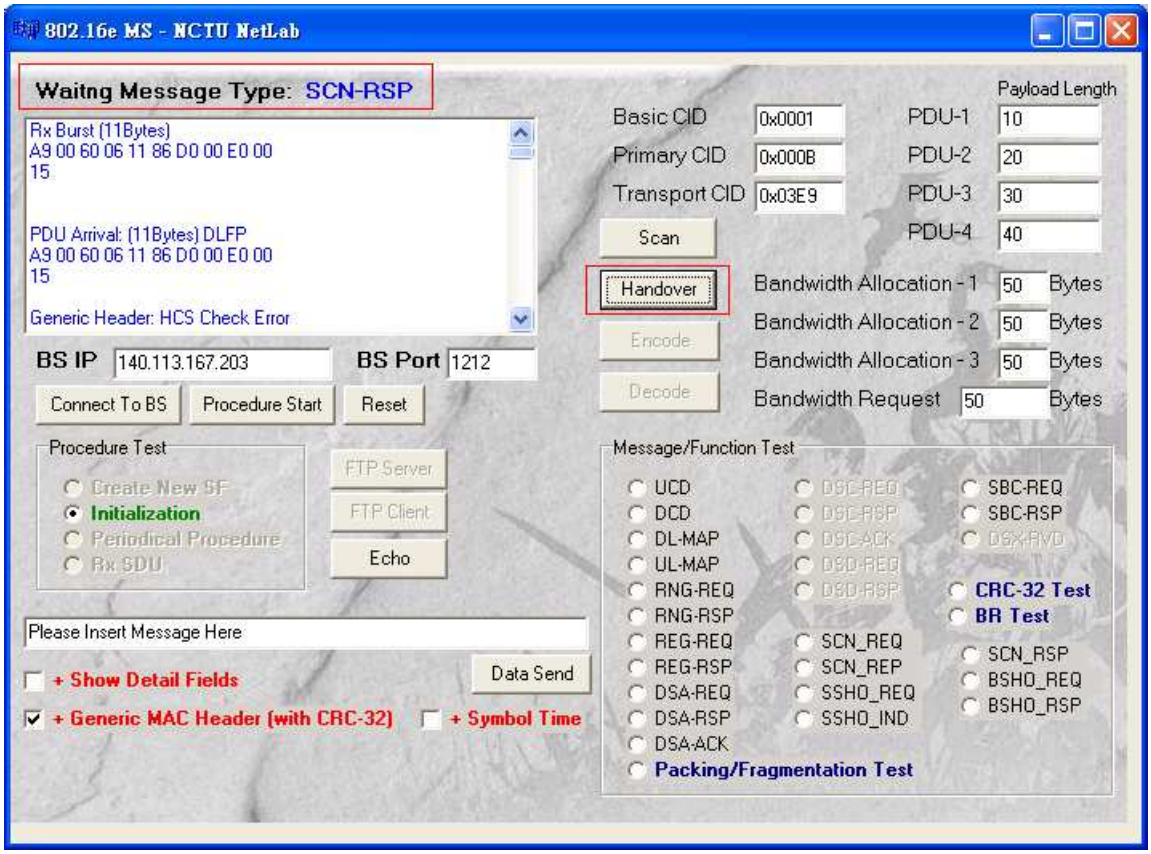


Figure 4.10: Mobile Station Interface: performing Scan.

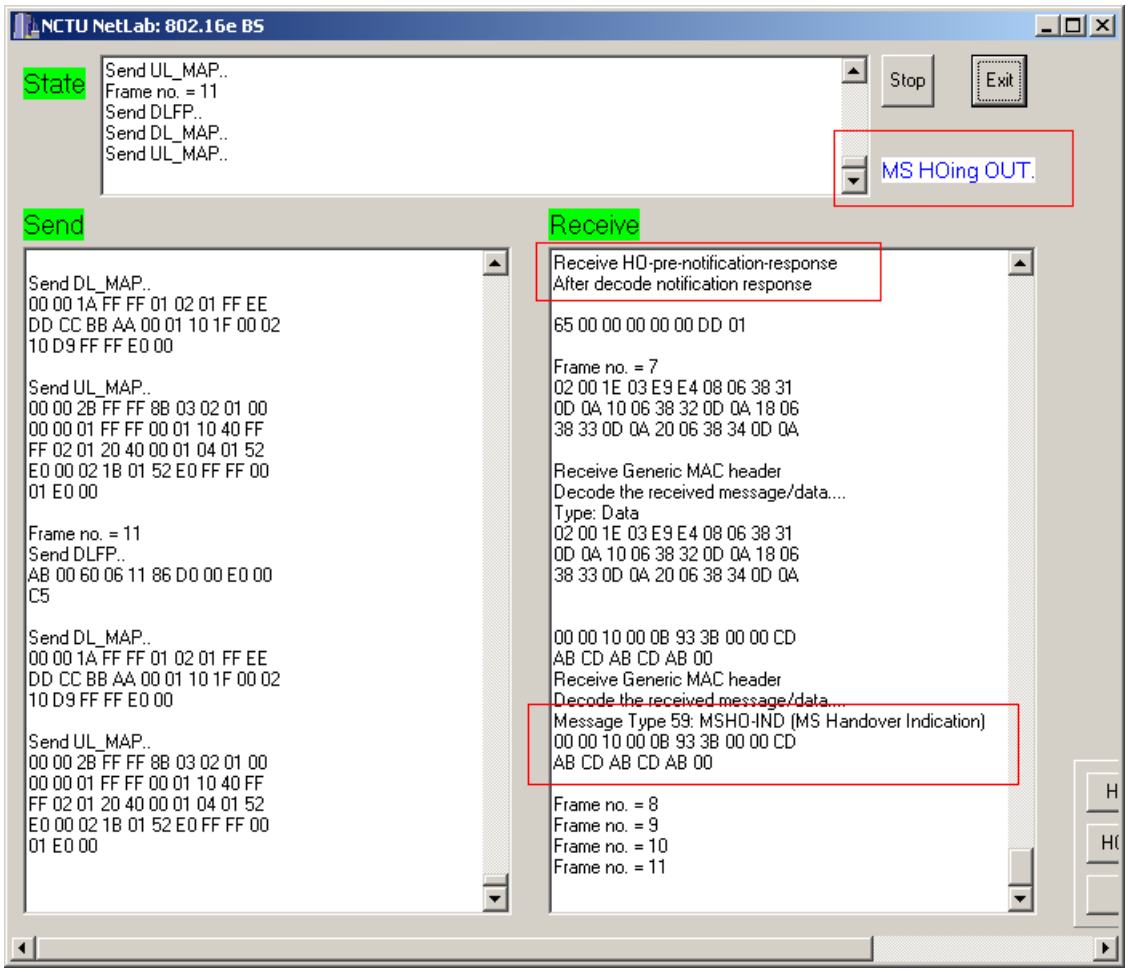


Figure 4.11: Base Station Interface: Mobile Station handover out.

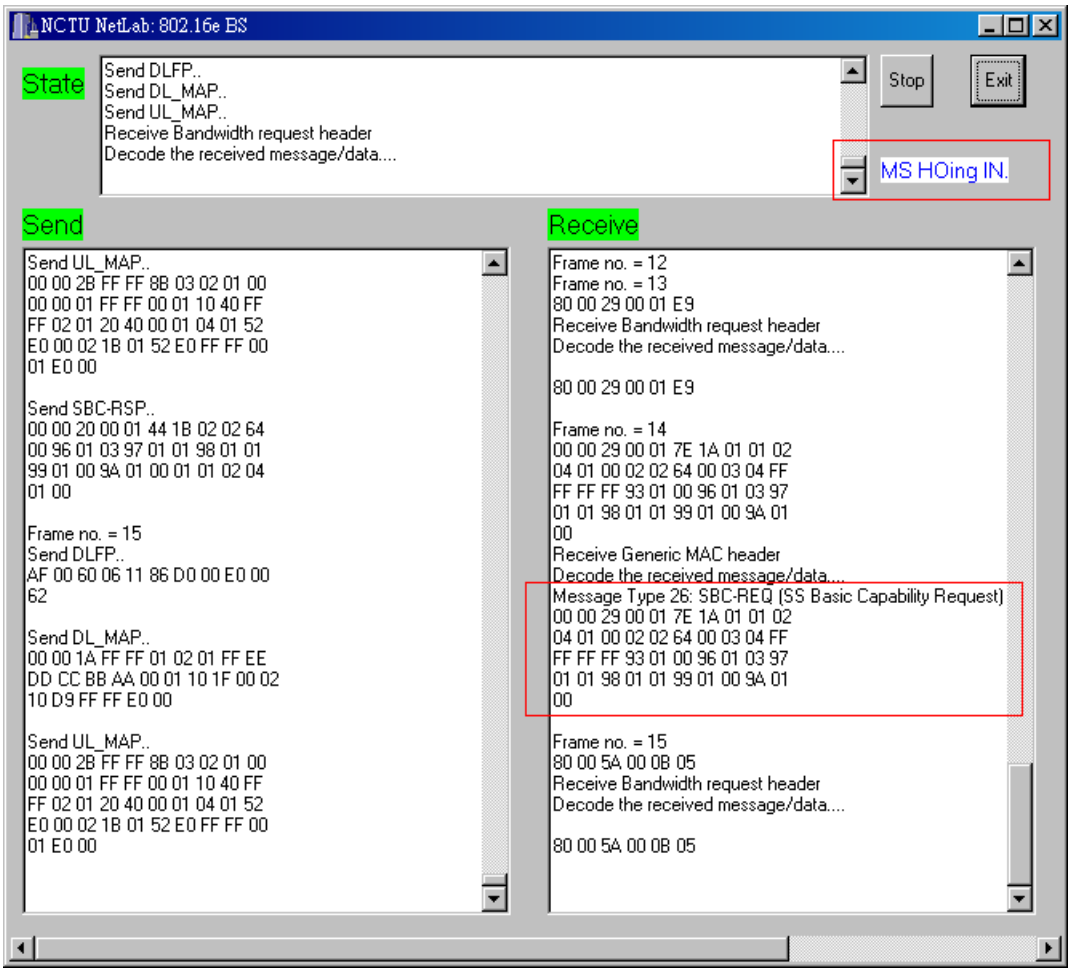


Figure 4.12: Base Station Interface: Mobile Station handover in.

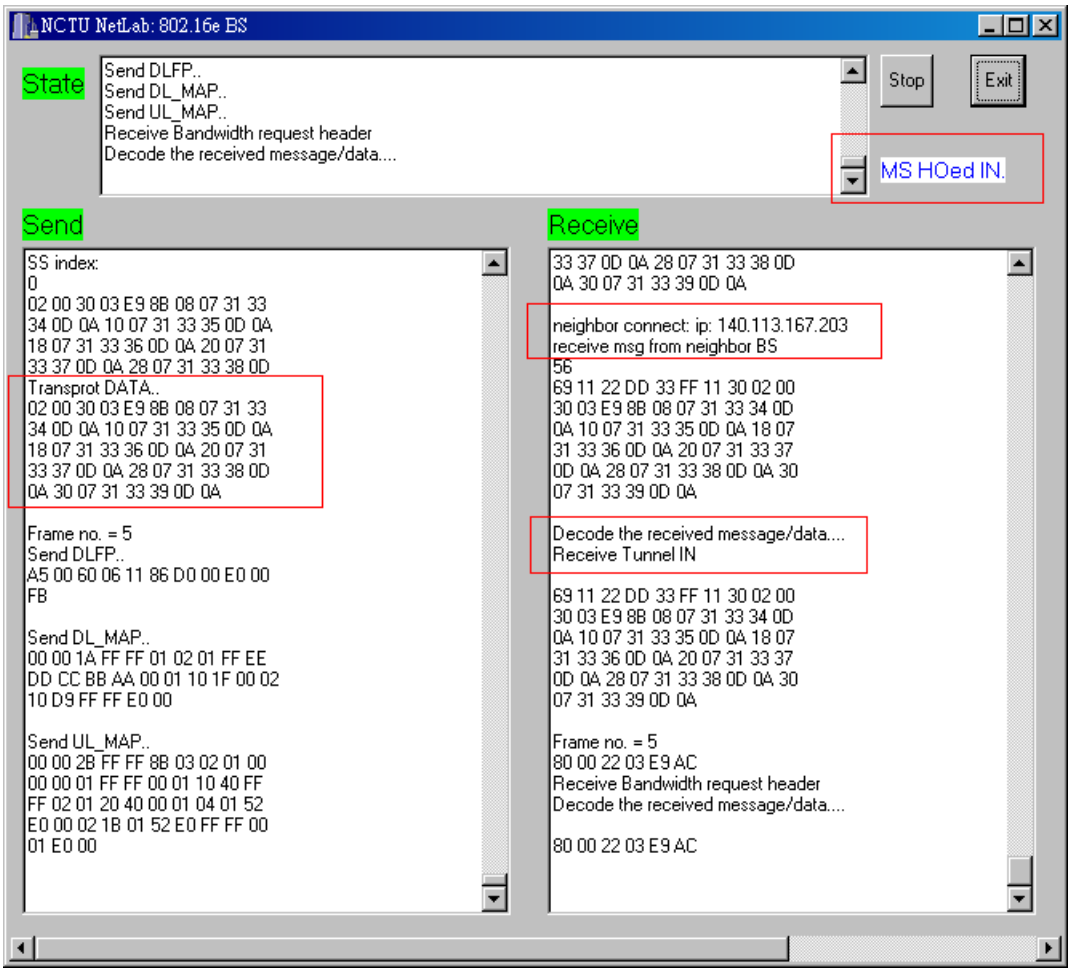


Figure 4.13: Base Station Interface: after handover procedure, Target BS.

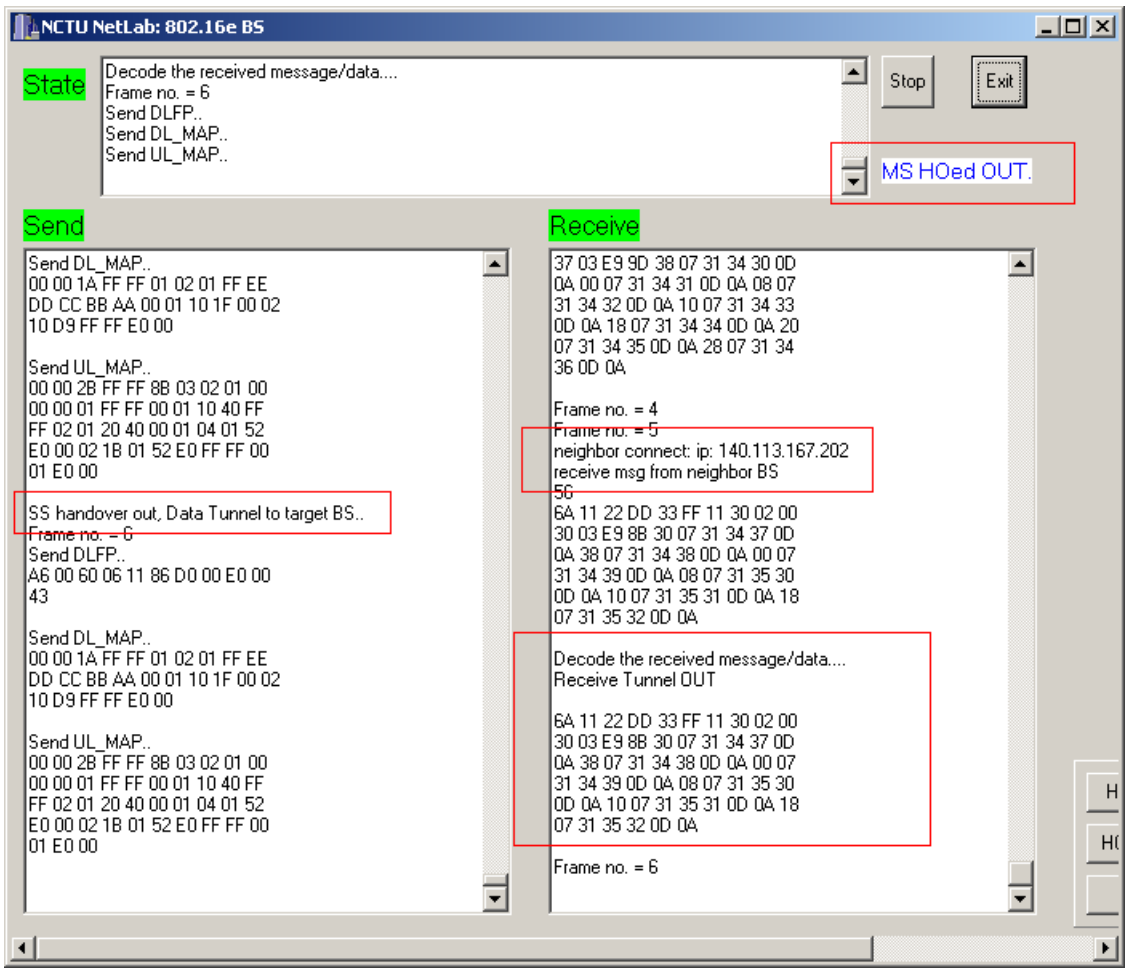


Figure 4.14: Base Station Interface: after handover procedure, original Serving BS.

Chapter 5

Conclusion and Future Works

While the implementation many issues showed up. Some of them may be a further research based on the emulator constructed in this thesis.

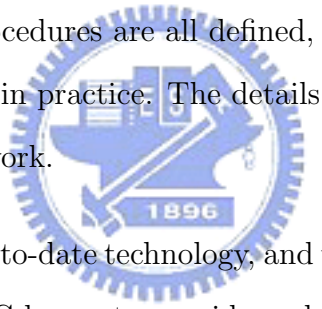
1. Eliminating handover delay: In IEEE standard 802.16e, there are some comments of HO-pre-notification. Since Serving BS is able to communicate with neighbor BSs before handover, the handover procedure can be eliminated by pre-ranging, pre-authentication and pre-registration. With the HO-pre-notification-response, Serving BS will know how many steps in handover procedure can be skipped. These optional functions may be the future work of the proposed emulator.

2. The decision of handover: To decide to perform handover is an abstract concept. Within the proposed emulator we only begin the handover according to the artificial CINR values. But there can be many other factors to trigger handover. Signal strength is the most critical problem for a BS to serve MS, but the available bandwidth is important, too. If MS needs some real-time services, the supports of QoS requirement will be a concern, too. These factors can be gathered to form a weighted function, and the weight of each

factor depends on the purpose of research.

3. The decision of Target BS (Service Level Prediction): As we described in chapter 3, the value of Service Level Prediction is a problem. In the proposed emulator we always give the value represent "acceptable". But if the number of MSs is huge and may cause a problem of load balancing, this parameter is sure to be significant. In fact, the factors to trigger handover are the factors to judge if Serving BS is able to keep on serving. Thus we may get a weighted function as well.

4. The handover mechanisms defined in IEEE standard 802.16e other than general handover: There are other three handover mechanisms defined in IEEE standard 802.16e not being implemented in the proposed emulator yet. Though the procedures are all defined, some of them are still questionable and discussible in practice. The details and issues of these mechanisms may be our future work.



WiMAX is an up-to-date technology, and the latest IEEE standard 802.16e defines the PHY and MAC layers to provide mobility support for WiMAX. Since there is no product based on IEEE standard 802.16e yet, our implementation of IEEE 802.16e emulator is an earlier research to figure out the details of IEEE standard 802.16e.

In chapter 2, we introduce four handover mechanisms defined in IEEE standard 802.16e. We describe the architecture of our implementation of the general handover mechanism emulator in chapter 3. The emulator can be a platform of testing for the development of applications based on IEEE standard 802.16e. The emulator can also be a good teaching material about the procedure of IEEE

standard 802.16d and IEEE standard 802.16e. Though IEEE standard 802.16e amends the PHY and MAC layer for IEEE standard 802.16d to provide mobility support, there are still many issues to be discussed. And those further researches of these issues, whether it is in MAC layer or network layer, can be based on the proposed emulator.

In chapter 3, we also introduce our experience of developing IEEE standard 802.16e emulator. The problems we mention in this thesis will certainly be the problems while constructing the real WiMAX environment. We also do some analysis in chapter 3 to discuss about the evaluation of the proposed emulator. Finally, we hope that this thesis has contribution to further researches in IEEE standard 802.16e.

Appendix A

Network Management Frames

The network layer related structure is not defined in IEEE standard 802.16e. In this appendix we will show our design of Network management frame formats. When knowing MS's longing for handover, Serving BS will send HO-pre-notification to all neighbor BSs as notification. Original BS MAC Address is the MAC address of Serving BS. TCID contains the TCID of MS assigned by Serving BS.

Figure A.1: The format of HO-pre-notification Network management frame.

Neighbor BS will send HO-pre-notification-response to Serving BS as a response of HO-pre-notification. The value of Service Level Prediction represents the measurement whether Neighbor BS is able to accept MS's handover in.

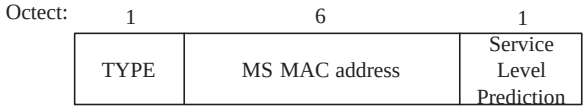


Figure A.2: The format of HO-pre-notification-response Network management frame.

Serving BS will send HO-Confirm to the Target BS selected by Serving BS. Serving BS can make the decision according to signal strengths collected by MS and HO-pre-notification-responses received by Serving BS. Target BS will send HO-Complete to Serving BS after MS complete the Network Re-entry procedure, notifying that MS is ready to continue the data connection.

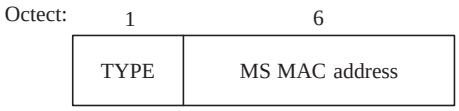


Figure A.3: The format of HO-Confirm and HO-Complete Network management frame.

After handover, the data produced by MS will be tunneled from Target BS to original Serving BS. And the data echoed from Echo Server will be tunneled from original Serving BS to Target BS.

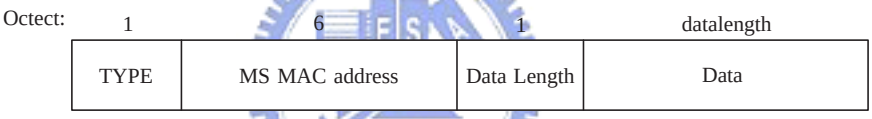


Figure A.4: The format of Data Tunneling Network management frame.

Bibliography

[1] C. Williams, M. Beach, D. Neirynck, A. Nix, K. Chen, K. Morris, D. Kitchener, and M. Presser, "Personal Area Technologies for Internetworked Services", *IEEE Communications Magazine*, Volume 42, Issue 12, Pages:S15-S26, Dec. 2004.

[2] ISO/IEC 8802-11 IEEE Std 802.11 Second edition 2005-08-01, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications (Includes IEEE Std 802.11, 1999 Edition; IEEE Std 802.11a.-1999; IEEE Std 802.11b.-1999; IEEE Std 802.11b.-1999/Cor 1-2001; and IEEE Std 802.11d.-2001)

[3] S. J. Vaughan-Nichols, "Achieving Wireless Broadband with WiMAX", *Journal of Computer*,Volume 37, Issue 6, Pages:10-13, Jun 2004

[4] IEEE 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks–Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[5] IEEE 802.16.2-2004, IEEE Recommended Practice for Local and metropolitan area networks – Coexistence of Fixed Broadband Wireless Access Systems.

[6] IEEE P80216e/D12, Approved Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks–Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems–Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

[7] K. K. Leung, S. Mukherjee and G. E. Rittenhouse, "Mobility Support for IEEE 802.16d Wireless Networks", *Wireless Communications and Networking Conference*, Volume 3, Pages:1446 - 1452, Mar 2005

[8] S. Choi, G.-H. Hwang, T. Kwon, A.-R. Lim and D.-H. Cho, "Fast Handover Scheme for Real-Time Downlink Services in IEEE 802.16e BWA System", *IEEE 61st Vehicular Technology Conference*,Volume 3, Pages:2028 - 2032, June 2005

[9] S. Cho, J. Kwun, C. Park, J.-H. Cheon, O.-S. Lee and K. Kim, "Hard Handoff Scheme Exploiting Uplink and Downlink Signals in IEEE 802.16e Systems", *IEEE 63rd Vehicular Technology Conference*, May 2006

[10] C.-H. Huang and S.-T. Sheu, "Analysis and Implementation of IEEE 802.16 WiMAX System Architecture on Linux Operating System and Software Physical Layer", *Department of Electical Engineering, Tamkang University*, 2004