MPLS-BASED MOBILITY MANAGEMENT FOR WIRELESS CELLULAR NETWORKS

by

KAIDUAN XIE

M.E., Beijing University of Posts and Telecommunications, China, 1996

B.Sc., Hubei University, China, 1993

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE

MASTER OF APPLIED SCIENCE

in

THE FACULTY OF GRADUATE STUDIES

Department of Electrical and Computer Engineering

We accept this thesis as conforming to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

April 2003

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Electrical & Computer Engineering

The University of British Columbia
Vancouver, Canada

Date April. 30. 2003

Abstract

In order to provide full end-to-end IP based service, 3GPP proposes the concept of an IP based access network. Recently, multi-protocol label switching (MPLS) has begun deployment in the Internet backbone to provide traffic engineering. MPLS is also proposed as a transport option in the access network of next generation wireless networks. One of the critical problems associated with mobile networks is mobility management; thus, it is important to handle mobility management in an MPLS based access network.

In this thesis, a domain-based MPLS mobility management scheme for wireless cellular networks, including label switched path setup when the mobile host first powers on and mobile host handoffs, is presented. A medium access control layer assisted packet recovery scheme is proposed to recover packet loss during handoff. In order to reduce the power consumption of the mobile host and signalling load in the access network, a paging server is introduced, which brings in a hierarchical structure in addition to the function of paging. Route optimization is proposed to handle situations when the two communicating parts are in the same domain, thus reducing communication delays and load on the access network. The performance of the MPLS-based mobility management scheme is studied in terms of UDP packet loss and TCP throughput. In addition, the performance of MPLS-based mobility management is compared with three other schemes for IP mobility management, Cellular IP, HAWAII, and Hierarchical Mobile IP.

TABLE OF CONTENTS

List of Tables

List of Figures

Acknowledgments

First of all, I would like to thank my supervisor, Professor Victor Leung for his guidance, advice and support my graduate studies. I feel very lucky that Professor Victor Leung offered me an opportunity to study here. It has also been a privilege and an honor to work under the guidance of my co-supervisor, Professor Vincent Wong. It is through his comments, thoughts and opinions that my research has gradually been crafted and refined.

I wish to express my sincere apologies to my parents, Hehua Song and Shuihai Xie, who live in the remote countryside of China. I could not stay with you during this time, and could not support you as before. Sorry, Dad and Mom.

Last but not least, many thanks to my wife, Lingzhi Liang, for her love, understanding, encouragement and patience, which helped me through this difficult and rewarding time.

Chapter 1 Introduction

The past few years have seen an exponential increase in the use of two kinds of communication services. The first kind is Internet-based data service, such as www, e-mail, and packetized voice. The second is wireless mobile services, particularly circuit-based wireless voice. As the penetration of Internet-based data services increases, more people will demand high speed, wireless, bandwidth data services. Although current widely deployed wireless networks (e.g., GSM, CDMA), can provide short message service (SMS), they cannot meet the ever increasing bandwidth requirements of data services. The intermediate solution to this problem is the general packet radio service (GPRS) [1], because it provides higher speed data service to the end user, and relies on IP for core network transportation. However, the access network still adopts a conventional circuit-based network. The inconsistency between the access network and core network causes many problems. One of these problems is the quality of service (QoS) support across the whole network. In order to fully address these problems, 3GPP proposes the concept of an IP based access network [2][3]. Recently, multi-protocol label switching (MPLS) has begun deployment in the Internet backbone to provide traffic engineering, which cannot be supported by the conventional Internet [4]. MPLS is also proposed as a transport option in the access network of next generation wireless networks [5]. One of the critical problems associated with mobile networks is mobility management; thus, it is important to handle mobility management in an MPLS based access network.

1.1 Motivations and Contributions

There has been a recent proposal to use MPLS in the third generation radio access network (3G RAN) [5]. After examining the QoS requirement in the radio access network, an MPLS based

transport architecture is presented. Two different LSP schemes are examined. The first scheme is a single label switched path between each base station (BS) and radio network controller (RNC), where multiple classes of traffic belonging to a base station are carried in one label switched path. QoS differentiation is provided by packet marking and per-hop behavior forwarding; this can be provided by explicit label switched path (E-LSP), and by allocating bandwidth reservation in the access network per base station. The second scheme involves multiple label switched paths being set up between each base station and radio network controller, where each label switched path carries one class of traffic, that is, label switched paths are class-specific. This can be implemented by label label switched path (L-LSP) and by allocating bandwidth resources in the access network per class. In [5], constraint based routing is used to calculate and set up the label switched path between the base station and radio network controller.

Since mobility management is one of the most important problems in a mobile network, after introducing MPLS into the access network as a transport architecture instead of conventional IP routing, it becomes very natural to ask, "Can MPLS be used to handle mobility management? If so, how?" These are the questions this thesis addresses.

In this thesis, an MPLS-based mobility management scheme for wireless cellular networks is proposed, and its performance then compared with other schemes. Our main contributions are as follows:

- A domain-based MPLS mobility management scheme for wireless cellular networks, including label switched path setup when the mobile host (MH) first powers on and mobile host handoffs, is presented.
- A medium access control (MAC) layer assisted packet recovery scheme is proposed to

recover packet loss during handoff.

- In order to reduce the power consumption of the mobile host and signalling load in the access network, a paging server (PS) is introduced, which brings in a hierarchical structure in addition to the function of paging.
- Route optimization is proposed to handle situations when the two communicating parts are in the same domain, thus reducing communication delays and load on the access network.
- The performance of the MPLS-based mobility management scheme is studied in terms of UDP packet loss and TCP throughput. In addition, the performance of MPLS-based mobility management is compared with three other schemes for IP mobility management, Cellular IP, HAWAII, and Hierarchical Mobile IP.

1.2 Organization

The thesis is organized as follows: in Chapter 2, related work including MPLS, Mobile IP, Hierarchical Mobile IP, Cellular IP and HAWAII, is briefly reviewed. Chapter 3 presents an MPLS-based mobility management scheme including label switched path setup, handoff processing, paging, route optimization and a medium access control layer assisted packet recovery scheme. A qualitative comparison of MPLS-based mobility management, Cellular IP, HAWAII and Hierarchical Mobile IP is also given in Chapter 3. Chapter 4 describes a detailed simulation model design, which includes an MPLS module, label distribution protocol module, mobility management module and a medium access control layer assisted packet recovery module. Simulation results and an analysis are presented in Chapter 5 and compared with Cellular IP, HAWAII and Hierarchical Mobile IP. Finally, Chapter 6 concludes this thesis with a summary and some suggestions for future work.

Chapter 2 Related Work

In this chapter, a general overview of MPLS is given with a focus on its basic principles and advantages as compared with conventional IP routing. Related work on network mobility management is then reviewed. After introducing basic mobile IP, the enhanced hierarchical Mobile IP is illustrated, followed by a discussion of two recently proposed host-based mobility management schemes. Finally, some schemes integrating MPLS and Mobile IP are also introduced.

2.1 Overview of MPLS

In this section, we first introduce the principles of MPLS and the constraint based routing that contributes to MPLS's advantage over conventional IP routing. Then, two promising applications of constraint based routing with MPLS, traffic engineering and fast reroute are illustrated.

2.1.1 What is MPLS?

Originally, MPLS was designed to bring the high efficiency of the ATM switch into IP routers and to provide a uniform way of offering IP services for underlying networks that were not designed for IP service (e.g., ATM, Frame Relay and FDDI). Basically, MPLS [6] can be thought of as an advanced forwarding scheme. In MPLS, each packet is assigned a label. A label is a short, fixed-length entity with no internal structure. Certain link layer technologies, for example, ATM and Frame Relay, can carry labels as part of their link layer header. For other link types that cannot carry labels in the link layer header, MPLS uses a shim header consisting of a stack of 32 bit words. Each entry in the stack contains a 20-bit label, a 3-bit experimental (Exp) field, a 1-bit label stack indicator, and an 8-bit "time to live" (TTL) field. This shim header is inserted between

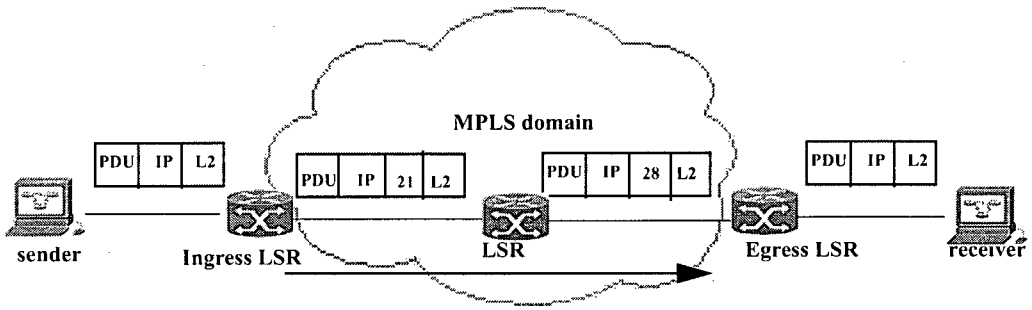


Figure 2.1 MPLS forwarding.

the link layer (L2) and the network layer headers. Packet forwarding is performed by means of label swapping. The label is the only information used to derive a packet's next hop. An MPLS capable router, called the label switching router (LSR), examines the label and possibly the Exp field to forward the packet.

At the ingress label switching routers of an MPLS capable domain, IP packets are classified and forwarded based on the information carried in the IP header of the packets and the local routing information maintained by the label switching routers. The shim header is inserted in the packet. We call this kind of packet a "labeled packet". When a label switching router receives a labeled packet, it extracts the label from the packet and uses it as an index to look up the forwarding table of the label switching router, called the label forwarding information base (LFIB). Each entry in the label forwarding information base consists of an incoming label, and one or more subentries. Each subentry consists of an outgoing label, an outgoing interface, and the next hop address. Then, the incoming label is replaced by the outgoing label and the packet is forwarded onto the outgoing interface to the next label switching router, as designated by the next hop address in label forwarding information base. Before a packet leaves an MPLS domain, this shim

header is removed. The whole process is shown in Figure 2.1. The paths between the ingress label switching routers and the egress label switching routers are called label switched paths (LSPs). Label distribution protocol (LDP) [7] is used to set up label switched paths.

2.1.2 Constraint Based Routing

Many people misunderstand that fast switching and quality of service (QoS) are the two driving factors behind MPLS. In fact, after adopting the high speed application specific integrated circuit (ASIC) chip and fast route look up algorithm [8], conventional IP routing can achieve the same forwarding performance as MPLS. Compared with other usages, such as traffic engineering and virtual private networks, QoS is not a very strong motivator for deploying MPLS. With respect to QoS, the goal has been to establish parity between the QoS features of IP and MPLS, not to make MPLS QoS somehow superior to IP QoS [6][9]. The attraction of MPLS over IP lies in constraint based routing (CBR) [6][10].

The goal of constraint based routing is to compute a route that is subject to constraints such as bandwidth and administrative policy. The key difference between conventional IP routing, such as OSPF [11], IS-IS [12] and constraint based routing is as follows: conventional IP routing algorithms aim to find a path that optimizes a certain scalar metric (e.g., minimizes the number of hops), while constraint based routing aims to find a route that optimizes a certain scalar metric and does not violate a set of constraints at the same time. There are four key components in providing constraint based routing:

- Constraint based routing requires route calculation at the source in such a way that the computation can take into account not just some scalar metric that is used as an optimization criteria, but also a set of constraints that should not be violated. Constrained

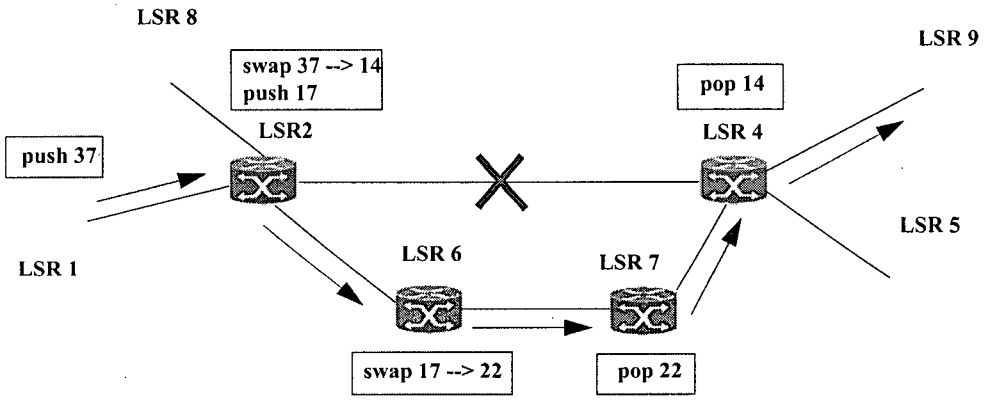
shortest path first (CSPF) algorithm [10] was proposed.

- When a path is determined by the source, forwarding along it cannot be performed using the destination-based forwarding scheme in the conventional IP routing; therefore, some kind of "explicit" routing capability is necessary. To provide this function, MPLS explicit routing is used. There are two reasons for choosing MPLS. One reason is that in MPLS the information used for forwarding (a label) is decoupled from the information carried in the IP header. The other reason is that mapping between the forwarding equivalence class (FEC) and a label switched path is completely confined to the label switching router at the source of the label switched path. In other words, the decision as to which IP packets will take a particular explicit route is completely determined by the label switch router that computes the route. This is precisely the capability that constraint based routing requires.
- In order to set up the explicit route computed by constraint based routing, as well as to reserve resources along that route, some kind of path setup signalling is needed. There are two methods to achieve this: RSVP-extension [13] and constraint-based routing LDP (CR-LDP) [14]. In both schemes, a new kind of object is added, explicit route object (ERO) in RSVP-extension (explicit route in CR-LDP). This object is carried in the PATH message and contains the explicit route that the message will take. The forwarding of such a message by a route is determined not by the destination address in the IP header of the packet that carries the message as in the conventional RSVP, but rather by the content of the ERO carried in the message.
- In order to perform constrained shortest path first algorithm, the node must have information not just about the state (up/down) of all links in a network, but also about vari-

ous link attributes, such as available bandwidth. One solution is to utilize flooding mechanism used by link-state protocols, such as OSPF or IS-IS, and to piggyback the information on top of the link-state information. In order to do that, OSPF and IS-IS extensions are proposed, respectively [15].

2.1.3 Traffic Engineering

Traffic engineering and fast reroute are the two major applications of constraint based routing. Traffic engineering is the process of controlling how traffic flows through a service provider's network so as to optimize resource utilization and network performance [10]. Traffic engineering is needed in the Internet mainly because the shortest path is used in current intra-domain routing protocols (e.g., OSPF, IS-IS) to forward traffic. The shortest path routing may give rise to two problems. First, the shortest paths from different sources overlap at some links, resulting in congestion at those links. Second, at some time, the traffic volume from a source to a destination could exceed the capacity of the shortest path, while a longer path between these two nodes remains under-utilized. The reason why conventional IP routing cannot provide traffic engineering is that it does not take into account the available bandwidth on individual links. For the purpose of traffic engineering, constraint based routing is used to route traffic trunk [16], which is defined as a collection of individual transmission control protocol (TCP), or user datagram protocol (UDP) flows, called "mircoflows" that share two common properties. The first property is that all microflows are forwarded along the same common path. The second property is that they all share the same class of service. By routing at the granularity of traffic trunks, traffic trunks have better scaling properties than routing at the granularity of individual microflows with respect to the amount of forwarding state and the volume of control traffic.



Label stack	LSR1	LSR2	LSR 6	LSR 7	LSR 4
	37	17	22	14	None
		14	14		

Figure 2.2 Fast reroute.

2.1.4 Fast Reroute

In conventional IP routing, when a link or node fails in the network, this information is distributed to all the nodes in the network, and all the nodes then recompute their forwarding tables based on this information. During this transient period, all the packets traversing the failed link/node get dropped. In practice, the time needed to converge within a single OSPF or IS-IS routing domain is in the order of seconds [17]. This limitation is caused by the fundamental nature of conventional IP routing, independent, hop-by-hop, and destination based forwarding. In MPLS, to handle link failure, a protection label switched path, constructed by constraint based routing is configured around a link. When the link fails, the label switching router attached to the failed link uses the label stacking capability of MPLS to "nest" all the label switched paths that are used to go over the failed link into the protection label switched path.

As shown in Figure 2.2, a protection label switched path (LSR 2 -> LSR 6 -> LSR 7 ->

LSR 4) is configured to protect a link (LSR2 -> LSR4). When the link between LSR 2 and LSR 4 fails, the LSR 2 activates a protection label switched path. At LSR 2, by pushing an entry including the outgoing label of 17 in the label stack, the following packets then follow the path (LSR2 -> LSR 6 -> LSR 7 -> LSR 4). Note that when the packet arrives at LSR 4, it carries the same label 14 as when the link (LSR 2 -> LSR 4) is up. From that point on, the fact that the link is down has no impact on the forwarding of the packets to the rest of the label switched path.

2.2 Mobile IP

Mobile IP (MIP) [18] is designed to provide mobility support in the IP layer and to isolate higher layers from terminal mobility. In particular, it aims to keep a continuous TCP connection since TCP connections break after changing IP addresses. In the IP layer, the IP routing mechanism remains unchanged. Two IP addresses are used in Mobile IP. A mobile host (MH) owns an IP home address and is assigned a temporary care-of address (CoA) in the foreign network. A correspondent host (CH) addresses the mobile host via its home address. Mobile IP introduces two elements to the network: home agent (HA) and foreign agent (FA). Routing is performed by address translation and IP-in-IP address tunneling. If a correspondent host wants to send packets to the mobile host, the packets are first delivered to the home address via normal IP forwarding. The home agent intercepts the packets and encapsulates the packets with IP-in-IP tunneling. The foreign agent decapsulates the packets and forwards the packets to the mobile host via normal IP forwarding. In the reverse direction, from mobile host to correspondent host, the packets are forwarded to the correspondent host directly without passing the home agent first. This is called triangular routing. The whole process is illustrated in Figure 2.3

In Mobile IP, the foreign agent periodically broadcasts a Mobile IP advertisement (MIP-

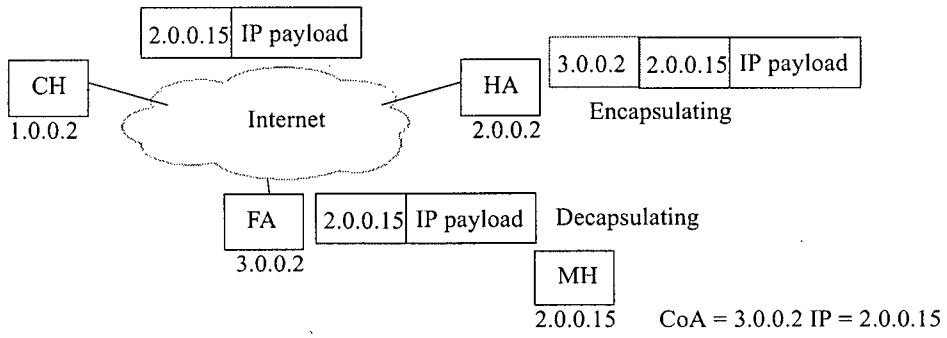


Figure 2.3 Mobile IP packet forwarding.

ADT) message to the mobile host to inform of its presence (step 1 in Figure 2.4). When a mobile host detects that it has moved to a new IP subnet and has obtained a new care of address from the new foreign agent, it registers its new care of address to the new foreign agent via a Mobile IP registration request (MIP-REG-REQUEST) message (step 2 in Figure 2.4). The new foreign agent then relays this registration request to the home agent, where a binding between mobile host's IP home address and the care of address is maintained (step 3 in Figure 2.4). The home agent then sends a Mobile IP registration reply (MIP-REG-REPLY) message to the foreign agent (step 4 in Figure 2.4). The foreign agent relays this message to the mobile host (step 5 in Figure 2.4). The packets subsequently follow this new care of address. Figure 2.4 shows the handoff process.

Although Mobile IP overcomes the problem associated with TCP due to IP address change, it has the following problems. The first is that triangular routing causes packets to drop in the router with ingress filtering configured, since the outgoing and the incoming addresses are different. To overcome this problem, route-optimization [19] is proposed to inform the correspondent host of the mobile host's care of address. Another problem is that when the mobile host is far

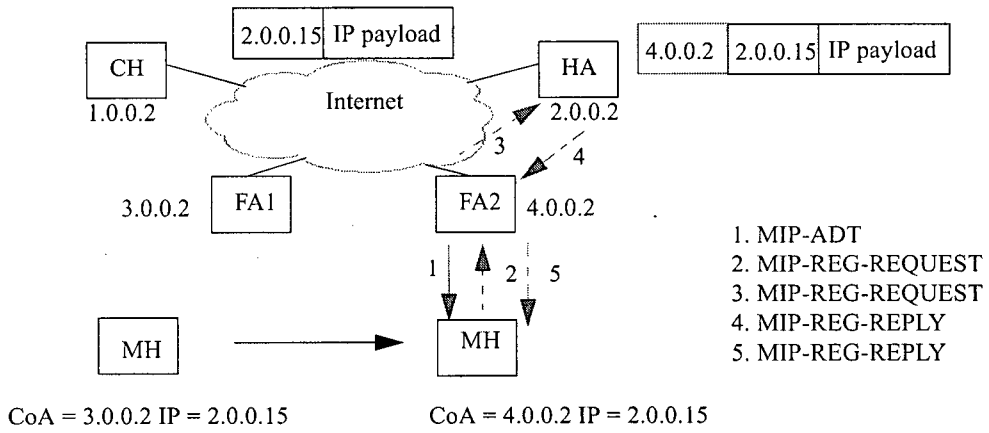


Figure 2.4 Mobile IP handoff.

way from the home agent, the signalling load caused by frequent registration increases dramatically, since every foreign agent change causes a Mobile IP registration, even when the handoff occurs locally. To cope with this problem, hierarchical Mobile IP [20] is proposed.

2.3 Hierarchical Mobile IP

To reduce the signalling load that results from frequent Mobile IP registration message when the mobile host is far away from the home agent, regional registration [20] has been proposed to enhance basic Mobile IP. The basic idea is that hierarchical foreign agents are adopted that allow the mobile host not to send Mobile IP registration message to the home agent each time it changes its point of attachment locally.

When a mobile host first arrives at a visited domain, it performs a Mobile IP home registration, defined as registration with its home agent. During a home registration, the home agent registers the care of address of the mobile host. When the visited domain supports regional registration, the care of address registered with the home agent is the publicly routable address of

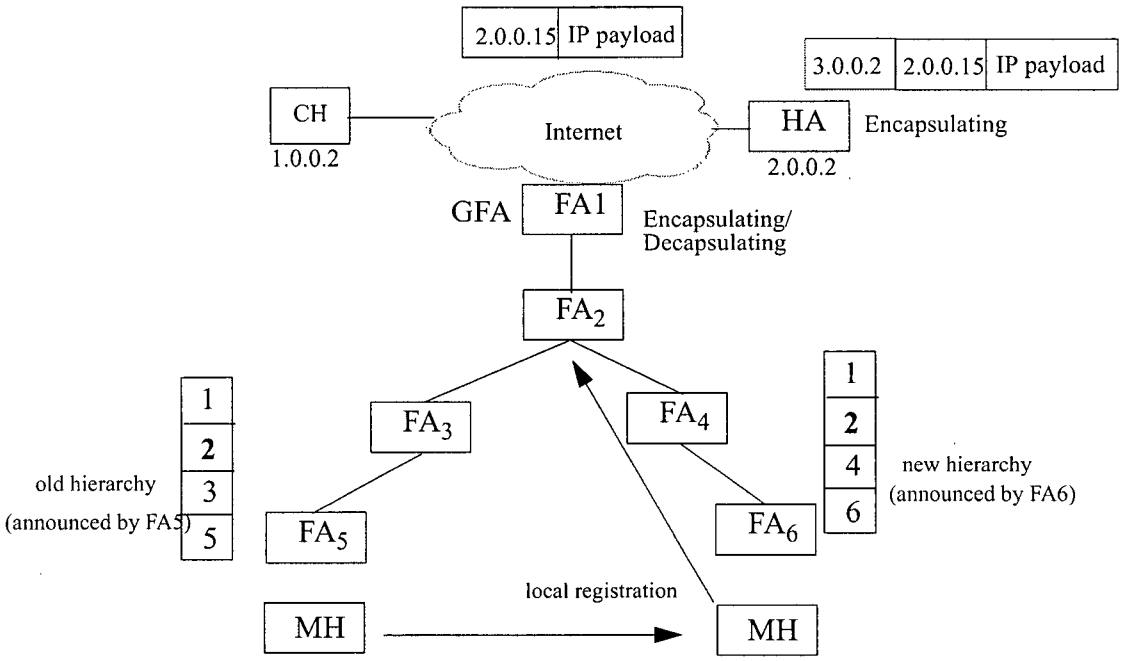


Figure 2.5 Hierarchical Mobile IP local registration.

a gateway foreign agent (GFA). This care of address does not change when the mobile host changes foreign agents under the same gateway foreign agent. When changing gateway foreign agent, a mobile host must perform a home registration. When changing foreign agent under the same gateway foreign agent, the mobile host may instead perform a regional registration within the visited domain. In the same gateway foreign agent, a hierarchical model is used. On each level, a regional foreign agent (RFA) is introduced. The lowest level regional foreign agent announces the hierarchy of regional foreign agents in its Mobile IP advertisement message. From this advertisement message, the mobile host knows where it should send the local registration. Figure 2.5 illustrates the hierarchical Mobile IP regional registration, where the mobile host moves from FA_5 to FA_6, and the local registration message is sent to FA_2.

When a correspondent host sends packets to the mobile host, the packets are first be routed to the home agent. The home agent tunnels them to the gateway foreign agent. The gateway foreign agent de-capsulates the packets, encapsulates them again and then sends the packets to the next regional foreign agent. The regional foreign agent en route to the mobile host applies the same process, decapsulating and encapsulating the packets. The lowest level regional foreign agent just de-capsulates the packets and forwards them to the mobile host via normal IP routing.

2.4 Cellular IP

Currently, Mobile IP does not support certain features, such as seamless handoff, passive connectivity and paging. These features are essential to current 2G wireless networks [21]. Borrowing these ideas from second generation cellular networks, Campell *et al.* proposes Cellular IP [22][23][24] to provide local mobility and handoff support.

Cellular IP assumes that the mobile host moves in a local area most of the time. The network model of Cellular IP is divided in two parts: the core network and the Cellular IP wireless access network. The core network (Internet) is supposed to work with classical Mobile IP. The wireless access network uses Cellular IP. The mobility of a user that is moving from one access network to another is managed by Mobile IP. Cellular IP handles the user's movements inside each access network. Each access network is connected to the Internet via a gateway router (GW). A mobile host located in an access network uses the IP address of the gateway as the Mobile IP's care of address.

In Cellular IP, routing is performed on a host-based instead of prefix-based method in current Internet, where network address and subnet-mask are used for routing [25]. The node in the access network maintains two different location information databases: *routing cache* and

paging cache. Normally, the *routing cache* is used to route the packet. When there is no entry for the destination in the *routing cache*, the *paging cache* is used instead. In Cellular IP, the gateway periodically broadcasts a beacon packet that is flooded in the access network. The base station (BS) records the neighbor it last received this beacon from, and uses it to route uplink packets towards the gateway. All uplink packets transmitted by the mobile host, regardless of their destination address are first routed towards the gateway using these routes. The uplink data packet is first used to update or refresh the passing node's *routing cache* and *paging cache* and is then forwarded to the node's uplink neighbor. Packets destined for the mobile host are routed along the reverse path via the *routing caches* and *paging caches* via a specialized algorithm [22].

Cellular IP supports two kinds of handoff processing: *hard handoff* and *semi-soft handoff*. *Hard handoff* is based on a simple approach that trades off some packet loss for minimizing handoff signaling and handoff delay, rather than trying to guarantee zero packet loss. *Semi-soft handoff* utilizes the fact that a mobile host can listen to/receive two base stations simultaneously in some kinds of wireless network, for example, CDMA system and wireless LANs. In *hard handoff*, a mobile host listens to the periodical beacon signal emitted by the base stations. It can thus detect the point at which handoff occurs. At this point, the mobile host sends a *route update* message to the new base station. Upon receiving the *route update* message, each node en route to the gateway first decides whether the downlink neighbor via which the *route update* message arrives is the same as the routing entry for the mobile host. If the two are not the same, the node updates the routing entry for the mobile host in the *routing cache/paging cache* and sends the *route update* message to the uplink neighbor to the gateway. If the two are the same, the node does not send the *route update* message to the uplink neighbor. The routing entry for the mobile host in the nodes which the packet to or from the mobile host does not traverse by eventually times out

and is removed automatically. The handoff latency is the time the *route update* message takes to arrive at the cross over node, which is defined as the first common node between the new and old path from the mobile host to the gateway (the gateway itself in the worst case). All packets destined for the mobile host that pass through the crossover node during this latency time are lost.

In order to minimize packet losses, Cellular IP also defines a new handoff mechanism called *semi-soft handoff* that exploits the nature that mobile host can listen to two base stations simultaneously for a short duration. The idea is that the network installs a routing entry in *routing cache/paging cache* before the regular handoff happens. Upon receiving the beacon signal from the new base station, the mobile host sends a *semi-soft* packet to the new base station and immediately returns to the old base station. After a fixed time, called *semi-soft delay*, it performs a regular handoff. During this delay, the *semi-soft* packet triggers the establishment of new routing/paging cache mapping on all nodes between the new base station and gateway. When the mobile host eventually hands off to the new base station, the packets are delivered through both the old and new base stations to the mobile host.

Delivering the packets through the two base stations ensures minimal packet losses, but this may cause a synchronization problem. The packet streams transmitted through the two base stations are unsynchronized due to the different delay between the path from the cross over node to the old base station, and the path from the cross over node to the new base station. If the stream transmitted by the new base station lags behind the old base station, the mobile host receives duplicated packets. This does not disrupt many applications. However, if the stream of the new base station is ahead of the old base station, the mobile host loses some packets at the moment of handoff. This loss makes the *semi-soft* handoff completely ineffective. To solve this problem,

Cellular IP requires that the crossover node be equipped with a delay device mechanism, since this node knows that a *semi-soft* handoff is in progress and can introduce an additional delay for the packets delivered on the new path until it receives the *route update* message that terminates the handoff. The problem is solved if the delay device provides a sufficient delay to compensate for the advance of the new stream.

Cellular IP supports paging implicitly. The mobile host transmits *paging update* packet to the gateway at regular intervals defined by *paging-update-time* while it is idle. When IP packets destined for a mobile host for which no up-to-date routing information is available arrive at the gateway, the *paging cache* is used to find the mobile host. The gateway queues the IP packets as they arrive and generates a control packet, called *paging packet* (the first data packet destined for the mobile host can also serve as the *paging packet*). The *paging packet* is routed in the access network by *paging caches* that simply reverse the route taken by recent *paging-update* packets. If some nodes do not have *paging cache*, then they broadcast the *paging packet* to all downlink ports. After the mobile host receives the *paging packet*, it sends a *route-update* to the gateway, thus installing a routing entry in *routing cache* in the nodes/base station on the way to the gateway. All the following packets route via the *routing cache* just established. *Paging cache* and *routing cache* have the same format and operation, except that *paging cache* mapping has a longer time-out value.

In Cellular IP, the location information stored in the *routing cache* and *paging cache* is associated with a timer called the *soft-state* timer. There are five kinds of timers: routing update timer, routing update time-out timer, paging update timer, paging update time-out timer, and active state timer.

2.5 HAWAII

HAWAII [26][27][28][29] stands for *Handoff Aware Wireless Access Internet Infrastructure*. In HAWAII, the mobile host retains its network address while moving within a domain. The home agent and correspondent host are unaware of the host's mobility in the domain. Routes to the mobile host are established by specialized path setup schemes that update the forwarding tables with host-based entries in selected routers in that domain. Like Cellular IP, HAWAII resorts to Mobile IP for inter-domain mobility. HAWAII aims at providing micro-mobility features, such as fast handoff, passive connectivity, paging, and QoS.

In HAWAII, the domain is composed of base stations and normal IP routers with extended capabilities. All nodes (base stations and IP routers) maintain a number of soft-state routing entries to efficiently forward the packets destined for the mobile host that moves in that domain. The nodes are organized hierarchically. At the top of this hierarchy, the domain root router (DRR) acts as a gateway towards the global Internet. When the mobile host connects to a base station, it is assigned a co-located care of address via dynamic host configuration protocol (DHCP) [26]. This address remains unchanged while the mobile host moves in the same domain.

HAWAII defines two schemes for handoff processing, *forwarding path setup* and *non-forwarding path setup*. When the mobile host detects a change of base station via a Mobile IP advertisement message, it must issue a Mobile IP registration request to the base station. HAWAII uses this registration to trigger HAWAII path setup schemes inside the domain. In *forwarding path setup* schemes, *packets are first forwarded from the old base station to the new base station before they are diverted at the crossover router* (the first common router in the path between the old base station and the domain root router, and the path leading from the new base station to the

old base station). The authors in [26] propose two variants, *Multiple Stream Forwarding (MSF)*

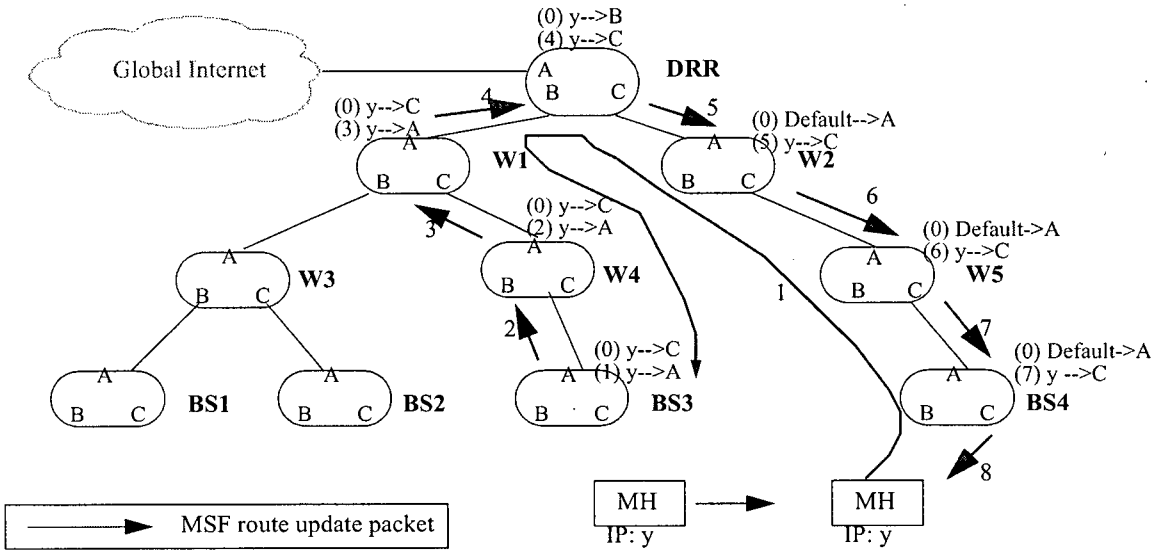


Figure 2.6 HAWAII MSF.

and *Single Stream Forwarding (SSF)*. Due to space limits, we only illustrate MSF. As shown in Figure 2.6, the forwarding table entries are shown adjacent to the routers. These entries are pre-appended with a message number, such as 1, indicating which message is responsible for establishing which entry (a message number of zero indicates a pre-existing entry). Letters such as "A" denote different interfaces. The mobile host sends a Mobile IP registration request message to the new base station (this message contains the old base station's address). The new base station then sends a *HAWAII path setup* message directly to the old base station. After receiving such a message, the old base station adds a forwarding entry for the mobile host in its routing table and sends this message to the next router on the path to the new base station. Each router on the path to the new base station adds or updates a forwarding entry for the mobile host and then forwards the message hop-by-hop to the next router. When the message eventually arrives at the

new base station, the new base station sends a Mobile IP registration reply to the mobile host.

Note that this order of updating the routers can lead to the creation of multiple streams of mis-ordered packets arriving at the mobile host. For example, during transient periods newer packets forwarded by the domain root router may arrive at the mobile host before the old packets forwarded by router W1, which may in turn arrive before even older packets forwarded by W4. The creation of multiple streams during handoff can affect both UDP and TCP applications. Also, this scheme may result in the creation of transient routing loops (for example, after the old base station has changed its entry to forward packets but before router W4 has processed message 2). However, note that mis-ordered streams and routing loops exist only for an extremely short period of time. The main benefit of this scheme is that it is simple and results in no packet loss.

In *non-forwarding path setup* schemes, as the path setup message travels from the new base station to the old base station, *data packets are diverted at the crossover routers to the new base station, resulting in no forwarding of packets from the old base station.* There are two variants, *Unicast Non-Forwarding (UNF) and Multicast Non-Forwarding (MNF).* Due to space limits, we only illustrate UNF. When handoff occurs, the mobile host sends a Mobile IP registration request message to the *new base station.* The new base station adds a forwarding entry for the mobile host and sends a path setup message to the next router on the path to the old base station. Every router on the path to the old base station applies the same process. Eventually the path setup message arrives at the old base station. The old base station then sends an acknowledgement for the path setup message to the new base station. The new base station then sends a Mobile IP registration reply to the mobile host. UNF is optimized for networks where the mobile host can listen to two base stations simultaneously for a short duration, for example, CDMA or Wireless

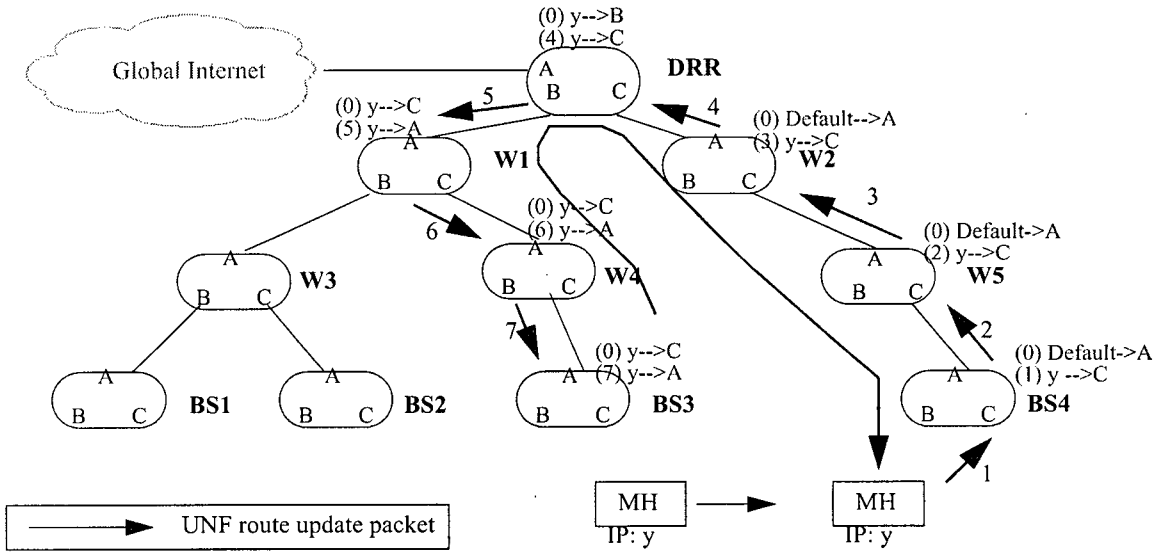


Figure 2.7 HAWAII UNF.

LANs. Figure 2.7 shows the whole process.

Unlike Cellular IP, HAWAII adopts explicit paging [29]. HAWAII resorts to classical IP multicast routing to implement this feature. HAWAII assumes that some paging areas have been defined inside each domain. The mobile host is able to detect that it is in a given paging area and the time it changes paging area. Each of these paging areas corresponds to IP multicast groups (i.e. all the nodes in a paging area are members of the same IP multicast group) and classical IP multicast routing is used to perform effective paging. HAWAII identifies the paging area by an IP multicast group address. Paging is eventually initiated by a router if it receives a packet for a mobile host for which it has no routing entry. The router first buffers the packets and sends a paging request to the multicast group corresponding to the paging area of the mobile host. The request is then forwarded to each member of the group, ultimately a set of base stations. Finally, the request arrives at the mobile host. The mobile host acknowledges the request to the initiator of

the paging. This reply is routed hop-by-hop to the concerned node and triggers the update or addition of routing entries by the routers on its path.

2.6 MPLS-based Mobility Management Schemes

An architecture integrating MPLS and Mobile IP which obviates the necessity for IP-in-IP tunneling is proposed in [30]. Linux based implementation shows that the main benefit of combining MPLS and Mobile IP is improved packet forwarding speed. As mentioned before, after introducing the high speed ASIC chip and fast route look up algorithm [8], conventional IP forwarding can achieve the same performance as that of MPLS; therefore, in the future, this would not be an advantage over IP in IP tunneling.

Basic label switched path setup and handoff processing for MPLS based micro-mobility management are proposed in [31]. This scheme divides the networks into domains. For each domain there is an MPLS-capable router acting as a gateway to the outside and as the mobility management agent for the mobile hosts in the domain. For Diff-Serv, each base station has a pre-configured label switched path to and from the gateway. When a mobile host first powers on, it uses a specialized label switched path called a signalling label switched path to convey the registration information to the gateway that sets up a label switched path for the mobile host. When the mobile host hands off to another base station, the mobile host sends a route update message to the gateway that changes the label switched path for the mobile host. The label switched path for the mobile host is associated with the label switched path from the gateway to the serving base station where the mobile host resides. For Inter-Serv, the RSVP is used to set up the label switched path for the flow. Each label switched path is set up dynamically, whereas a static label switched path is used in Diff-Serv. When the mobile host hands off to another base

station, the mobile host sends an RSVP reservation message to the gateway. For each intermediate label switched router en route to the gateway, if there is a corresponding entry for the flow, it changes the label mapping for the flow and does not forward the message to the gateway. If there is no entry for the flow, it changes the label mapping for the flow and continue forwarding the message to the gateway. In thesis, there are some questions to be further studied. First, the accurate message format is not given. In fact, Mobile IP message with minor modifications can be used to convey the route update and registration message since Mobile IP is a standard mechanism that will be implemented in the mobile host and base station. Second, there is no hierarchy in the domain. Every cell boundary crossing results in a route update message to the gateway. Third, paging is not discussed, which has been proved to be an effective way to reduce power consumption and signalling load in the access network. Fourth, the case when two communicating parts are in the same domain is not studied. Finally, there is no information on how the RSVP message arrives at the mobile host in the Inter-Serv model. This is the key factor for providing the Inter-Serv service.

In [32], an enhanced label edge router called the label edge mobility agent (LEMA) is proposed to create a hierarchical overlay network above the access network. The access router connecting the access point to the IP network is the lowest layer LEMA. The localized mobility of a mobile host is handled by an appropriately chosen LEMA. In fact, the architecture looks like a hierarchical MPLS-based mobility management as hierarchical Mobile IP. For each mobile host, a chain of hierarchical LEMAs is used to handle mobility management and packet forwarding. New registrations are required only when the reachability chain is broken due to mobility. In order to reduce packet loss, *redirect* message is send to the old serving LEMA. The authors in [32] pointed out that the most attractive property of this architecture is that the mobile host has the flexibility to

create its own hierarchy of LEMAs, more accurately, the chain of LEMAs based on its mobility pattern, the bandwidth availability in the network and other factors. However, it is very difficult to implement this in a real life network. When handoff occurs how does the mobile host know to which LEMA it should send the registration message? This is because the beacon signal from the access point cannot accommodate the information with regard to the customized hierarchy of LEMA for each mobile host. As in the case of [31], paging and route optimization are not discussed. In [32], a qualitative comparison among other schemes, for example, Cellular IP, HAWAII and hierarchical Mobile IP is given. However, no quantitative comparison among those schemes is presented. We discuss these problems in our proposed MPLS-based mobility management in the next chapter.

In order to overcome the shortcoming of previous MPLS-based micro-mobility management, we propose an enhanced MPLS-based micro-mobility management scheme [33][34]. In our scheme, besides the basic label switched path setup and handoff processing, we propose hierarchy and paging, route optimization and a medium access control layer assisted packet recovery scheme. We also compare the performance of our enhanced MPLS-based micro-mobility management with Cellular IP, HAWAII and HFA via simulation.

Chapter 3 MPLS-based Micro-Mobility Management

In this chapter, we illustrate how to support micro-mobility management in MPLS-based wireless access networks. First, we discuss the basic label switched path setup, packet forwarding and handoff processing in Section 3.1. Following that discussion, the concepts of paging and hierarchy are introduced in Section 3.2. Route optimization, which is used to handle the scenario where two communicating parts are in the same domain, is discussed in Section 3.3. Medium access control layer assisted packet recovery is proposed in Section 3.4. Finally, a qualitative comparison among MPLS-based micro-mobility management and the other three schemes, Cellular IP, HAWAII and HFA, are presented in Section 3.5.

3.1 Label Switched Path (LSP) Setup

In our proposed framework, the *Mobile IP registration* protocol is used to set up a label switched path (LSP) for the mobile host. The network is divided into domains. In each domain there is an MPLS capable router acting as the gateway (GW) to the outside network. With respect to mobility management, the gateway acts as the home agent for the mobile hosts, and handles the mobility management for the mobile hosts in the domain. With respect to packet forwarding, the gateway acts as an egress label switched router and an ingress label switched router at the same time. When the mobile host moves in the same domain, its IP address does not change. The first problem is how to set up the label switched path for the mobile host after powering on. As shown in Figure 3.1, the base station periodically broadcasts the *Mobile IP advertisement* message to all mobile hosts. Upon receiving the *Mobile IP advertisement* message, the mobile host sends a *Mobile IP registration request* as a reply (step 1 in Figure 3.1). From this *Mobile IP registration request* message, the base station can determine whether the mobile host is powered on, and

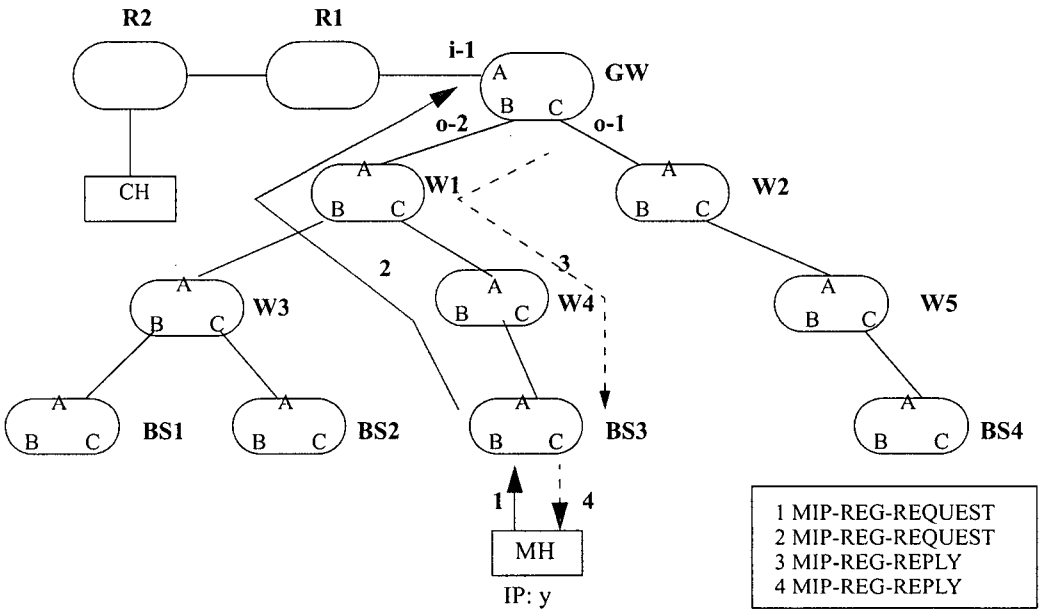


Figure 3.1 Registration process.

Table 3.1LFIB after registration.

I/F	I/L	FEC	O/F	O/L	S	Timer	Node	Note
A	i-1	y	-	-	1	-	GW	R2-->GW
-	-	BS3	B	o-2	0	-	GW	GW-->BS3
-	-	y	B	o-2	0	*Ta*	GW	GW-->MH

whether the mobile host is in its home domain. If the mobile host is in its home domain, the base station sends a *Mobile IP registration request* message to the gateway (step 2 in Figure 3.1). The gateway creates a label switched path entry for the mobile host in its label forwarding information base. It places the mobile host's address on the forwarding equivalence class field of the label switched path entry for the mobile host's serving base station. The gateway then sends a *Mobile IP registration reply* message to the base station that relays this message to the mobile host (steps 3 and 4 in Figure 3.1). In this case, in the downlink direction, there are two label switched path segments for the mobile host. One is from the correspondent host's label switched router to the

gateway. The other is from the gateway to the mobile host's serving base station. In the uplink direction, all packets from the mobile host travel to the gateway first, and are then forwarded to the destination. The label distribution protocol [7] can be used to establish the label switched paths. We assume that the label switched path between the correspondent host and the home agent/gateway and the label switched path between the gateway and base station are pre-configured via label distribution protocol. In Figure 3.1, all the intermediate nodes (e.g., R1, W1, GW, and BS1) are assumed to be MPLS capable routers. The label information for the mobile host in label forwarding information base of related node is shown in the Table 3.1. The notations used in Table 3.1 are as follows: I/F: Incoming interFace; I/L: Incoming Label; O/F: Outgoing interFace; O/L: Outgoing Label; S: *Segmented* flag. The *segmented* flag (with a value of 1 or 0) is used to indicate the need for further label forwarding information base lookup for packet forwarding. In our architecture, we use the active timer T_a to decide whether or not the mobile host is active (i.e., transmitting or receiving data packets). Each incoming or outgoing data packet refreshes the timer T_a. When the timer expires, the network assumes the mobile host is in "idle" state, and removes the label switched path entry for this user in the label forwarding information bases.

3.2 Packet Forwarding

If a correspondent host wants to communicate with the mobile host, the packets are transmitted via the pre-configured label switched path between the correspondent host's label switched router and the mobile host's home agent. The home agent knows whether there is another label switched path segment for the mobile host via checking the *segmented* flag in the label forwarding information base. If the value of the *segmented* flag is 1, after stripping the label and obtaining the destination address, the home agent selects a label switched path for the mobile

host using the destination address as an index. All packets destined for the mobile host use this label switched path to reach the mobile host's serving base station via the normal label forwarding scheme. If the mobile host has roamed to another domain, the foreign gateway performs the same procedure described above. Finally, the packets arrive at the mobile host's serving base station. The base station relays the packets to the mobile host via wireless channel.

From the above description, there are three label switched path segments between the correspondent host and the mobile host: the correspondent host's label switched router to home agent, home agent to foreign gateway, and foreign gateway to the mobile host's serving base station. For the outgoing direction, data packets follow the path to the gateway and are then forwarded to the destination via normal label swapping scheme.

3.3 Handoff

As in Mobile IP, the base station periodically sends the *Mobile IP advertisement* message to the mobile host. The mobile host replies with a *Mobile IP registration request* (step 1 in Figure 3.2). When a mobile host hands off from one base station to another within the same domain, the new base station informs the gateway via the *Mobile IP registration request* message (step 2 in Figure 3.2). The new BS also sends a *handoff-notification* (A special kind of *Mobile IP registration request* message that does not need to be acknowledged.) to the old base station so that the old base station can forward packets for the mobile host to the new base station (step 3 in Figure 3.2). Upon receiving the *Mobile IP registration request* message, the gateway updates the entry for the mobile host in its label forwarding information base. It places the mobile host's address on the forwarding equivalence class column of the entry for the new base station, and sends a *Mobile IP registration reply* (step 4 in Figure 3.2). The new base station then sends a *Mobile IP registra-*

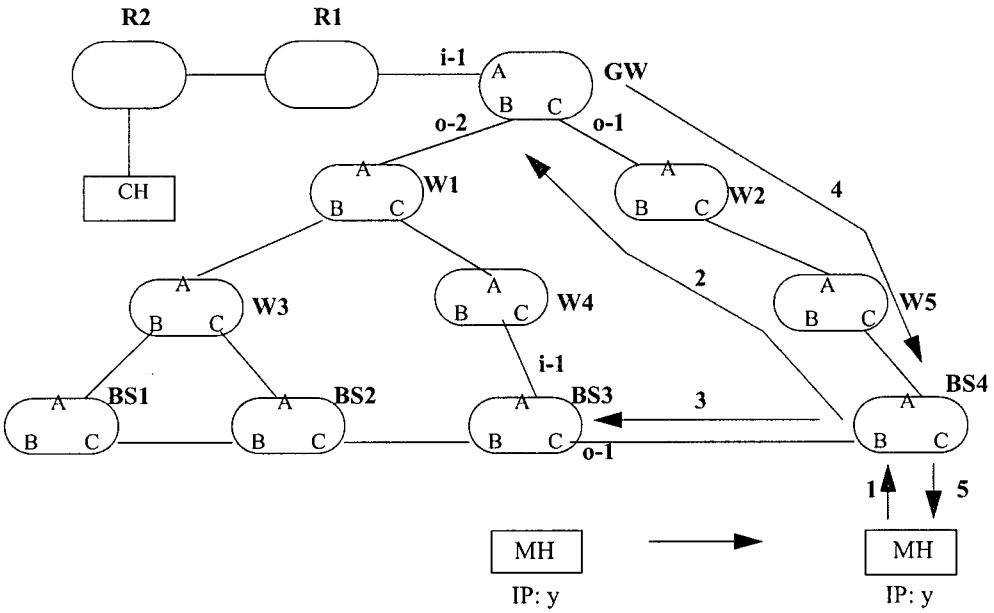


Figure 3.2 Handoff process.

Table 3.2 LFIB after handoff.

I/F	I/L	FEC	O/F	O/L	S	Timer	Node	Note
A	i-1	y	-	-	1	-	GW	R2-->GW
-	-	BS4	C	o-1	0	-	GW	GW-->BS4
-	-	y	C	o-1	0	*Ta*	GW	GW-->MH
A	i-1	BS3	-	-	1	-	BS3	GW-->BS3
-	-	BS4	C	o-1	0	-	BS3	BS3-->BS4
-	-	y	C	o-1	0	*Ta*	BS3	BS3-->MH

tion reply message to the mobile host (step 5 in Figure 3.2). Upon receiving the *handoff-notification* message from the new base station, the old base station adds a label switched path entry in label forwarding information base for the mobile host by including the mobile host's address to the forwarding equivalence class column of the label switched path entry for the new base station and starts the active timer T_a. At the same time, the old base station sets the *segmented* flag to 1 in

the entry for the label switched path from the gateway to itself. From this point on, the old base station diverts packets destined for the mobile host to the new base station on the appropriate label switched path until the timer T_a expires. The handoff process is illustrated in Figure 3.2. The label forwarding information base in the associated nodes is shown in Table 3.2.

3.4 Paging

From the above description, for every handoff the mobile host sends a *Mobile IP registration request* to the gateway no matter how close the two neighboring base stations are. This is not effective when the covering area of the gateway is large. To overcome this shortcoming, an extra level of hierarchy is introduced. At the same time, in order to reduce the power consumption of mobile hosts and the signalling load in the access network, which is caused by frequent registrations, which are in turn caused by handoffs, we propose to employ paging in MPLS-based micro-mobility management architecture. The wireless access network domain is divided into different paging areas. We assume that there is a paging server (PS) in each paging area. After introducing paging server, the gateway only maintains the location information of that mobile host in the granularity of a paging area.

When an idle mobile host crosses a paging boundary, it sends a *Mobile IP registration request* message to the gateway to report its current paging area. When an idle mobile host crosses a cell boundary, but stays within the same paging area, it does not need to send a *Mobile IP registration request* message to the paging server to report its location. When a mobile host is in its active state, upon every cell boundary crossing, the mobile host sends a *Mobile IP registration request* message to the paging server. The paging server knows whether or not the mobile host has moved to another paging server from this *Mobile IP registration request* message. If this

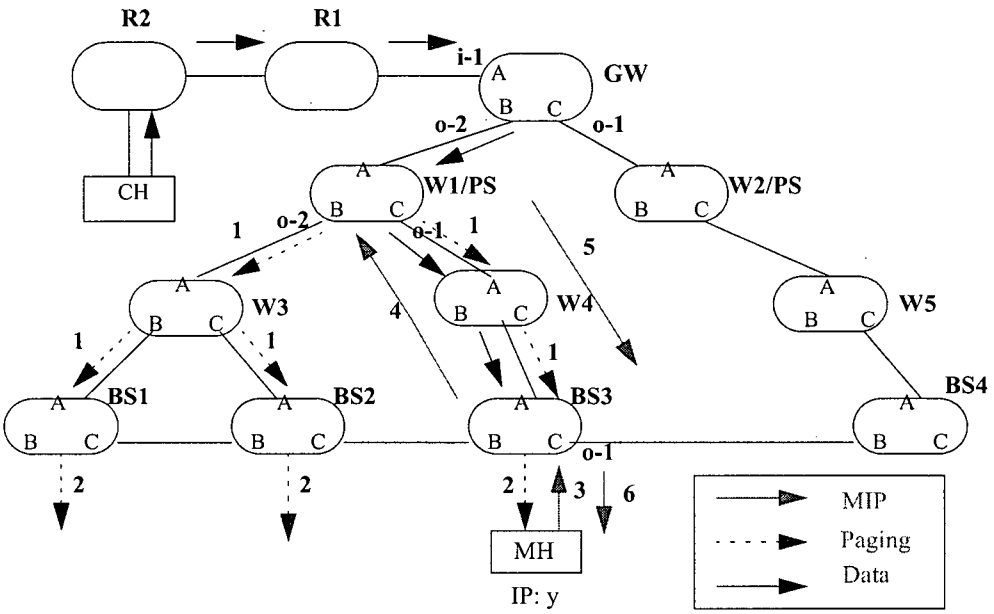


Figure 3.3 Paging process.

Table 3.3 LFIB with paging.

I/F	I/L	FEC	O/F	O/L	S	Timer	Node	Note
A	i-1	y	-	-	1	-	GW	R2-->GW
A	o-2	W1	-	-	1	-	W1	GW-->W1
-	-	BS3	C	o-1	0	-	W1	W1-->BS3
-	-	y	C	o-1	0	*Ta*	W1	W1-->MH

movement spans two paging servers, the paging server sends a *Mobile IP registration request* message to the gateway to report this handoff. The gateway updates the routing entry for the mobile host in its label forwarding information base. In this way, we introduce an extra level of hierarchy after adopting the paging server.

When a mobile host is in its active state, in the forward path (from the gateway to the mobile host), incoming packets destined for the mobile host are intercepted by the gateway. The

gateway then forwards those packets to the corresponding paging server. The paging server forwards those packets to the mobile host's serving base station. In the reverse path (from the mobile host to the gateway), outgoing packets are sent to the paging server first. The paging server then forwards those packets to the gateway. The gateway forwards those packets to the appropriate destinations.

When a mobile host is in its idle state, the paging server buffers all the incoming packets corresponding to that mobile host and sends a *paging request* to all base stations within its paging area via multicast (step 1 in Figure 3.3). Those base stations then send a layer 2 (link layer) *paging request* via wireless channel (step 2 in Figure 3.3). Upon receiving the *paging request*, the mobile host sends a *Mobile IP registration request* message to the base station (step 3 in Figure 3.3). The base station sends a *Mobile IP registration request* message to the paging server (step 4 in Figure 3.3). Finally, the paging server installs a label switched path entry for the mobile host. The whole process is illustrated in Figure 3.3. The associated label forwarding information base is shown in Table 3.3.

3.5 Route Optimization

In the MPLS-based IP micro-mobility scheme described above, all packets from a mobile host are routed to the destination via the gateway regardless of whether the destination is in the same domain or not. Normally, when a mobile host moves to another domain, most of the traffic is exchanged with the hosts in the same domain. In order to reduce the load of the gateway and shorten the latency, when the mobile host communicates with a correspondent host in the same domain, the traffic should not traverse the gateway. We define this as *route optimization.*

When a mobile host wants to send packets to a correspondent host, the first packet uses the

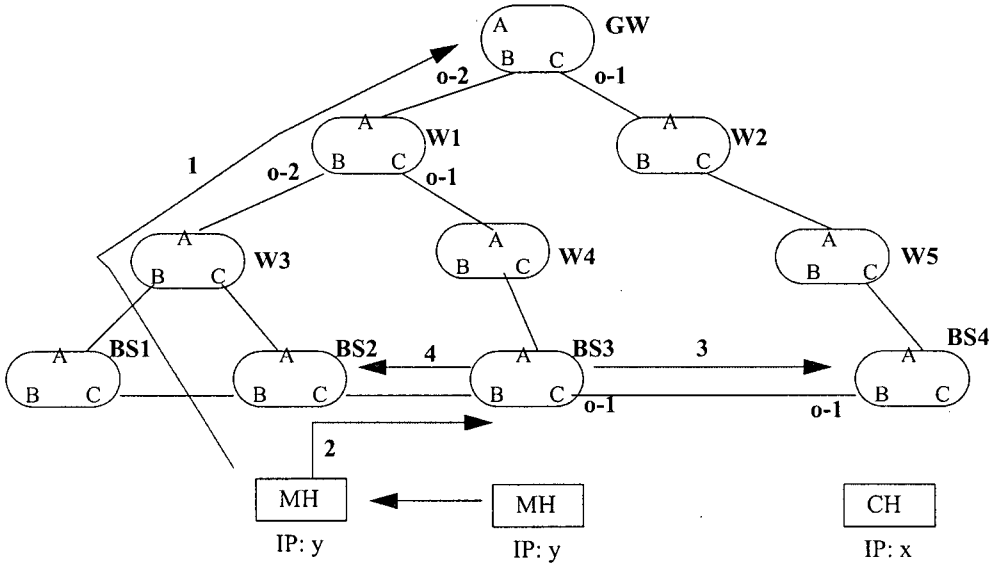


Figure 3.4 Route optimization.

Table 3.4 LFIB after route optimization.

I/F	I/L	FEC	O/F	O/L	S	Timer	Node	Note
-	-	GW	A	o-2	0	-	BS3	BS3-->GW
-	-	BS4	C	o-1	0	-	BS3	BS3-->BS4
-	-	CH	C	o-1	1	*Ta*	BS3	BS3-->CH
-	-	BS3	B	o-1	0	-	BS4	BS4-->BS3
-	-	MH	B	o-1	0	*Ta*	BS4	BS4-->MH

default label switched path from the serving base station to the gateway to reach the gateway. The gateway then strips the label and uses the destination address in the IP header as an index to look up the label forwarding information base. If the destination is also in the label forwarding information base, it means that the correspondent host is in the same domain as the mobile host. The gateway then informs the mobile host's serving base station of the base station serving the correspondent host (assuming it is also mobile) by means of *route-notification message.* At the same time, the gateway also sends a *route-notification* message to the correspondent host's

serving base station to identify the base station serving the mobile host.

Upon receiving the gateway's *route-notification*, the mobile host's serving base station puts the correspondent host's address in the forwarding equivalence class column of the label switched path entry for the correspondent host's serving base station in its label forwarding information base and starts the associated active timer T_a. Subsequently, all packets follow the label switched path between the base stations serving the mobile host and the correspondent host. The same updating process takes place at the label forwarding information base of the base station serving the correspondent host. For example, in Figure 3.4, the mobile host served by BS3 wants to communicate with the correspondent host served by BS4. After the *route optimization* process, the relevant label switched path entries in the label forwarding information base in BS3 and BS4 are shown in Table 3.4, respectively.

While the above method facilitates *route optimization*, it leads to a problem in refreshing the location information of the mobile host and correspondent host in the gateway. With *route optimization*, packets between the correspondent host and mobile host no longer traverse the gateway, thus no information is available to refresh the location state in the gateway. This results in a possible inconsistency between the mobile host's state in the gateway and the actual state of the mobile host, and the possibility of unnecessary paging events. One possible solution to this problem is to have the mobile host/correspondent host periodically sends a *route-refresh* message to the gateway to refresh its state when the mobile host/correspondent host is in active state as designated by the T_a timer. This keeps the state in the gateway consistent with the actual state of the mobile host/correspondent host while minimizing the access network's traffic load due to refreshing.

Another problem is how to maintain *route optimization* after a handoff. When the mobile host hands off to a new base station during its active state, the new base station needs to be informed about the base station serving the correspondent host, and vice versa. The following four steps ensure that *route-optimization* is maintained after a handoff. First, the mobile host sends a route-update message to inform the gateway of the new base station serving the mobile host (step 1 in Figure 3.4). Second, the mobile host notifies the old base station about the new base station (step 2 in Figure 3.4). Third, the old base station notifies each correspondent host's serving base station of the mobile host's new base station, so that each correspondent host's serving base station can install a path from the correspondent host to the mobile host by adding the mobile host's address to the forwarding equivalence class column of the forwarding entry for the mobile host's new base station (step 3 in Figure 3.4). Fourth, the old base station notifies the new base station of each correspondent host's serving base station so that the new base station can install a path from the mobile host to each correspondent host by adding the correspondent host's address to the forwarding equivalence class column of the forwarding entry for the correspondent host's serving base station (step 4 in Figure 3.4).

3.6 Packet Loss Recovery

In Section 3.3, when a handoff occurs, the new base station informs the old base station so that the old base station can set up a label swtiched path for the mobile host. Subsequent packets follow this path to the new base station that relays them to the mobile host. However, before the old base station receives the *handoff notification* message from the new base station, the packets destined for the mobile host still take the path to the mobile host via the old base station. Unfortunately, the mobile host has been moved to the new base station, so these packets eventually lose on wireless channel. Depending on the network topology and the wireless network capability,

these dropped packets due to handoff may decrease the application's performance. In order to minimize packet loss due to handoff, two different methods are used as described below.

3.6.1 Buffer Time-based Packet Recovery

This method was first proposed by Campbell *et al*, in [35]. It works as follows. In each base station, there is a buffer. During handoff, all the incoming packets destined for the mobile host are buffered at the old base station. The old base station also stamps each packet the instant the packet arrives. After receiving the *handoff notification* from the new base station, the old base station uses the *buffering time* T_b to decide which packets should be forwarded to the new base station. If the elapsed time between the arrival instant and the current time is smaller or equal to T_b, the packet is forwarded to the new base station. Otherwise, it is discarded. The whole process is illustrated in Figure 3.5. At time t1, the packet p1 arrives at the old base station. This packet is the last packet received by the mobile host from the old base station before handoff to the new base station. All the following packets, p2, p3, and p4 are lost since the mobile host has already moved to the new base station. At time t3, the new base station sends a *handoff notification* message to the old base station. At time t4, the old base station receives the *handoff notification* message and forwards the packets in the buffer to the new base station by applying the buffer time based method. Finally, those packets arrive at the mobile host at time t6.

The optimal T_b causing zero packet loss is equal to the sum of the second layer handoff time and the link delay between the old and new base stations. Since it is difficult to estimate the optimal T_b for each handoff, a sub-optimal value is used, 1/2 $T_{beacon.}$ T_{beacon} is the interval at which the base station emits the beacon signal to mobile hosts.

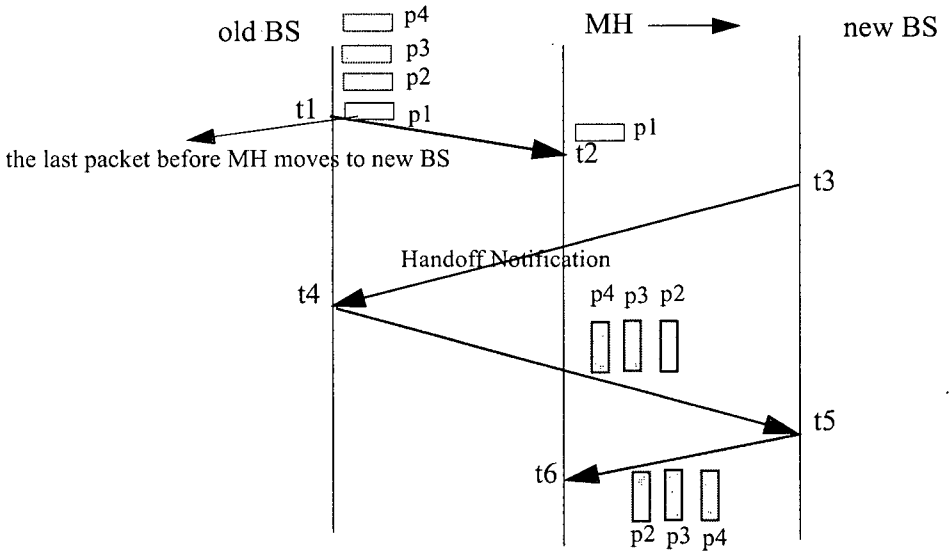


Figure 3.5 Buffer time based packet recovery.

3.6.2 MAC Layer Assisted Packet Recovery

In wireless networks, such as GPRS and Wireless LANs, automatic retransmission is used to counteract the error-prone wireless channel to improve transmission reliability. The medium access control (MAC) layer in Wireless LAN [36] uses Request To Send (RTS), Clear To Send (CTS), DATA, and Acknowledgement (ACK) for data exchange. The MAC layer uses the RTS control frame and a short CTS frame to reserve access to the channel. After data transmission, the ACK frame confirms the success of the transmission. In this way, the MAC layer maintains information about which frames have been successfully delivered.

Our proposed MAC layer assisted packet recovery scheme is designed to prevent packet loss due to handoff. In general, packet loss during handoff is caused by the broken or deteriorated wireless connection between the old base station and the mobile host. In our proposed scheme, a buffer in the MAC layer is used to cache the packets dropped by the MAC layer. These packets

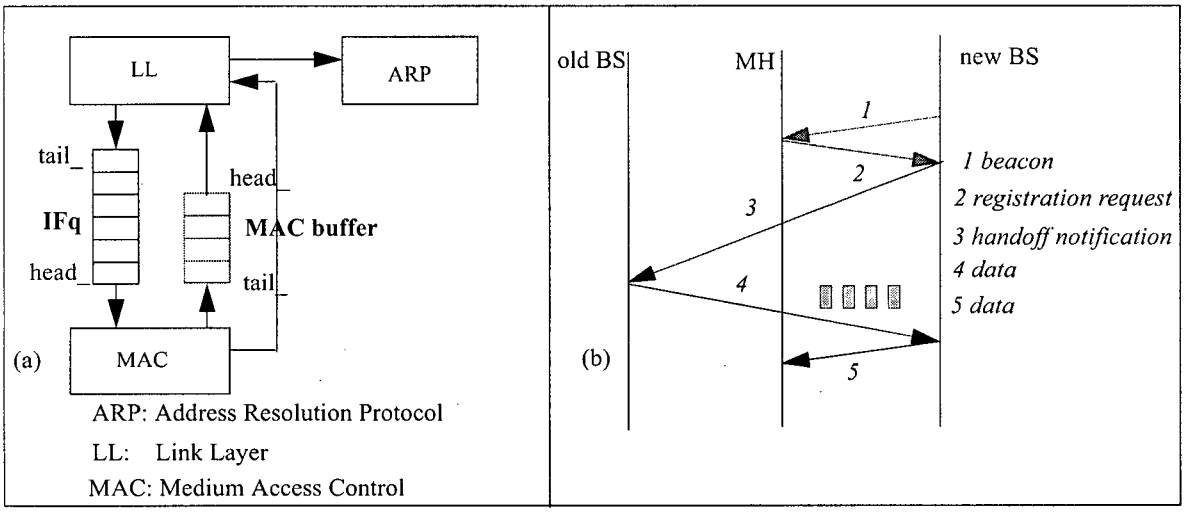


Figure 3.6 MAC assisted packet recovery.

are then transmitted from the old base station to the new base station.

The MAC layer assisted packet recovery procedure is illustrated in Figure 3.6 (a). IP packets are passed from the network layer down to the link layer (LL). Within the LL module, a MAC layer frame is constructed from an IP packet by adding the appropriate MAC layer header and trailer. The MAC layer frame is then placed in the interface queue IFq for transmission. The MAC module in Figure 3.6 (a) is responsible for channel access (i.e., RTS/CTS/DATA/ACK). If a particular frame transmission is not successful after a certain number of times, this frame is then placed in the MAC buffer.

After receiving a *handoff notification* from the new base station, the old base station forwards those frames in the MAC buffer corresponding to that mobile host to the new base station via the pre-condfigured label switched path. After that, those frames in the IFq buffer corresponding to that mobile host are also forwarded to the new base station. Note that all mobile hosts within the coverage of the same base station share the MAC buffer. The base station uses the

mobile host's MAC address carried in the *handoff notification* to identify which packets belong to the corresponding mobile host. Accordingly, we can eliminate packet loss due to handoff, and thus improve application performance. The MAC layer assisted packet recovery process is illustrated in Figure 3.6 (b).

3.7 Qualitative Comparison with Other IP Mobility Managements

In this section, we compare the different IP mobility management schemes from the following perspectives: registration, paging support, support of traffic inside the same network, QoS and traffic engineering support, reliability, packet recovery, and deployment consideration. We call the schemes in [31], [32] basic MPLS mobility management and LEMA, respectively. Our scheme is referred to as enhanced MPLS mobility management [33][34].

- **Registration**: Mobile IP, or its extension is used in enhanced MPLS mobility management, HFA and HAWAII, while Cellular IP uses its own proprietary protocol. There is no specific information with regard to whether or not Mobile IP is used in basic MPLS mobility management and LEMA.
- **Location Information Create or Refresh**: In enhanced MPLS mobility management, label switched path setup is control-driven. Data packets originating from or destined to the mobile host are used to refresh the label switched path for the mobile host. In HAWAII and HFA, location information for the mobile host is created and refreshed by control packets. In Cellular IP, location information for the mobile host is created by data packets and refreshed by data or control packets. The authors in [31][32] did not mention how to refresh the location information associated with the mobile host in basic MPLS mobility management and LEMA.

- **Paging Support**: In enhanced MPLS mobility management and HAWAII, explicit paging is adopted. When the mobile host is in its idle state, a paging packet is sent by the related node (the paging server in the enhanced MPLS mobility management, the selected node in HAWAII). While in Cellular IP, paging is performed in an implicit way. The paging cache is used to route the packet. In basic HFA, no paging is supported. There is a proposal to introduce paging in Mobile IP [37][38], which also adopts explicit paging. There is no information regarding paging in basic MPLS mobility management and LEMA.
- **Traffic inside the Domain:** Enhanced MPLS mobility management and Cellular IP apply *route optimization* [39] to handle when two communicating parts are in the same domain. However, since HFA and HAWAII work on classic IP routing, this kind of traffic definitely benefits from classical IP routing. No special schemes are required. No schemes are proposed to handle the scenario where traffic is inside the domain in basic MPLS mobility management and LEMA.
- **QoS Support**: Enhanced MPLS mobility management relies on QoS support with MPLS, such as Diff-Serv and Inter-Serv support by MPLS. HFA and HAWAII can provide IP based QoS since it works on classical IP routing. However, there is no inherent support for QoS in Cellular IP. Basic MPLS mobility management and LEMA can also provide QoS support since this is the capability of MPLS.
- **Traffic Engineering**: Enhanced MPLS mobility management can use constraint based routing to provide traffic engineering. Traffic trunk is used to collect a group of traffic with the same requirement to prevent some parts of the network from being over-utilized, while other parts of the network are under-utilized. HFA and HAWAII cannot

support traffic engineering since conventional IP routing cannot provide traffic engineering. In Cellular IP, supporting traffic engineering is more difficult. Basic MPLS mobility management and LEMA can also provide traffic engineering since this is the capability of MPLS.

- **Reliability**: Constraint based routing based fast reroute can be used to protect link or node failure in enhanced MPLS mobility management. HFA and HAWAII rely on the underlying IP capabilities, for example, the OSPF/IS-IS protocol to distribute the link information and re-compute the path, which is much slower than fast-reroute. In Cellular IP, no special schemes are used. The network has to rely on the periodic beacon signal transmitted by the gateway and the routing refresh sent by the mobile host. Basic MPLS mobility management and LEMA have the same capability as our scheme.
- **Packet Recovery**: MAC assisted packet recovery is proposed to eliminate packet loss due to handoff in enhanced MPLS mobility management. In Cellular IP, semi-soft handoff with delay device is proposed to cope with packet loss due to handoff. However, it is very difficult to estimate the accurate value of the delay. In HAWAII, UNF can utilize the mobile host's capability to listen to the neighboring base stations simultaneously for a while to provide better service. In HFA, basic MPLS mobility management and LEMA, no special methods are designed to reduce packet loss.
- **Deployment Requirements**: Only the gateway and paging servers need to be retrofitted to support mobility management, provided that all nodes in the domain are MPLS capable routers in enhanced MPLS mobility management. In HFA, only the gateway foreign agent and regional foreign agent need to be retrofitted. While in HAWAII and Cellular IP, all nodes in the domain need to be retrofitted to support mobility manage-

ment. In basic MPLS mobility management, only the gateway needs to be upgraded. For LEMA, some nodes in the access network should be upgraded to configure LEMA capable software. However, as mentioned in Section 2.5 of Chapter 2, in a real life network, it is difficult to implement customized LEMA chain for each mobile host based on the mobility pattern of the mobile host, the available bandwidth and other factors. Table 3.5 summarizes the overall comparison.

Table 3.5 IP mobility management: A qualitative comparison.

	Enhanced MPLS-based	**HFA [20]**	**Cellular IP [22]**	**HAWAII [26]**	**Basic MPLS-based [31]**	**LEMA [32]**
Registration	Mobile IP	Mobile IP	proprietary	Mobile IP	not specified	not specified
Location create/refresh	control packet/data packet	control packet/control packet	data packet/ control, data packet	control packet/control packet	not specified	not specified
Paging Support	explicit	no	implicit	explicit	no	no
Traffic inside the domain	route optimization	IP based	route optimization	IP based	no	no
QoS Support	MPLS based	IP based	no	IP based	MPLS based	MPLS based
Traffic Engineering	CBR based	no	no	no	CBR based	CBR based
Reliability	fast reroute	inter-domain routing based	simple	inter-domain routing based	fast reroute	fast reroute
Packet Recovery	MAC assisted	no	semi-soft + delay device	UNF	no	no
Deployment Requirement	GW, PS	GW	every node	every node	GW	some nodes

For a more comprehensive comparion among IP based mobility management schemes (not including MPLS based), please refer to [35][40][41][42].

Chapter 4 Simulation Model

In order to investigate the performance of our proposed MPLS-based mobility management, a simulation environment based on ns-2 is designed. In this chapter, following the overview of ns-2 in Section 4.1, the design principles and the internal structure of the MPLS module are provided in Section 4.2. In Section 4.3, the mobility management module is illustrated. In Section 4.4, we first analyze the internal structure of the mobile node and the process of an IP packet. We then present the design of the MAC layer assisted packet recovery module.

4.1 Overview of ns-2

The *ns* network simulator [43] is an event driven simulator for computer networks and network protocol research. Since it has been widely used in the research community, a large number of network components is available for ns. NS is chosen as the simulation tool for several reasons. First, it is a modular, open, and free software. Second, there is a contributed module Columbia IP Micro-mobility Software (CIMS) from Columbia University [44] that compares the performance among Cellular IP, HAWAII and HFA. These three architectures are the most popular proposals for IP micro-mobility management in Internet Engineering Task Force (IETF) communities. We plan to compare the MPLS-based micro-mobility with these three proposals.

The ns-2 simulator uses a split-language programming approach. OTCL, an object-oriented version of Tool Command Language (TCL) is used for the scheduling of events and the dynamic configuration of network topology, components and parameters for the simulation. The actual core of the simulator (i.e., low level event processing, scheduling, packet forwarding and protocol implementation, such as TCP) is written in C++ to allow for fast simulation of large scenarios. The original design principle for ns-2 is that most simulations just involve the changing

of simulation parameters in the TCL space without changing the C++ source code. In the past, this has been true since ns-2 was designed for the study of TCP, mostly on the impact of TCP throughput with different parameter values, such as window size, round trip time (RTT) value, and so forth. However, as more network research is carried on ns-2, changing only the parameter is not sufficient, and C++ programming work is unavoidable.

In our research, we need to investigate the performance of MPLS-based mirco-mobility management, and compare it with three other popular schemes. In order to simulate the MPLS-based micro-mobility management we proposed, the following modules are necessary: Mobile IP, MPLS packet forwarding, Wireless LAN, and MPLS-based micro-mobility management. However, in current ns-2, the MPLS module [45] from Gaeil Ahn only supports flat address format and works in TCL space. Hierarchical address such as the one currently used in IP network is a prerequisite for Mobile IP simulation; therefore a totally new MPLS module is redesigned in this thesis. Moreover, MPLS-based mirco-mobility management module should be implemented on the basis of MPLS. Furthermore, in order to study the improvement in performance with MAC layer assisted packet recovery, a MAC assisted packet recovery module is designed.

4.2 MPLS Module

MPLS module consists of two submodules, the LDP module and the packet forwarding module. The LDP module takes care of the label switched path setup via LDP in LDP request and LDP mapping messages. The label switched path setup is performed in the downstream control-driven way [7]. The packet forwarding module is responsible for the real packet forwarding, in other words, label pre-appending and label swapping.

In ns-2, a node consists of agents and classifiers. An agent is the sender and receiver

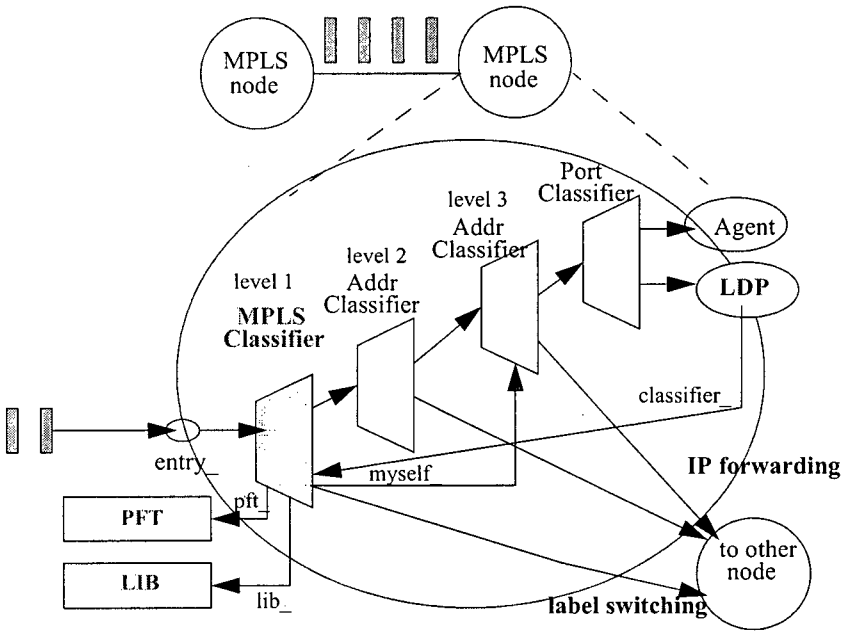


Figure 4.1 Classifier structure of MPLS node.

object of a protocol, and a classifier is the object that takes care of the packet classification required for forwarding packets to the next node. In order to simulate an MPLS node, *the MPLS Classifier* and *LDP agent* are added into the normal ns node.

Figure 4.1 shows the classifier structure of the MPLS node in our simulator. *Node entry* points to the entry point for the node. This is the first element that handles the packets arriving at the node. The *entry_* points to the *MPLS Classifier* that first classifies the incoming packet into labeled or unlabeled one. For an unlabeled packet, it is processed in the conventional way by *Addr Classifier* (i.e., IP forwarding is executed). For a labeled packet, the *MPLS Classifier* is responsible for label swapping. *Addr Classifier* is responsible for packet forwarding based on the IP destination, and the *Port Classifier* is responsible for agent selection.

On receiving a packet, an MPLS node operates as follows. *MPLS Classifier* determines

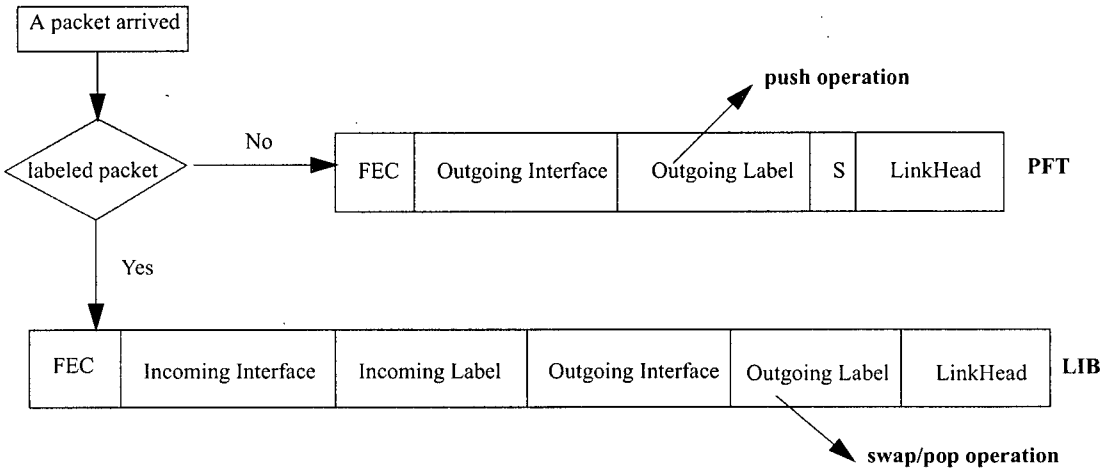
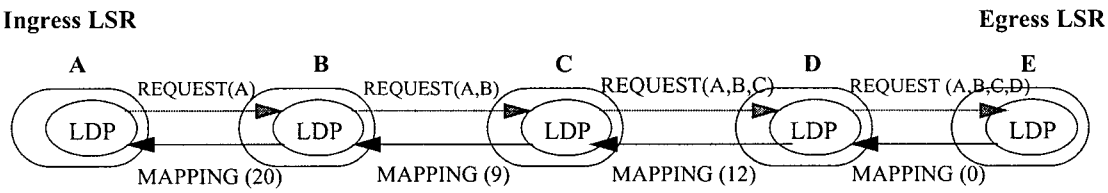


Figure 4.2 PFT and LIB structure in MPLS node.

whether or not the received packet is labeled. If the packet is a labeled one, label switching is executed to send the packet directly to the next node. If the packet is not a labeled one and there is a label switched path for this packet, a label is be pre-appended to the packet. Afterwards, label switching is performed as labeled packet forwarding. Otherwise, *MPLS Classifier* passes it to *Addr Classifier*. *Addr Classifier* performs IP forwarding by examining the packet's IP destination address. If the next hop of the packet is itself, *Port Classifier* takes care of sending the packet to the corresponding agent.

An MPLS node has two tables for managing information related to the label switched path: *Partial Forwarding Table* (PFT) and *Label Information Base* (LIB). The PFT contains the FEC, outgoing interface and outgoing label. The PFT is used to find the label for the destination packet. The PFT is searched for an unlabeled packet. The LIB contains the information for each LSP. Figure 4.2 shows the structure of these two tables and the simple algorithm for forwarding packets.

When a packet arrives at an MPLS node, lookup of the PFT/LIB is performed. If the packet is an unlabeled packet, the PFT is searched with the packet's FEC (packet's destination address) as the index. If an entry exists for the FEC, the MPLS node performs a *label push* operation for the packet. Otherwise, the packet is classified by *AddrClassifier*. Note that the actual packet delivery to the next node is performed by passing the packet to the *LinkHead,* that is, the head of the link between this node and the next hop. If the packet is a labeled one, the MPLS node searches the LIB to find the outgoing label with the incoming label as the index, performs the label swapping that replaces the packet's incoming label with an outgoing label, and decreases the TTL value. If the outgoing label is zero, which means the packet is destined for itself, *label pop* is performed instead of *label swapping*, and the packet is passed to the classifier *myself.*



LSP: 20------> 9-------> 12---->0

Figure 4.3 LDP agent.

The operation of an LDP agent is illustrated in Figure 4.3. For example, if node A wants to set up a label switched path to node E, the LDP agent in node A sends an LDP-REQUEST message to node B, which is the next hop on the path to node E. At the same time, node A puts its address on the *path vector* in the REQUEST message, which is used to route the returning LDP-MAPPING message so that the MAPPING message takes the same path as the REQUEST message. All intermediate nodes on the path to D apply the same process, filling its address in the *path vector* and sending the LDP-REQUEST to the next hop to the destination. Destination E

knows that it is the egress label switching router for this label switched path. Node E allocates an incoming label 0, puts the label in the LDP-MAPPING message, and sends the message to the next hop to the source via the *path vector.* After receiving the LDP-MAPPING message, node D allocates an incoming label (12 for this label switched path), uses the label in the LDP-MAPPING message as the outgoing label, and binds the incoming label with an outgoing label in its LIB. All intermediate nodes on the path to the source, ingress label switching router, apply the same process as D. Node A, the ingress label switching router, installs an entry in its PFT for this label switched path after receiving the LDP-MAPPING message. From the above description, we can see that the *down-stream localized* label allocation scheme [7] is used to set up the LSP.

4.3 MPLS-based Micro-Mobility Management Implementation

In order to support MPLS-based micro-mobility management, a special module called *MMAgent* is designed to handle the mobility management. Each MPLS node configures this kind of agent. In the base station and mobile host, the existing *MIPBSAgent* and *MIPMHAgent* are modified to handle the MPLS related mobility management. Figure 4.4 shows the relationship between the *MIPBSAgent*, *MIPMHAgent* and *MMAgent.*

After introducing the paging server, two fields for the old paging server and new paging server are added in the Mobile IP message. The *MIPBSAgent* broadcasts a *Mobile IP advertisement* message to advertise its address, and the paging server's address which it belongs to, at a preconfigurable time interval. The *MIPMHAgent* stores the addresses of the base stations within range in a list associated with an expiration timer. When no *Mobile IP advertisement* of a registered base station is received for a certain amount of time, the expiration timer times out, and the associated entry is removed from the list. If the mobile host receives a *Mobile IP advertise-*

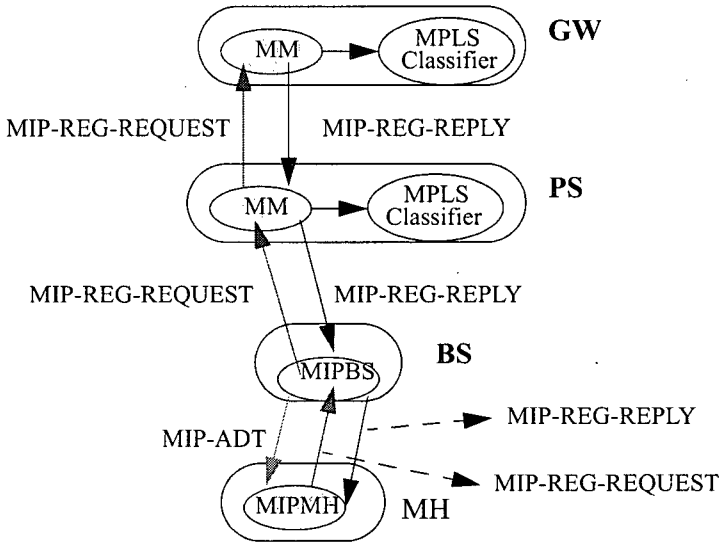


Figure 4.4 MM, MIPBS and MIPMH agent illustration.

ment message from a base station which is on the list, the value of the corresponding expiration timer is adjusted. If the base station is not on the list, a new entry is created. The mobile host then sends a *Mobile IP registration request* message to the base station. From this message, the base station determines that the mobile host has handed off to it, and then relays the *Mobile IP registration request* message to the paging server and gateway. The paging server and gateway perform the corresponding processing.

When there is no entry in the list (e.g., when the mobile host powers up for the first time), the mobile host broadcasts a *Mobile IP solicitation* message. Upon receiving the *Mobile IP solicitation*, the base station sends a *Mobile IP advertisement.* The mobile host replies with a *Mobile IP registration request*. From this message, the base station knows that the mobile host has just powered on, and relays the *Mobile IP registration request* message to the paging server and gateway. The paging server and gateway performs corresponding processing.

The *MMAgent* directly communicates with each other and with the *MIPBSAgent* to handle mobility related functions, such as mobile host power up, mobile host registration request, mobile host registration reply, and mobile host handoff. In each node, the *MMAgent* also communicates with the *MPLS Classifier* to add and update the PFT/LIB entry for the mobile host in PFT/LIB. In addition, after introducing the paging server, the *MMAgent* also decides whether the mobile host moved to another paging server. If the mobile host moved in the same paging server, the *MMAgent* does not forward the *Mobile IP registration request* message to the gateway. Otherwise, the *MMAgent* in the paging server forwards the *Mobile IP registration request* message to the gateway.

4.4 MAC Layer Assisted Packet Recovery

In order to exploit the MAC acknowledgement information to recover the dropped packets due to handoff, we must first understand how a packet is processed in the base station and in the mobile host. The node structure of a base station and a mobile host is shown in Figure 4.5.

- NOAH agent: In ns-2, a wireless node contains an ad-hoc routing agent to communicate with other wireless nodes. However, in Mobile IP, a mobile host always uses foreign agent (i.e., base station) as the intermediate gateway to the other nodes in the Internet. A new routing agent, a Non-Ad-Hoc routing agent (NOAH) [46], is designed for this purpose. After introducing this agent, the base station acts as the gateway for the mobile host to communicate with other nodes. NOAH is also the default target for the base station and mobile host node.
- Packet processing in base station/mobile host: When the *MPLS Classifier* decides that a packet is destined for the mobile host, it passes the packet to the default target (the

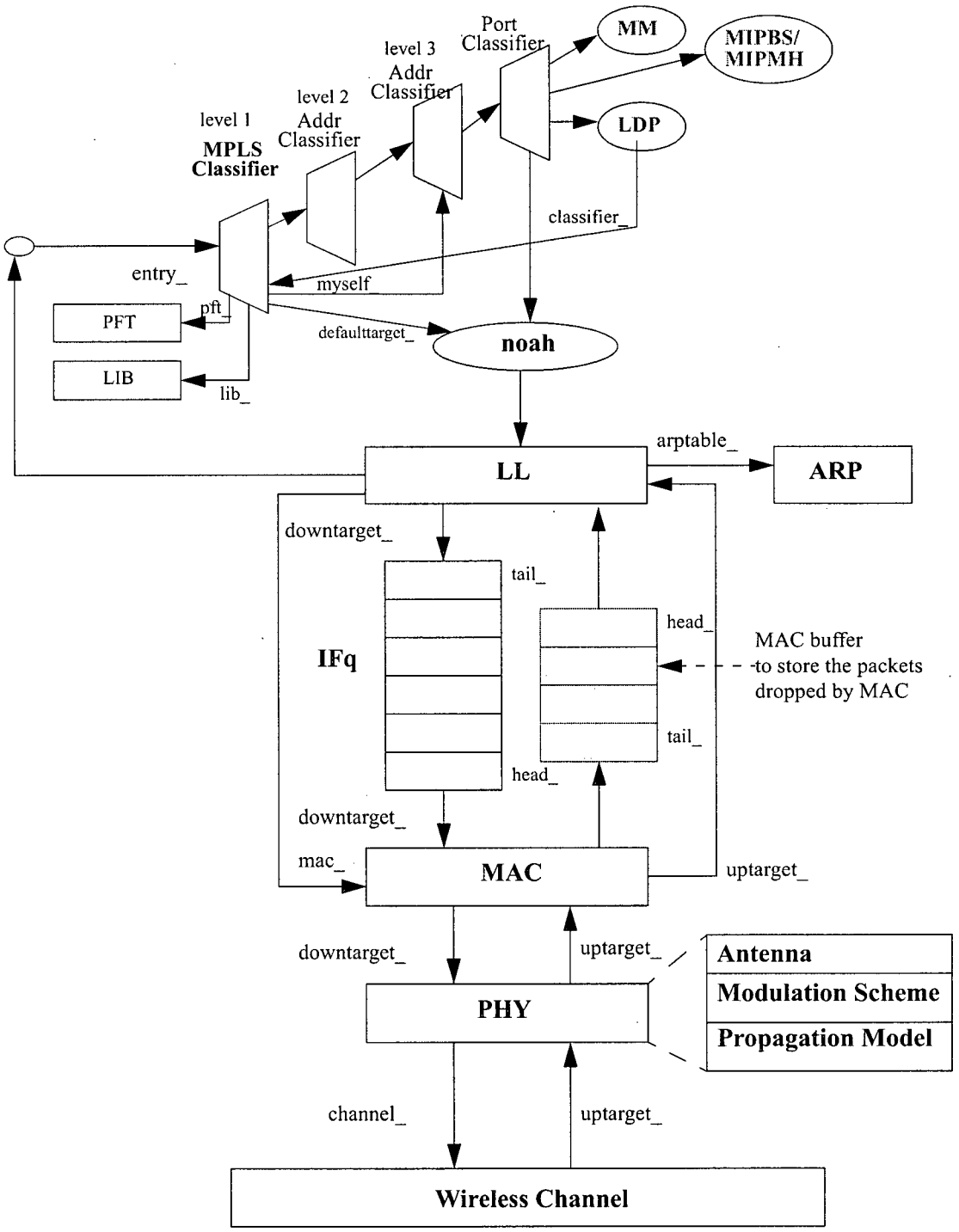


Figure 4.5 Internal structure of BS/MH.

NOAH) agent to route the packet to the mobile host. The NOAH sends the packet to the link layer (LL). The link layer first calls the address resolution protocol (ARP) to get the destination's MAC address. If there is no entry for the destination IP address, the ARP sends an ARP-REQUEST to the whole network via a broadcast message, and holds the IP packet in its cache, which can only hold one packet. The destination mobile host replies with an ARP-REPLY message. Upon receiving the ARP-REPLY message, the ARP in the sender sends the packet in its cache with this MAC address. If there is an entry for the destination IP address in ARP table, the link layer passes the packet to IFq, which is a first in and first out drop tail queue. The MAC layer takes the packet from the IFq, and transmits the packets with RTS/CTS/DATA/ACK four-way handshake method. In the physical layer (PHY), after being stamped with the transmitting power of the base station, the packet is passed to the shared channel, which sends the packet to all nodes attached to the channel. On the receiver side, the packet is first passed to the PHY layer. The PHY calculates the receiving signal power via radio propagation model. The two ray ground reflection model is used. Each PHY layer has a receiving threshold. If the signal power with the packet is below the receiving threshold, it is marked as an error and is dropped by the MAC layer. In the MAC layer, all the nodes attached to the shared channel get a copy of this packet. However, only the targeted destination processes the packet and passes it to the upper layer LL. Other nodes just simply ignore the packet and drop it. Note that nodes within range of each other have full connectivity, and that nodes beyond that range have no connectivity at all. In other words, when nodes are within range of a base station, there is no packet loss due to abrupt or random air link impairments.

From the above description, when the mobile host receives a *Mobile IP advertisement* message from a new base station, it replies with a *Mobile IP registration request* message. From this message, the new base station knows that handoff has occured. The new base station sends a *handoff notification* message to the old base station. After receiving the *handoff notification* message, the old base station sets up a label switced path to the new base station for the mobile host. The old base station then retrieves the packets in the *MAC buffer*, and forwards these packets to the new base station via the label switched path that has just been configured. Afterwards, the old base station also retrieves the packets in the IFq for the mobile host and forwards these packet to the configured label switched path if there are any packets for the mobile host in the IFq.

MAC buffer and IFq are implemented with a bi-directionally linked list. The "add" operation is performed at the *tail_* of the link. The "delete" operation is performed at the *head_* of the link. The "retrieve" operation is performed sequentially starting from the *head_* of the list. In the mobile host, the same MAC buffer is used, and the same process applies when handoff occurs. In the base station, the MAC buffer is shared by all mobile hosts served by this base station. When the number of mobile hosts increases, retrieving the packets for the mobile host sequentially takes a long time since for each mobile host, the whole list must be searched from the beginning to the end. In order to improve the retrieving speed, we designed a new data structure to accomodate the packets dropped by MAC. Each entry in the buffer represents a packet. Each entry has a *packetlink_* to the next packet belonging to the same mobile host. Each entry also has a *timelink_* to the next packet in the order of arriving time to this buffer. Every first packet for a mobile host has an *mhlink_* to the first packet which belongs to another mobile host. This link is also in the order of arriving time to this buffer. For example, there are three mobile hosts in the base station, and the MAC layer dropped the packets in the order: 1 2 3 4 5 6 7 8. The packets belong to: MH3,

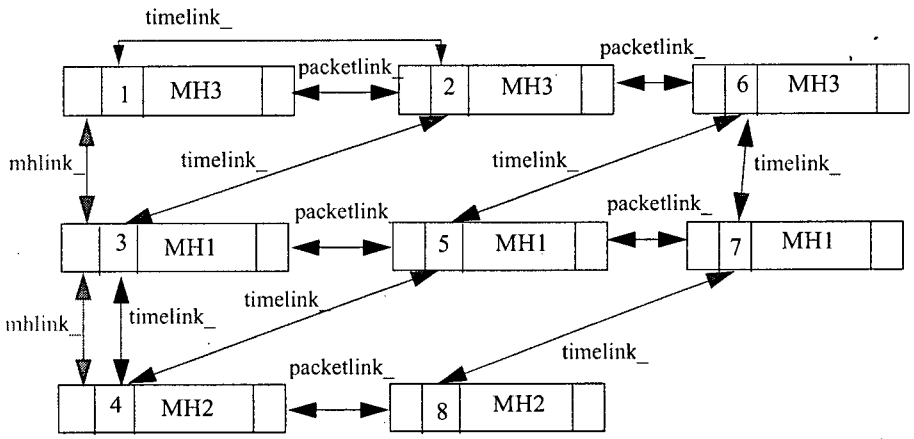


Figure 4.6 MAC buffer structure.

MH3, MH1, MH2, MH1, MH3, MH1, and MH2 respectively. The structure of the MAC buffer is shown in Figure 4.6. In Figure 4.6, all links are bi-directional. After receiving a *handoff notification* message from the new base station, the old base station only needs to traverse the *mhlink_*. After locating the mobile host, the *packetlink_* is traversed, updating the corresponding *packetlink_* and *timelink_*. When all packets for a mobile host are forwarded, the *mhlink_* is updated correspondingly. In this way, the retrieving operation can be performed quickly.

Chapter 5 Result Analysis

In this chapter, we first introduce the simulation configuration. Following that, we simulate and analyze the performance of the MPLS-based mobility management in terms of UDP packet loss, TCP behavior during handoff, and TCP throughput. Finally, the TCP throughput comparisons with three other schemes, Cellular IP, HAWAII, and HFA, are given.

5.1 Simulation Configuration

In our simulation, IEEE 802.11 LAN, which works as a 914 MHz Lucent WaveLAN radio interface, is adopted. The parameters are shown as follows:

- Antenna: Omni-directional, (X, Y, Z) coordinates = (0, 0, 1.5), transmitting gain Gt = 0.2, and receiving gain Gr = 0.2.
- Wireless channel frequency: 914 MHz, wave length L = 1.0 meter, CPThresh = 10, CSThresh = 1.559e-11, and RXThresh = 3.652e-10.
- Propagation model: Two ray ground reflection model [47].

In order to model the scenarios where neighboring base stations overlap with each other, we adjusted the transmitting power of the base stations according to the overlapping distance, denoted by d(overlap). Figure 5.1 shows the concept of overlapping distance. When a mobile host crosses the cell boundary, upon receiving the first beacon signal from the new base station, the mobile host assumes that a handoff has occurred, and notifies the base station [48].

The network topology is shown in Figure 5.2. The coordinates for four base stations are (0,0), (140,140), (280,280), and (420,420). We assume that the network in Figure 5.2 is the mobile host's home network. In the network, each wired connection is modeled as a 10 Mb/s

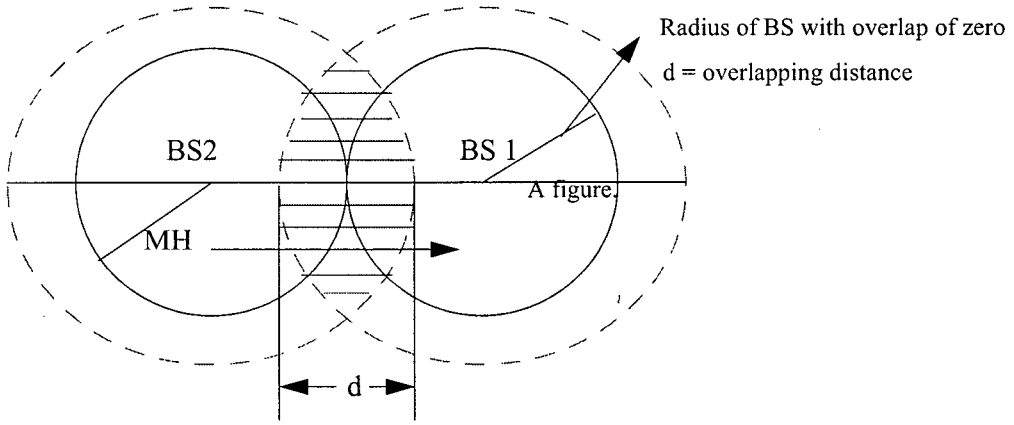


Figure 5.1 Overlapping distance illustration.

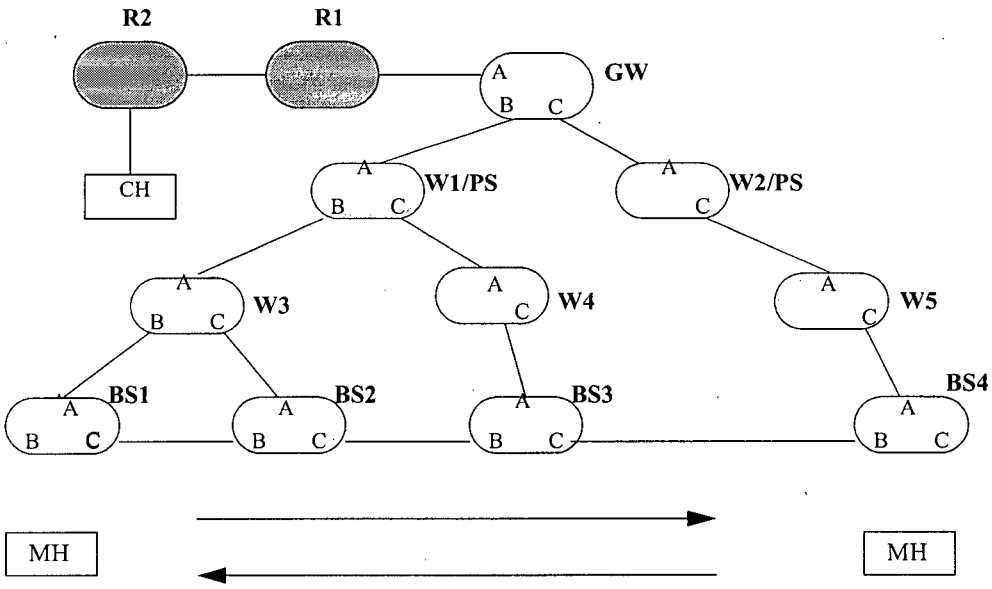


Figure 5.2 Simulation network topology.

duplex link with a link delay of 10 ms. Since the base stations are assumed to be label switching routers with mobility management capability, we assume that there is a direct connection between each pair of neighboring base stations. The base station broadcasts an *Mobile IP advertisement* at an interval of 0.5s.

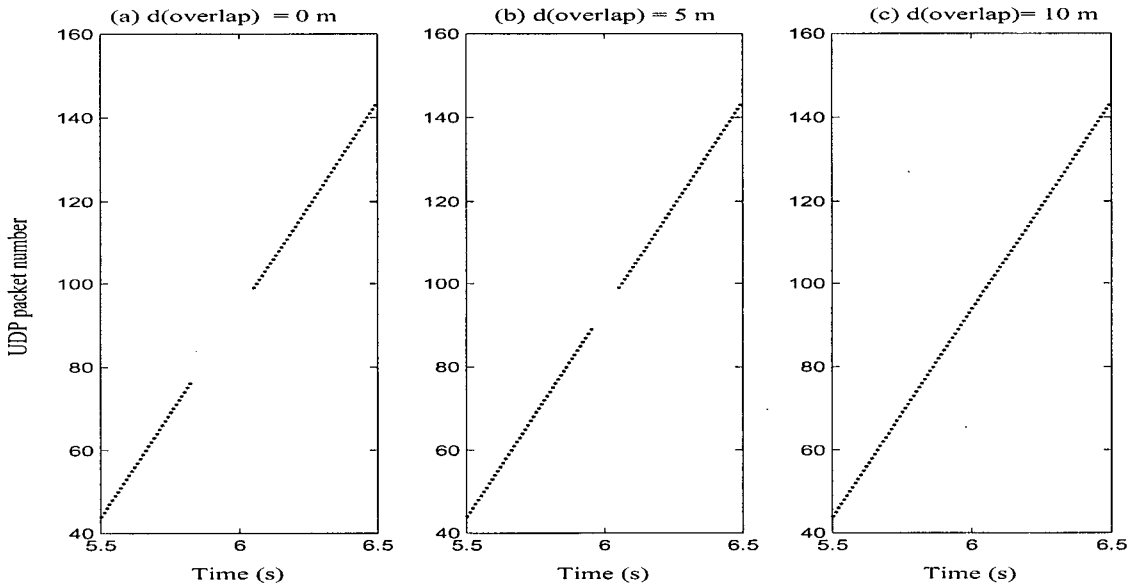


Figure 5.3 UDP packet number.

5.2 Performance without Any Packet Recovery Schemes

First, we investigate the performance of MPLS-based micro-mobility where no packet recovery schemes are used. We study the UDP packet loss, TCP throughout, and TCP packet number during the handoff period.

5.2.1 UDP Packet Loss

In this experiment, UDP probing traffic is directed from the correspondent host to the mobile host and consists of 210 byte packets transmitted at 10 ms intervals. The mobile host moves from BS1 to BS2 at a speed of 20 m/s. In Figure 5.2, label switching routers W1 and W2 are assumed to be paging servers. We used real-time transmission protocol (RTP) sequence number to record the UDP packets. As shown in Figure 5.3, the number of packet loss is 22, 9 and 0, with an overlapping distance of 0, 5 and 10 meters, respectively. We can see that the overlap-

ping of neighboring base stations does reduce the packet loss during handoff. However, in some networks, for example, GSM, the mobile host cannot listen to two neighboring base stations simultaneously. Therefore, it is still necessary to minimize the packet loss due to handoff.

5.2.2 TCP Performance

This experiment is performed to investigate the impact of handoff on TCP throughput. The mobile host moves back and forth between BS1 and BS4 at different speeds. The simulation time is 400s. TCP Reno is used. From Figure 5.4, it is obvious that as the overlapping distance increases, the TCP throughput also increases. This again demonstrates that an increasing overlapping distance is effective for TCP based applications. In order to demonstrate this more clearly, the TCP packet number observed at the mobile host is shown in Figure 5.5 with a speed of 20m/s and an overlapping distance of zero when handoff occurs.

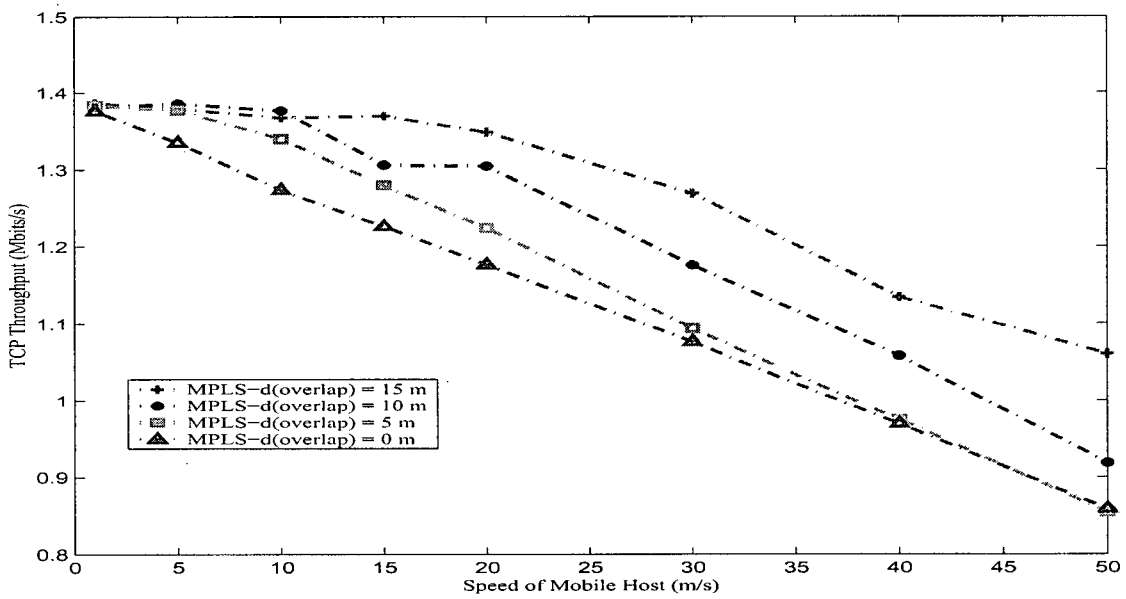


Figure 5.4 TCP throughput with different overlapping distances.

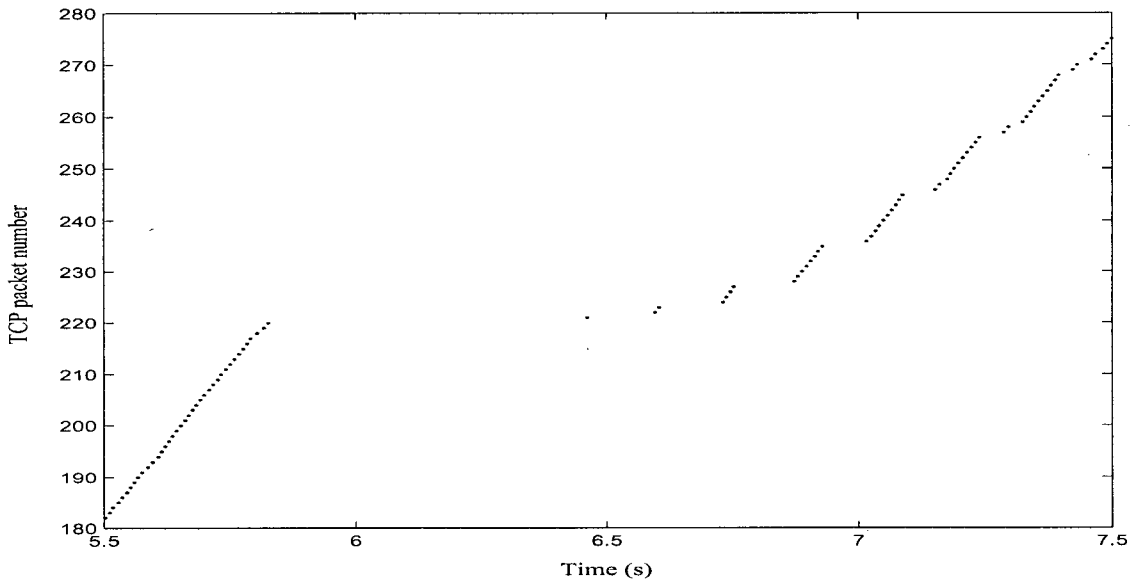


Figure 5.5 TCP packet number at MH.

At time 6.006s, the mobile host receives the beacon signal (*Mobile IP advertisement message*) from the new base station. A handoff has occurred. From Figure 5.5, we can observe that TCP slow start [49] is initiated due to a timeout.

5.3 Performance with Buffer Time-based Packet Recovery

5.3.1 UDP Packet Loss

In this experiment, the effect of using a buffer time based packet recovery scheme in the old base station is studied. The simulation configurations are the same as those in Section 5.2 with the exception that a buffer in each base station is configured. The mobile host moves back and forth between BS1 and BS4 with a speed of 20 m/s. The overlapping distance is 0 m.

In Figure 5.6 (a), the UDP packet number is shown during the first handoff when the mobile host moves from BS1 to BS2. No buffer time based packet recovery is applied. Figure 5.6

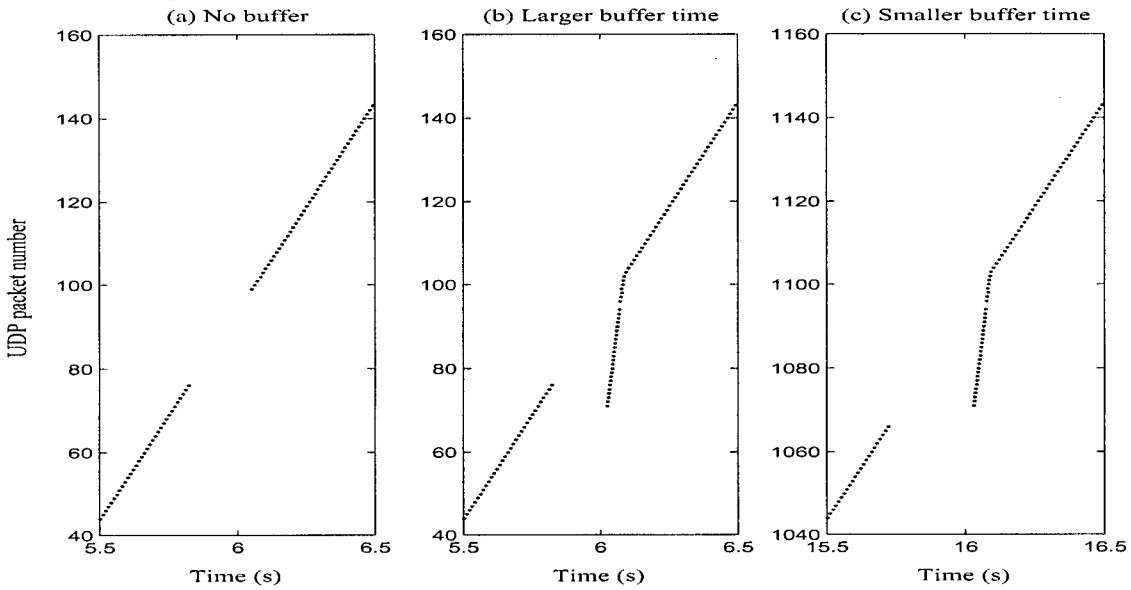


Figure 5.6 UDP packet number with buffer time based packet recovery.

(b) shows the UDP packet number with a buffer time of 250 ms. Some duplicated packets arrive at the mobile host. With the same buffer time, the UDP packet number during the second handoff, when mobile host moves from BS2 to BS3, is shown in Figure 5.6 (c). However, at this time, some packets are dropped due to handoff. Figure 5.6 (a), (b), and (c) show the average buffer time is approximately half the *Mobile IP advertisement* interval, plus the delay between the new and old base station. However, we cannot guarantee that there is zero packet loss, or zero duplicated packets in the mobile host during handoff, after applying the buffer and buffer time in the old base station. In other words, the buffer time based packet recovery scheme results in a suboptimal performance.

5.3.2 TCP Performance

Next, the TCP packet number during handoff after introducing buffer time based packet recovery in the old base station is examined. In Figure 5.7 (a), buffer time based recovery method

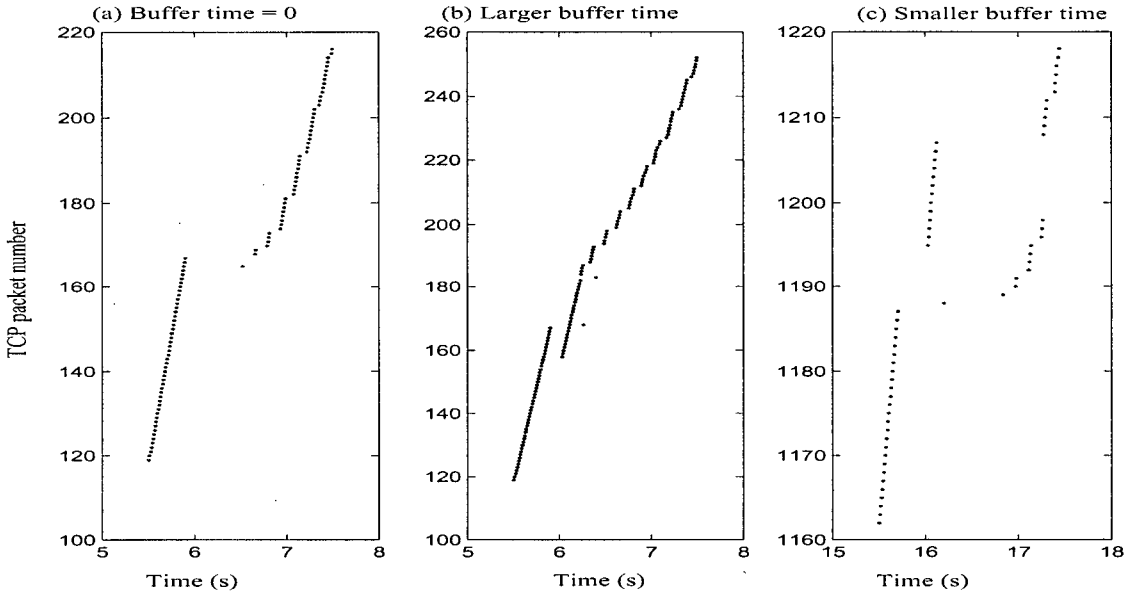


Figure 5.7 TCP packet number with buffer time based packet recovery.

is not used. The result is the same as that of Figure 5.5. TCP slow start is initiated. Figure 5.7 (b) and (c) show the TCP packet number for the first and second handoff when the mobile host moves from BS1 to BS2, and from BS2 to BS3 with a buffer time of 250 ms, and a speed of 20m/s, respectively. In Figure 5.7 (b), some duplicated packets arrive at the mobile host. In Figure 5.7 (c) some packets are dropped due to the smaller buffer time value. TCP slow start is initiated. Figure 5.8 shows the throughput for the TCP new Reno after introducing buffer time based packet recovery with a buffer time of 250 ms, comparing this with no buffer time based packet recovery at all.

From Figure 5.8, the same conclusion in the previous section can be drawn. Although buffer time based packet recovery in the old base station can improve the TCP throughput in some sense, the gain is not so obvious since it is difficult to determine the accurate buffer time value for each handoff.

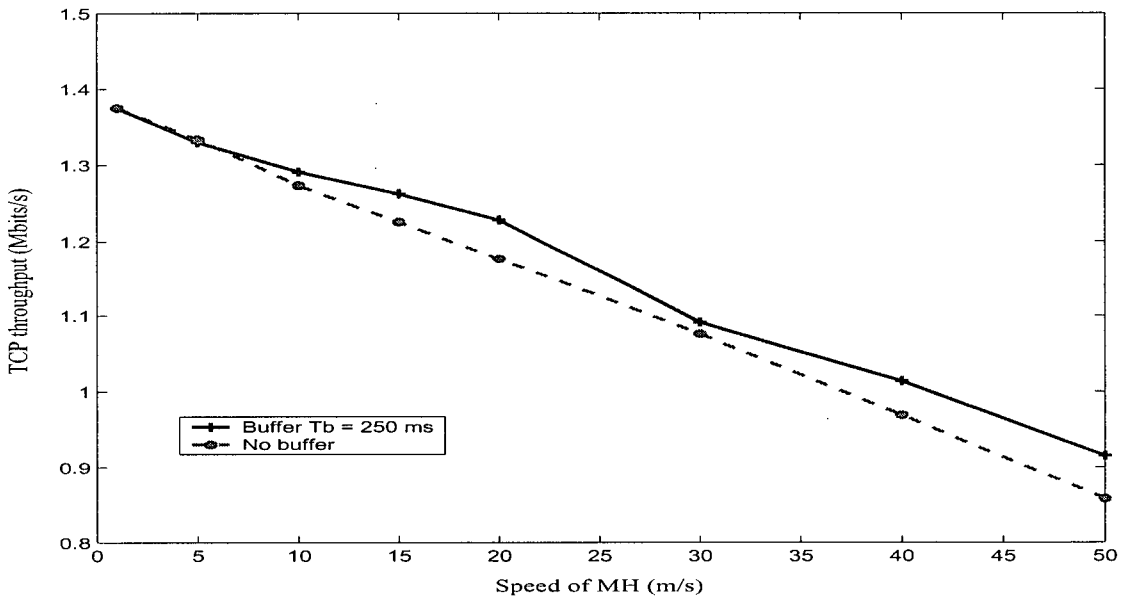


Figure 5.8 TCP throughput with buffer time based packet recovery.

5.4 Performance with MAC Layer Assisted Packet Recovery

From the above results, we can observe that buffer time based packet recovery in the old base station can reduce packet loss and improve TCP throughput. In real life it is difficult to estimate the accurate handoff time for each handoff. We introduce MAC layer assisted packet recovery in the base station and mobile host, and provide our results in this section.

5.4.1 UDP Packet Loss

In this experiment, the UDP probing traffic is directed from the correspondent host to the mobile host, and consists of 210 bytes packets transmitted at 10 ms intervals. The mobile host moves from BS1 to BS2, at a speed of 20 m/s. In Figure 5.2, label switching routers W1 and W2 are assumed to be the paging servers. From Figure 5.9, we can observe that the MAC layer assisted packet recovery can totally eliminate packet loss during handoff. As the overlapping

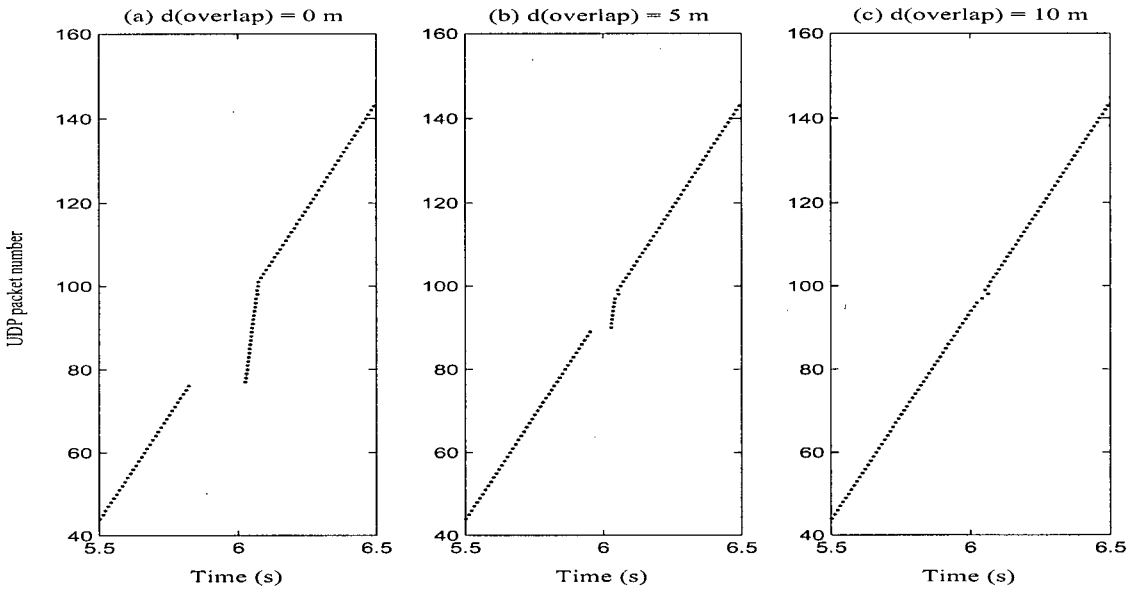


Figure 5.9 UDP packet number with MAC layer assisted packet recovery.

distance increases, the time gap between the packet stream from the old base station to the mobile host, and the other stream from the old base station via the new base station to the mobile host becomes smaller. Comparing Figure 5.9 (b) and Figure 5.9 (c), we can see that when the overlapping distance is large enough, the MAC layer assisted packet recovery has no gain. The reason is that the mobile host can connect to two neighboring base stations simultaneously for a time that is long enough to accommodate the handoff.

5.4.2 TCP Performance

In order to examine the TCP behavior during handoff, the TCP Reno packet number after introducing MAC layer assisted packet recovery during handoff is shown in Figure 5.10. The mobile host moves from BS1 to BS2 at a speed of 20 m/s. The overlapping distance is 0 m. From Figure 5.10 (b), we can see that no TCP packet is dropped, and no TCP slow start is performed. The gap between the packet stream from the old base station to the mobile host, and the other

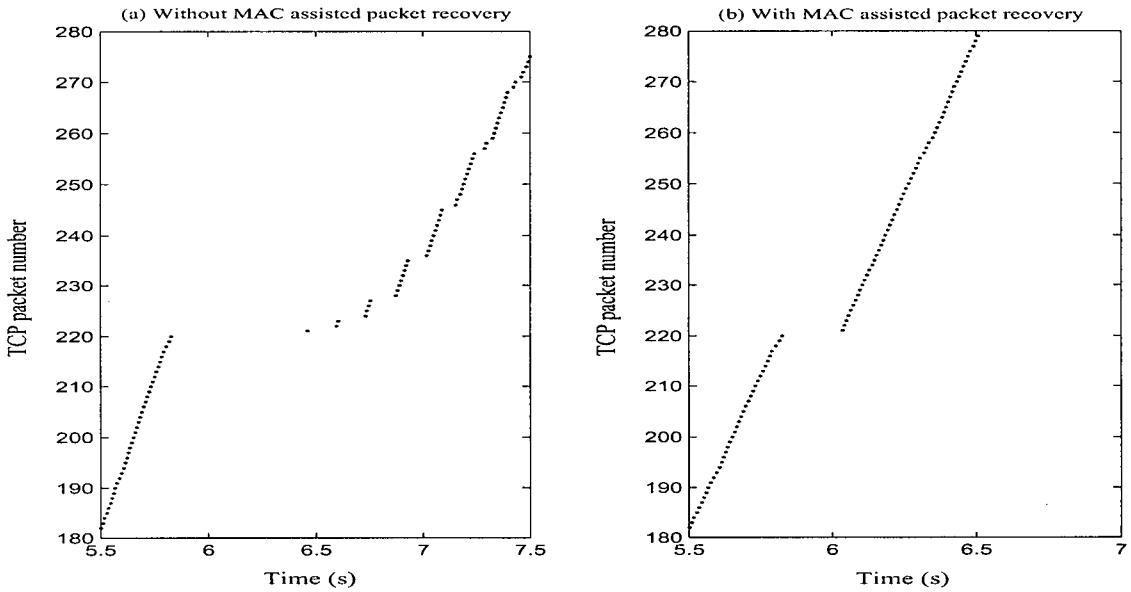


Figure 5.10 TCP sequence number with MAC layer assisted packet recovery.

stream from the old base station via the new base station to the mobile host, 210 ms is the handoff time plus the link delay from the new base station to the old base station via which the *handoff notification* message passes.

The next experiment is performed to investigate the impact of link delay between neighboring base stations on the performance of TCP throughput after introducing MAC layer assisted packet recovery. The mobile host moves back and forth between BS1 and BS2. The simulation time is 400 s. W1 and W2 are paging servers. The overlapping distance is 0 m. From Figure 5.11, we can observe that as the neighboring base station delay increases, the TCP throughput for MAC layer assisted packet recovery decreases. The reason is that the longer the link delay from the new base station to the old base station, the later the *handoff notification* message arrives at the old base station, the later the MAC layer assisted packet recovery performs, the more packets get lost.

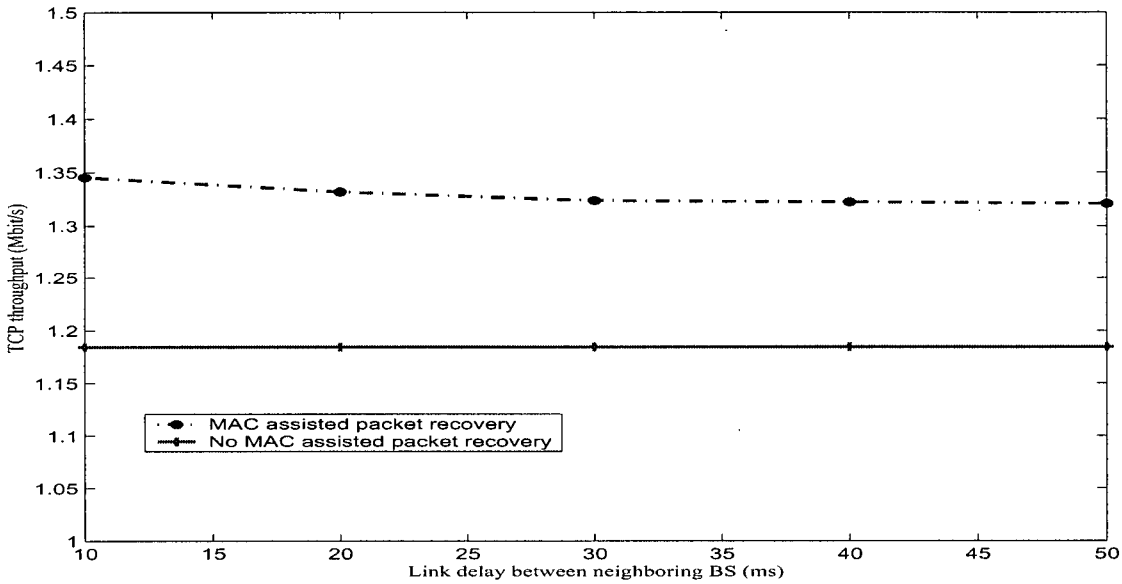


Figure 5.11 TCP throughput with different neighboring BS link delay.

The next experiment is performed to investigate the TCP Reno performance under different overlapping distances. In Figure 5.12, TCP throughputs for MPLS-based mobility management with and without MAC layer assisted packet recovery under varying overlapping distances are compared. From this figure, we can make the following observations. First, a higher TCP throughput can always be achieved with the use of MAC layer assisted packet recovery. The larger the overlapping distance between neighboring base stations, the higher the TCP throughput, regardless of whether MAC buffer is used. This can be explained as follows. With a larger overlapping distance, the mobile host can receive the beacon signal from the new base station sooner, and can also maintain the connection with the old base station longer. We can also observe that the TCP throughput decreases as the speed of the mobile host increases.

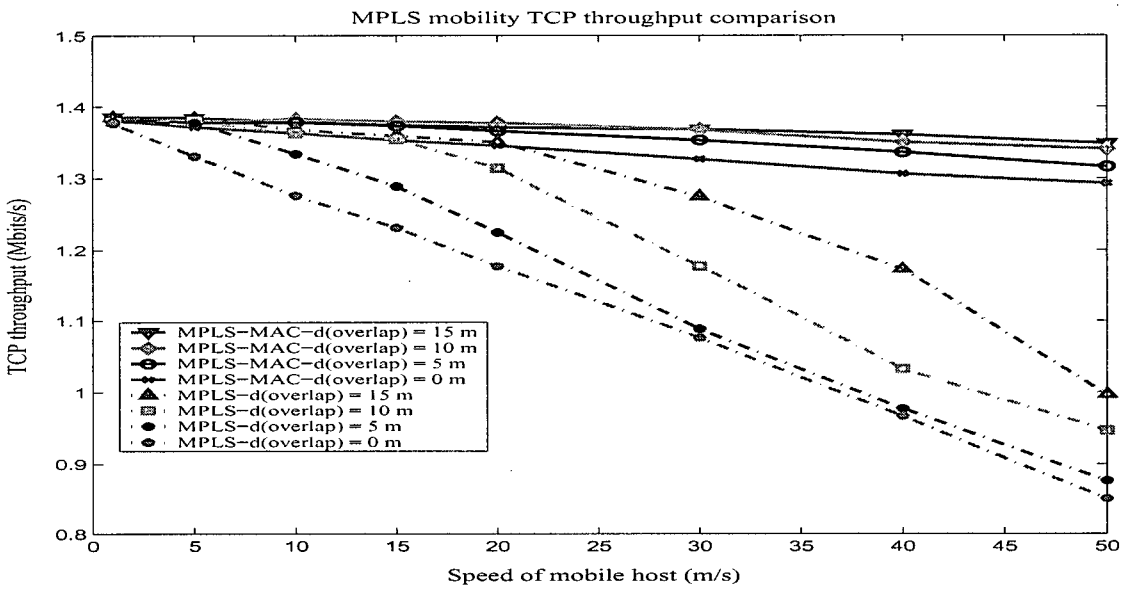


Figure 5.12 TCP throughput with MAC layer assisted packet recovery under different overlapping distances.

5.5 Performance Comparison with Cellular IP, HAWAII, HFA

5.5.1 HFA TCP Throughput

In order to provide a fair comparison, we made some modifications in the HFA and HAWAII module from CIMS. In the original CIMS, upon receiving the first beacon signal (Mobile IP advertisement) from the new base station, the connection between the mobile host and the old base station is cut off to simulate the network where the mobile host can only listen to a base station's signal. We remodel this by adjusting the transmitting power of the base station. The TCP Reno throughput with different overlapping distances are shown in Figure 5.13. The simulation configurations are the same as those of MPLS-based micro-mobility management. In HFA, one level of hierarchy is used, and the gateway is the gateway foreign agent. Each base station is the regional foreign agent. No mechanism is used to recover the packet loss.

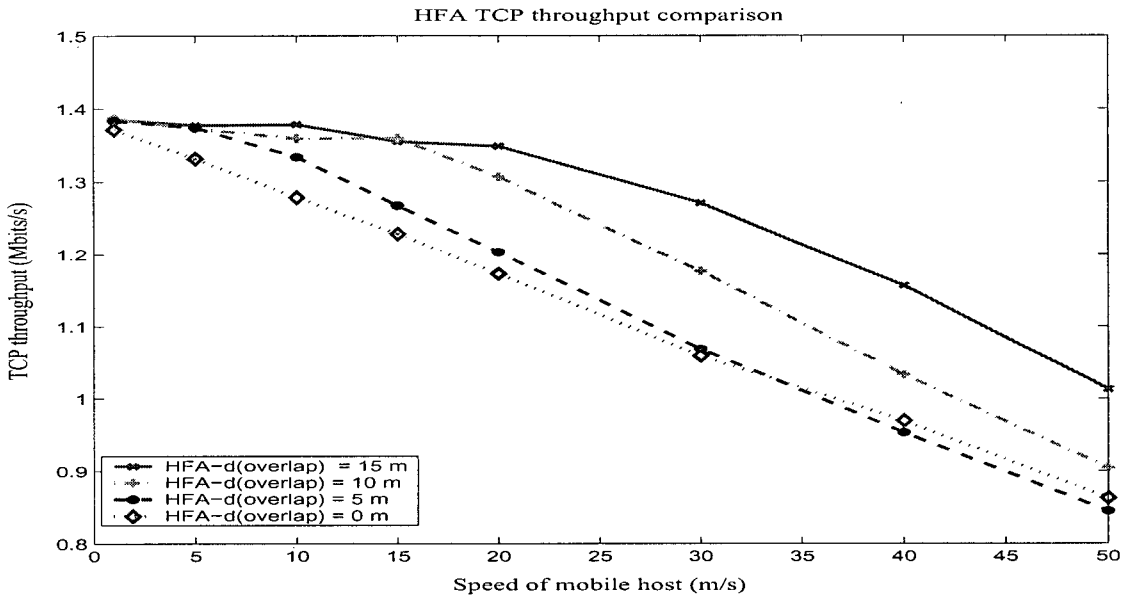


Figure 5.13 HFA TCP throughput with different overlapping distances.

From Figure 5.13, we can also observe that as the overlapping distance increases, the TCP throughput increases. The reason is the same as MPLS-based mirco-mobility without any recover mechanism. The larger the overlapping distance, the sooner the mobile host receives the beacon signal from the new base station, and the longer the mobile host keeps connection with two neighboring base stations simultaneously. As the speed increases, the TCP throughput decreases. The reason is that as mobile host speeds up, it moves more trips between BS1 and BS4; thus, more handoffs occur in fixed simulation time.

5.5.2 HAWAII TCP Throughput

The same simulations are performed with HAWAII UNF and MSF. The results are shown in Figure 5.14. Two phenomena can be observed from this experiment. First, with larger overlapping distances, we gain a higher TCP throughput in UNF and MSF. Second, the difference between UNF and MSF is very small.

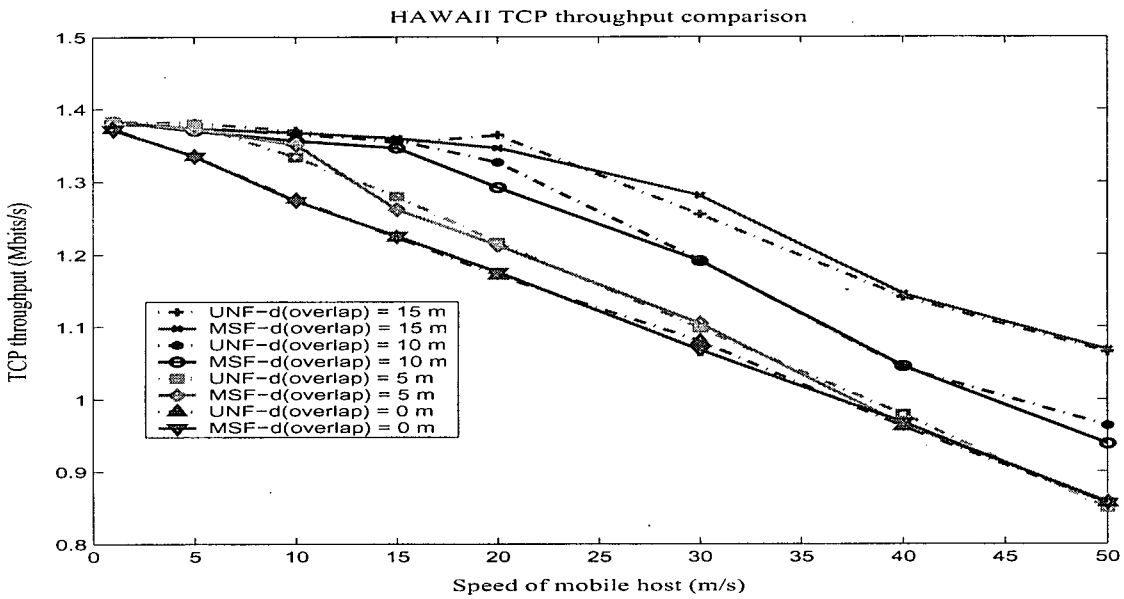


Figure 5.14 TCP throughput comparison with overlapping distance of 0 meter.

As defined in [26], in MSF, *packets are first forwarded from the old base station to the new base station before they are diverted at the cross over router.* Thus, it is possible to introduce some kind of packet recovery mechanism in the old base station, for example, buffer time based packet recovery [35]. Here, we give the TCP throughput after introducing the buffer time based packet recovery method in the old base station in MSF, as shown in Figure 5.15.

When the overlapping distance is small, for example 0 or 5 m, after introducing buffer time based packet recovery, the TCP throughput improves. When the overlapping distance becomes larger, for example 10 or 15 m, in some cases even the TCP throughput decreases. The explanation is as follows. The buffer time based packet recovery method recovers some unnecessary packets, resulting in duplicated packets being received in the mobile host, which decreases the TCP throughput instead.

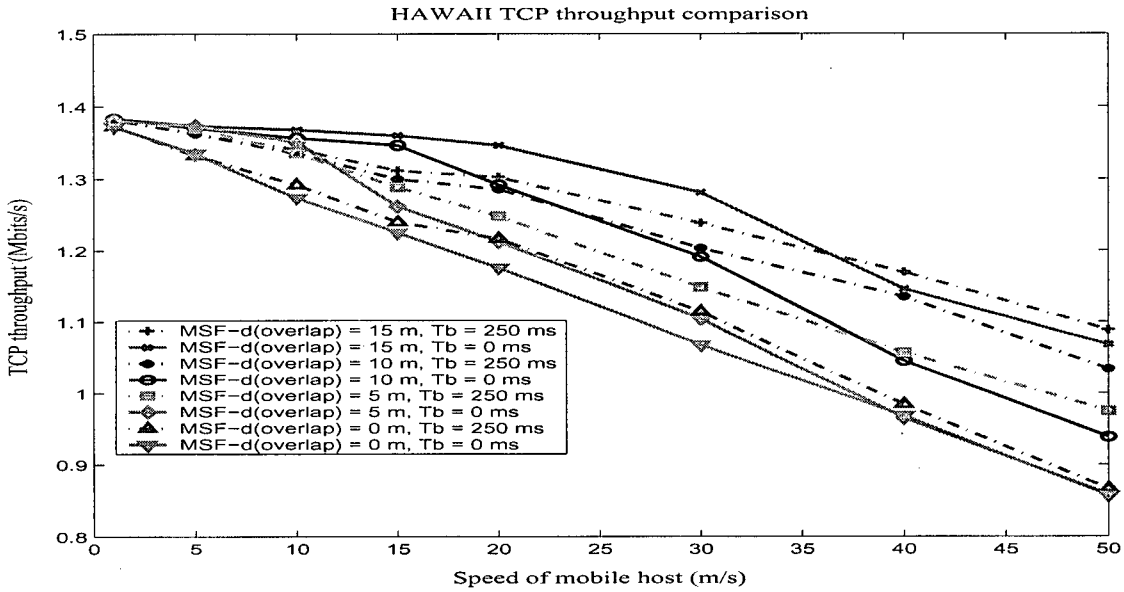


Figure 5.15 MSF TCP throughput after introducing packet loss recovery.

5.5.3 Cellular IP TCP Throughput

Without any changes in the original Cellular IP module from CIMS, the TCP Reno throughputs with different overlapping distances are shown in Figure 5.15. Here, the simulation configurations are the same as those of the MPLS-based micro-mobility management. The route update interval is 0.5s. The routing cache time-out is 1.5s. The paging cache time-out is 15s. The active time is 2s. The semi-soft time is 50ms. All nodes except CH, R1 and R2 are CIP capable nodes and all nodes are configured with a routing cache and paging cache. In Figure 5.16, the gain from a larger overlapping distance in Cellular IP *hard handoff* is not obvious as compared with the gain in Cellular IP *semi-soft* handoff. The TCP throughput of *semi-soft handoff* is always greater than that of *hard-handoff* with the same overlapping distance. This again demonstrates that the *hard-handoff* is designed for networks where the mobile host can only receive a signal from one base station at any given time, for example, GSM network, and *semi-soft handoff* is

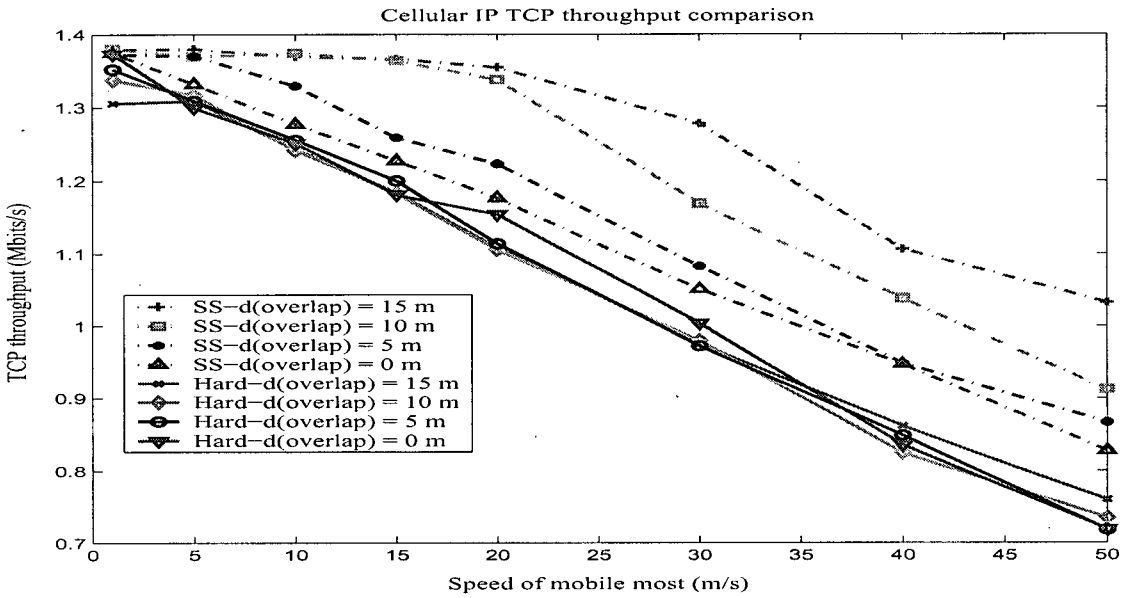


Figure 5.16 Cellular IP TCP throughput with different overlapping distances.

designed for a network where the mobile host can receive signals from neighboring base stations simultaneously, for example, CDMA network. This conclusion complies with the original design principles in [22].

5.5.4 TCP Throughput Comparisons

In this section, the TCP throughput of MPLS-based micro-mobility management and those of Cellular IP, HFA, HAWAII with the same network configurations are compared.

First, the TCP throughput when the overlapping distance is 0 meter is shown in Figure 5.17. From this figure, we can make the following observations. First, our proposed MPLS-based micro-mobility management with MAC layer assisted packet recovery outperforms all other IP micro-mobility schemes. Second, the performance between MPLS-based micro-mobility management without MAC layer assisted packet recovery and HFA is very similar since HFA does not

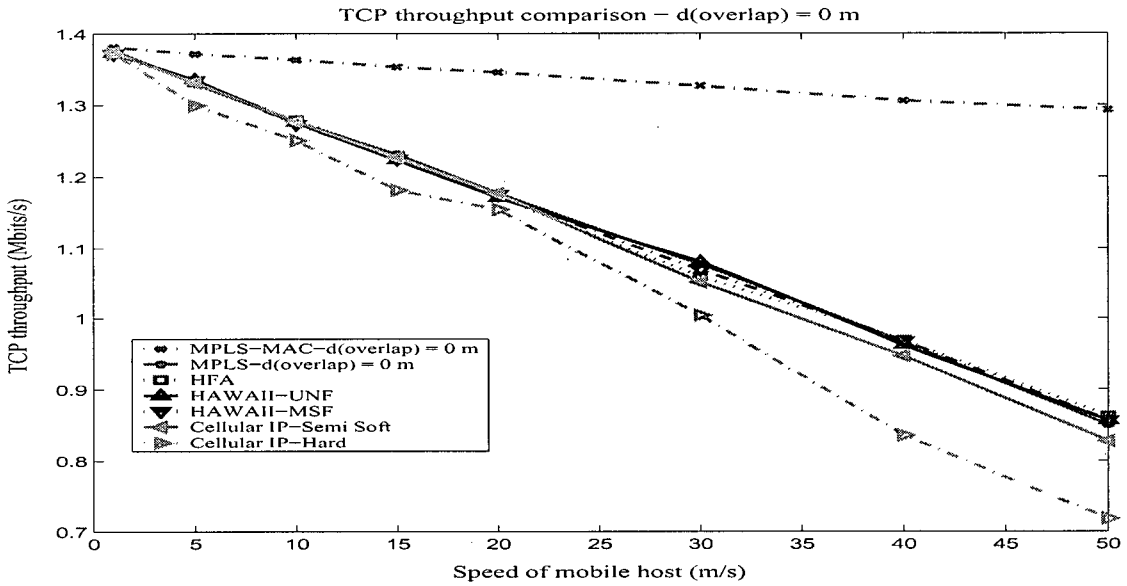


Figure 5.17 TCP throughput comparison with overlapping distance of 0 meter.

use any packet recovery scheme. Third, HAWAII MSF gains a small edge over HFA, MPLS without packet recovery, as well as Cellular IP semi-soft handoff. When no packet recovery scheme is used, the performance of MSF and UNF in HAWAII is very similar. The advantage of MSF over UNF is that the packet recovery scheme can be applied in the old BS. In addition, we observe that in Cellular IP, periodical route-update and paging-update messages are sent that would compete with the shared wireless channel with data packets. Cellular IP gives a lower TCP throughput when compared with other schemes.

Next, the TCP throughputs with overlapping distances of 5, 10 and 15 meters are shown in Figures 5.18-5.20, respectively. The comparison result is the same as that with an overlapping distance of 0 meters.

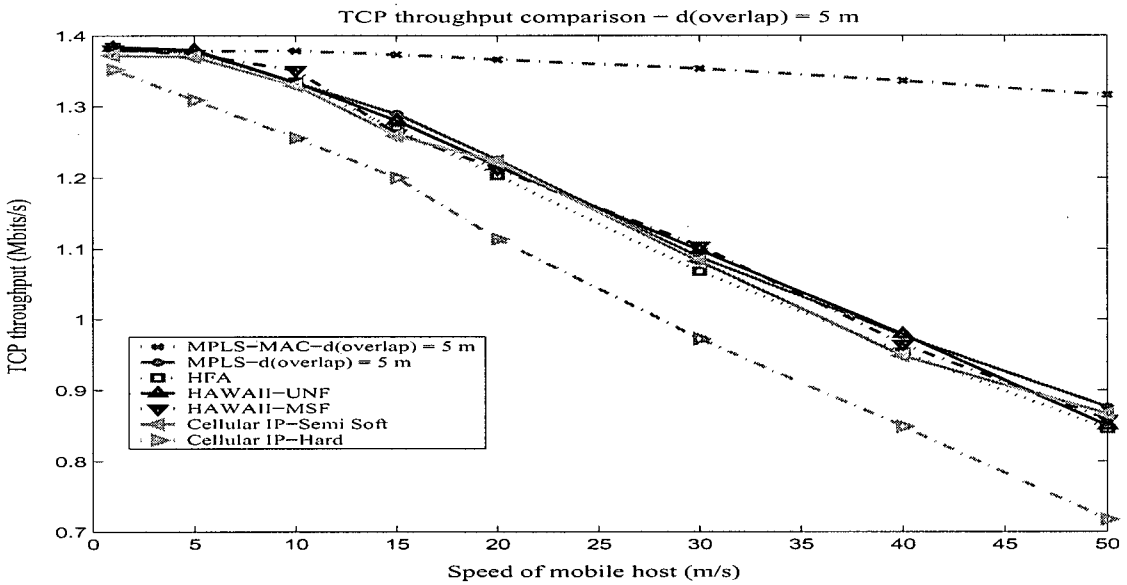


Figure 5.18 TCP throughput comparison with overlapping distance of 5 meters.

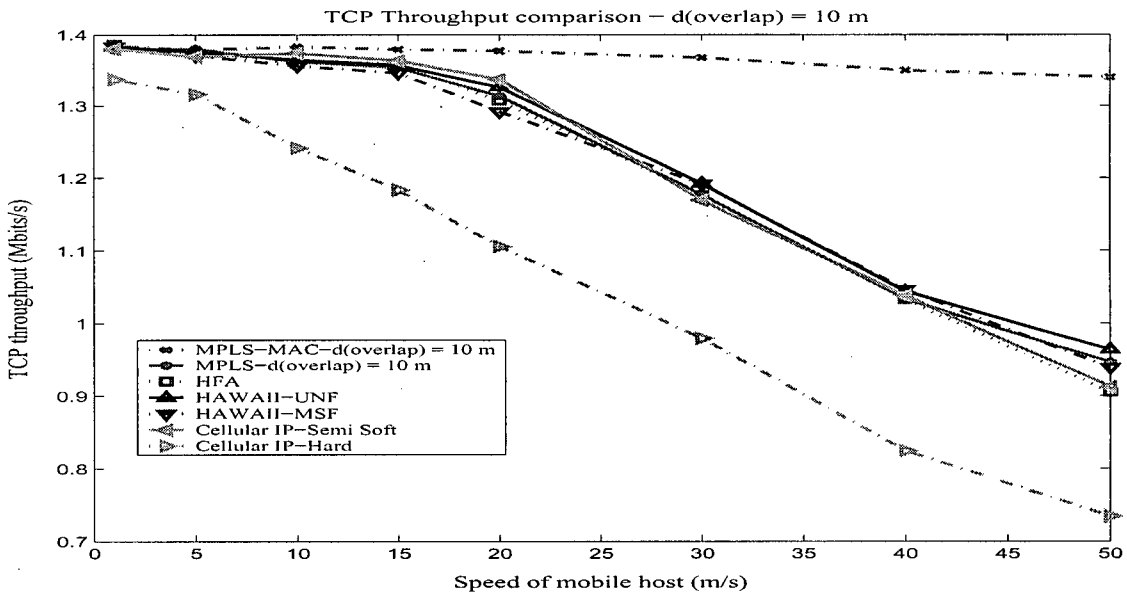


Figure 5.19 TCP throughput comparison with overlapping distance of 10 meters.

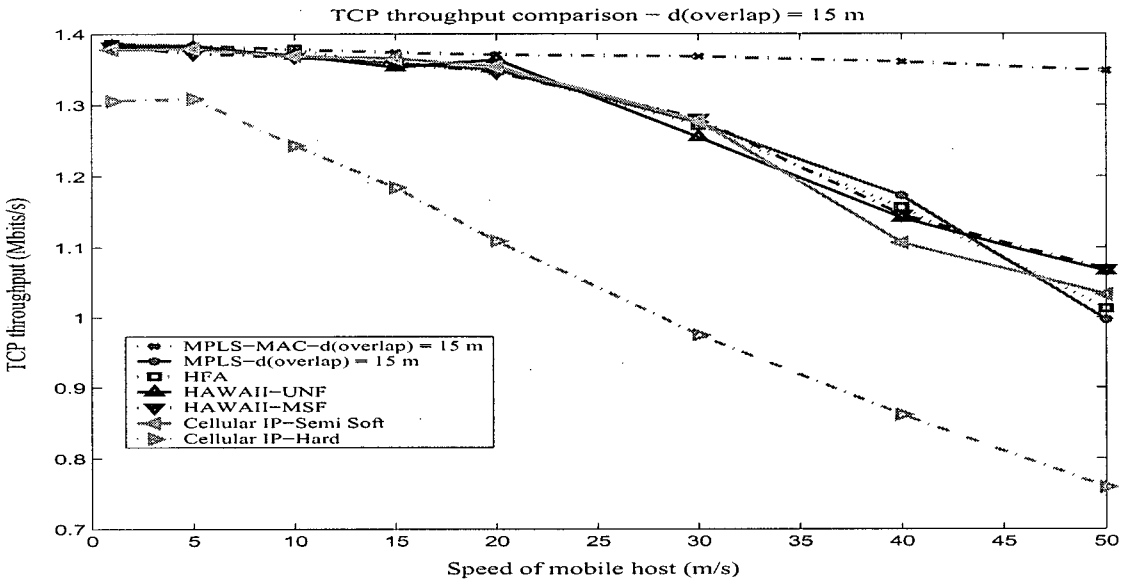


Figure 5.20 TCP throughput comparison with overlapping distance of 15 meters.

Chapter 6 Conclusions

In this thesis, after providing the motivations and contributions in Chapter 1, we gave an overview of related works on MPLS and IP-based micro-mobility management, including Mobile IP, hierarchical Mobile IP, Cellular IP and HAWAII, in Chapter 2.

Chapter 3 proposes the MPLS-based micro-mobility management schemes. We discussed the label switched path setup, handoff processing, paging, route optimization and MAC layer assisted packet recovery due to handoff. In addition, a qualitative comparison among MPLS-based micro-mobility management and Cellular IP, HAWAII, HFA was given.

Chapter 4 describes the detailed ns-2 based implementation for the proposed MPLS-based micro-mobility management. We presented the design of an MPLS forwarding module, LDP module, mobility management module, and MAC layer assisted packet recovery module.

In Chapter 5, the simulation results were presented and analyzed. We investigated UDP packet loss, TCP behavior during handoff and TCP throughput with or without any packet recovery schemes. Simulation results showed that MAC layer assisted packet recovery can eliminate packet loss and dramatically improve TCP throughput. In addition, we also compared the TCP performance among HAWAII, HFA, Cellular IP and MPLS-based micro-mobility management. Results showed that without using any packet recovery scheme, MPLS-based micro-mobility management can achieve the same performance as HAWAII, HFA whereas an outstanding lead over other schemes after introducing MAC layer assisted packet recovery was gained.

The contributions of this thesis can be summarized as follows:

- The presentation of a domain based MPLS micro-mobility management for wireless cellular network including label switched path setup, and mobile host handoff.
- The proposal of a medium access control (MAC) assisted packet recovery scheme to recover packet loss due to handoff.
- The proposal of a paging server that introduced a hierarchical structure and paging in order to reduce power consumption of the mobile host and the signalling load in the access network.
- The proposal of route optimization to handle the scenario where the two communicating parts are in the same domain, thus reducing communication delay and signalling load on the access network.
- The presentation of the performance of MPLS-based micro-mobility management in terms of UDP packet loss and TCP throughput by simulation. Moreover, the performance between MPLS-based micro-mobility management and the other three schemes for IP mobility management, Cellular IP, HAWAII, and Hierarchical Mobile IP were quantitatively compared.

Not withstanding the above, some problems need further investigation:

- Can traffic engineering and mobility management be integrated? For example, when a mobile host moves to a new base station, can we resolve the problem where the network has insufficient resources to support the mobile host's QoS requirement?
- Can we determine the optimal value for the active timer for the mobile host? To calculate the optimal value for active timer T_a, we must consider the traffic pattern on the packet level [50][51][52], and the mobility pattern for the designated mobile host such that the signalling load on the access network is minimized.

Appendix A. Basic Principles of CSMA/CA

In order to avoid collisions, MAC layer applies mechanisms for sensing whether the medium is in use before transmitting. If the medium is in use, the mobile host waits according to a predefined algorithm before attempting to transmit. This method of sensing the medium and waiting before transmitting is called *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA). MAC supports complementary physical and virtual carrier sense mechanisms. Physical sensing of the medium is called clear channel assessment, and is physical channel dependent. Although physical sensing is very efficient, it is susceptible to the *hidden node* problem caused by the fact that mobile hosts in a radio network are not guaranteed to hear every other mobile host's transmissions. In virtual carrier sensing, no actual physical sensing of the medium occurs. A sequence of control frames of a short length is exchanged to identify whether the medium is idle or not. These control frames are called *Request to Send* (RTS) and *Clear to Send* (CTS). The duration during which the medium is busy is presented by the *Network Allocation Vector* (NAV). This is a timer that indicates the amount of time that remains before the medium can be used. This value counts down on a regular basis. When it reaches zero, it indicates that the medium is free. It is updated every time an RTS or CTS with a larger value is received. By combining the physical sensing of the medium with the RTS/CTS procedure, it is possible for a hidden node that is unable to receive from the originating node to avoid collisions with an impending data transmission. The whole process is illustrated in Figure A.1.

In addition to the RTS/CTS control frames, the CSMA/CA procedure requires an acknowledgement (ACK) frame to be sent upon every successful receipt of data frames. Due to the link impairment and handoff, there may be two kinds of errors. One occurs in the RTS/CTS

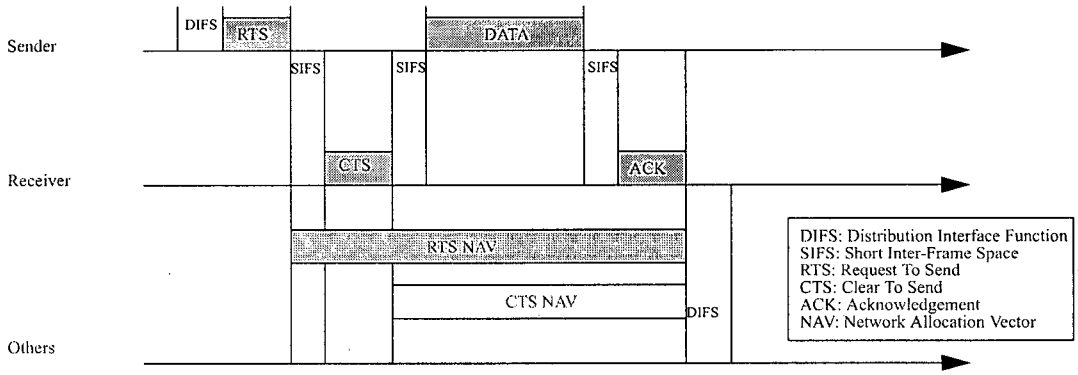


Figure A.1 CSMA/CA access.

exchange phase. After sending an RTS, the sender waits for the CTS, and starts a timer. If the RTS is lost on the way, or the CTS lost on its return path, the timer eventually expires. The sender retransmits the RTS for a system defined threshold. After the retransmitting time exceeds the threshold, the sender drops the frame to be transmitted. The second occurs in the data transmitting phase. After sending a data frame, the sender waits for the ACK from the destination. If it cannot receive the ACK for a predefined time, it resends the data packet. After the retransmitting time exceeds the system threshold, the sender drops the frame. The whole process is illustrated in the Figure A.2.

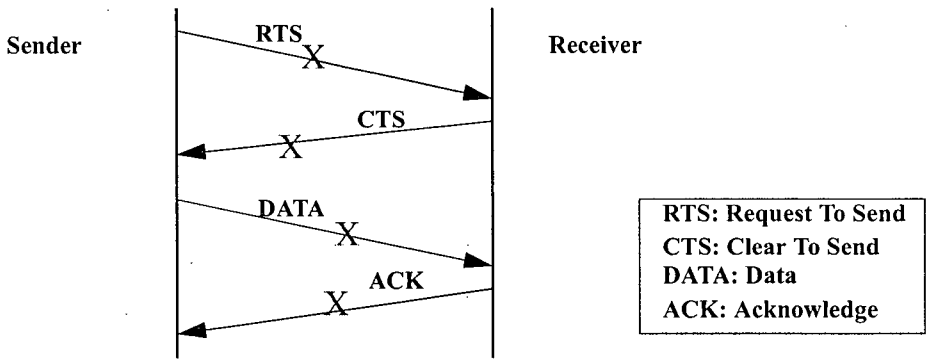


Figure A.2 RTS/CTS/DATA/ACK exchange.

Bibliography

[1] ETSI, "Digital cellular telecommunications system (Phase 2+): General Packet Radio Packet Service, GSM 02.60 Service Description Stage 1, version 5.1.0," October 1997.

[2] 3GPP: www.3gpp.org.

[3] G. Patel and S. Dennett, "The 3GPP and 3GPP2 movements toward an all-IP mobile network," *IEEE Personal Communications*, Volume 7, Issue 4, August 2000, Page(s) 62-64.

[4] X. P. Xiao, A. Hannan, B. Bailey, and L. M. Ni, "Traffic Engineering with MPLS in the Internet," *IEEE Network*, Volume 14, Issue 2, March 2000, Page(s) 28-33.

[5] Y. L. Guo, Z. Antonious, and S. Dixit, "IP Transport in 3G radio access networks: an MPLS-based approach," in *Proc. IEEE WCNC'02*, Volume 1, Orlando, FL, March 2002, Page(s) 11-17.

[6] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF RFC 3031, January 2001.

[7] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "LDP Specification," IETF RFC 3036, January 2001.

[8] P. Gupta, S. Li, and N. Mckeown, "Routing lookups in hardware at memory access speeds," in *Proc. IEEE Infocom'98*, Volume 3, San Francisco, CA, April 1998, Page(s) 1241-1248.

[9] F. Le Faucheu, Ed. "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," IETF RFC 3270, May 2002.

[10] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS," IETF RFC 2702, September 1999.

[11] J. Moy, "OSPF Version 2," IETF RFC 2328, April 1998.

[12] R. Callon, "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments IS-IS," IETF RFC 1195, December 1990.

[13] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," IETF RFC 3209, December 2001.

[14] J. Ash, M. Girish, E. Gray, B. Jamoussi, and G. Wright, "Applicability Statement for CR-LDP," IETF RFC 3213, January 2002.

[15] T. Li, G. Swallow, and D. Awduche, "IGP requirements for Traffic Engineering with MPLS," IETF Internet draft <draft-li-mpls-igp-te-00.txt>, February 1999.

[16] T. Li and Y. Rekhter, "A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)," IETF RFC 2430, October 1998.

[17] B. Davie and Y. Rekhter, *MPLS Technology and Application*, Morgan Kaufmann Publishers, 2000.

[18] C. Perkins, Ed. "IP mobility support," IETF RFC 2002, October 1996.

[19] D. B. Johnson and C. Perkins, "Route Optimization in Mobile IP," IETF Internet Draft, <draft-ietf-mobileip-optim-10.txt>, February 2000.

[20] E. Gustafsson, A. Jonsson and C. Perkins, "Mobile IPv4 Regional Registration," IETF Internet Draft, <draft-ietf-mobileip-reg-tunnel-07.txt>, October, 2002.

[21] G. Heine, *GSM Networks: Protocols, Terminology and Implementation*, Artech Hourse Publishers, 1999.

[22] A. Campbell, J. Gomez, S. Kim, A. Valko, C.Y. Wan, and Z. Turanyim "Design, implementation and evaluation of Cellular IP," *IEEE Personal Communications*, Volume 7, Issue 4, August 2000, Page(s) 42-49.

[23] A. Valko, *et al.*, "Cellular IP, A New Approach to Internet Host Mobility," *ACM Computer Communication Review*, Volume 29, Issue 1, January 1999, Page(s) 50-65.

[24] A. Valko, J. Gomez, S. Kim, and A. Campbell "On the Analysis of Cellular IP Access Networks," *Sixth IFIP International Workshop of Protocols for High-Speed Networks (PfHSN'99)*, Salem, August, 1999.

[25] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 2nd edition, Addison Wesley, 2002.

[26] R. Ramjee, K. Varadhan, L. Salgarelli, S. Thuel, S.Y. Wang, and T. La Porta, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," *IEEE/ ACM Transactions on Networking*, Volume 10, Issue 3, June 2002, Page(s) 396-410.

[27] R. Ramjee, T. La Porta, L. Salgarelli, S. Thuel, K. Varadhan, and L. Li, "IP-Based Access Network Infrastructure for Next-Generation Wireless Data Networks," *IEEE Personal Communications,* Volume 7, Issue 4, August 2000, Page(s) 34-41.

[28] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and L. Salgarelli, "IP Micro-Mobility Support using HAWAII," IETF Internet Draft <draft-ietf-mobileip-hawaii-00.txt>, June 1999.

[29] R. Ramjee, T. La Porta, and L. Li, "Paging Support for IP Mobility using HAWAII," IETF Internet Draft <draft-ietf-mobileip-paging-hawaii-00.txt>, June 1999.

[30] R. Zhong, C.K. Tham, C.K. Foo, and C.C. Ko, "Integration of Mobile IP and Multi-Protocol Label Switching," in *Proc. IEEE ICC 2001*, Volume 7, Helsinki, Finland, June 2001, Page(s) 2123-2127.

[31] H. Kim, K.S.D. Wong, C. Wai, and L.C. Leung, "Mobility-Aware MPLS in IP-Based Wireless Access Networks," in *Proc. IEEE Globecom'01*, Volume 6, San Antonio, TX, November 2001, Page(s) 3444-3448.

[32] F.M. Chiussi, D.A. Khotimsky, and S.Krishnan, "A Network Architecture for MPLS-Based Micro-Mobility," in *Proc. IEEE WCNC'02*, Volume 2, Orlando, FL. March 2002, Page(s) 549-555.

[33] Kaiduan Xie and Victor C.M. Leung, "A MPLS Framework for Macro- and Micro- mobility Management," in *Proc. IASTED Wireless and Optical Communications (WOC'02)*, Banff, AB, Canada, July 2002

[34] Kaiduan Xie, Vincent W.S. Wong, and Victor C.M. Leung, "Support of Micro-Mobility in MPLS-based Wireless Access Networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, Louisiana, March 2003

[35] A. Campbell, J. Gomez, S. Kim, C.Y. Wan, Z. Turanyi, and A. Valko, "Comparison of IP Micro-Mobility Protocols," *IEEE Wireless Communications*, Volume 9, Issue 1, Febuary 2002, Page(s) 72-82.

[36] IEEE 802.11 standard, 1999.

[37] X. Zhang, J. Castellanos, A. Campbell, K. Sawada, and M. Barry, "PMIP: Minimal Paging Extenions for Mobile IP," IEFT Internet Draft <draft-zhang-pmip-00.txt>, July 2000.

[38] X. Zhang, J. Castellanos, and A. Campbell, "Design and Performance of Mobile IP Paging," *ACM Mobile Networks and Applications (MONET), Special issue on Modeling Analysis and Simulation of Wireless and Mobile Systems*, Volume 7, Issue 2, March 2002.

[39] Dionisios D. Gatzounas, *et al.*, "Route Optimization for Cellular IP networks," *in Proc. IP Cellular Network (IPCN) 2001*, May, Paris, 2001.

[40] A. Campbell and J. Gomez, "IP Micro-Mobility Protocols," *ACM SIGMOBILE MobileComputer and Communocation Review (MC2R)*, Volume 4, Issue 4, October 2001, Page(s) 45-54.

[41] K. D. Wong, H. Y. Wei, A. Dutta, and K. Yong, "Performance of IP Micro-Mobility Management Schemes using Host Based Routing," *Wireless Personal Multimedia Communications*, September 2001.

[42] P. Reinbold and O. Bonaventure, "A Comparison of IP Mobility Protocols," Technical Report Infonet-2001-07, University of Namur, June 2001.

[43] The Network Simulator: NS-2 notes and documentation and source codes: www.isi.edu/nsnam/ns/

[44] Columbia IP Micro-Mobility Software: http://www.comet.columbia.edu/micromobility/

[45] MPLS Network Simulator: http://flower.ce.cnu.ac.kr/~fog1/mns/

[46] Non Ad Hoc routing agent (NOAH): http://www.icsi.berkeley.edu/~widmer/mnav/ns-extension/

[47] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, New Jersey, 1996.

[48] C. Perkins, *Mobile IP Design Principles and Practices*, Addison-Wesley Longman, Reading. 1998.

[49] W. R. Stevens, *TCP/IP Illustrated: The Protocols*, Addison Wesley Professional, 1993.

[50] ETSI UMTS, "Selection Procedures for the Choice of Radio Transmission Technologies of the UMTS," Technical Report TR 101 112, 1998.

[51] A. Klemm, C. Lindemann, and M. Lohmann, "Traffic Modeling and Characterization for UMTS Networks," in *Proc. IEEE Globecom'01*, Volume 3, San Antonio, TX, November 2001, Page(s) 1741-1746.

[52] D. Staehle, K. Leibnitz, and P. Tran-Gia, "Source Traffic Modeling of Wireless Applications," University of Wurzburg, Technical Report No. 261, 2000.