CHAPTER II

LITERATURE REVIEW

2.1 Mobile Internet Protocol (Mobile IP)

Mobile IP (RFC 3344) [3] is a proposed internet standard that improves the previous Internet Protocol to support mobility. It allows a mobile host to move from one network to another without breaking the ongoing communication by assigning two Internet Protocol addresses to the mobile host. The first is Home Address which is fixed and the second is Care-of Address (CoA) which changes at each new point of attachment. There are two types of CoA [3], which are Foreign Agent CoA and Co-located CoA. Foreign Agent (FA) provides a Foreign Agent CoA by means of broadcasting Agent Advertisement messages periodically. The Mobile Node (MN) gets the Co-located CoA through some methods such as conducting Dynamic Host Configuration Protocol (DHCP) or using long term address owned by the MN which is utilized only when the MN is on the foreign network. Mobile IP resides in Network Layer [1] in providing internet mobility. This, therefore, makes Mobile IP not depend on the media where the communication takes place. A mobile host in Mobile IP can roam from one type of medium to another without breaking its connectivity.

Mobile IP consists of three main entities: MN, Home Agent (HA), and FA [1] [3]. Figure 2.1 shows the entities and their relationship in Mobile IP. MN is a device such as a cellular phone or a laptop which can roam from one network to another without losing connectivity and simply uses Internet Protocol Home Address to maintain the ongoing communication. HA is a router on the home network which keeps the current location of the MN by recording the MN's CoA. HA intercepts each packet sent by a device on the internet, called a Correspondent Node (CN), to the MN's Home Address and forwards the packets to the MN's CoA. FA is a router in the foreign network that helps the MN to inform the HA of its current location, provides a CoA for the MN, forwards packets from the HA to the MN and serves as a default router if the MN wants to send packets to another node in the internet.

There are three main phases in Mobile IP: Agent Discovery, Registration, and Tunneling [1] [3]. The MN finds out its HA or FA, identifies its current point of attachment, knows whether it has moved to a new network, and gets a CoA if it is connected to the FA during Agent Discovery phase. The HA and FA broadcast their existence periodically through Agent Advertisement messages. This allows the MN to

determine whether any agents are present or not. A MN may optionally force any agents to broadcast Agent Advertisement messages by sending an Agent Solicitation message. This is useful in the situation where the MN is moving very fast from one agent to another while the transmission rate of Agent Advertisement sent by the agents is too low [1]. Although security is one of the important parts, Agent Advertisement and Solicitation messages are not required to be authenticated in Mobile IP because of key management difficulties. The MN accepts the Agent Advertisement messages and decides whether it is in its home network or a foreign network. If the MN notices that it is in its home network, it operates like any other fixed host in the home network. On the other hand, if the MN detects that it has moved to a FA network, it obtains a CoA in that network.

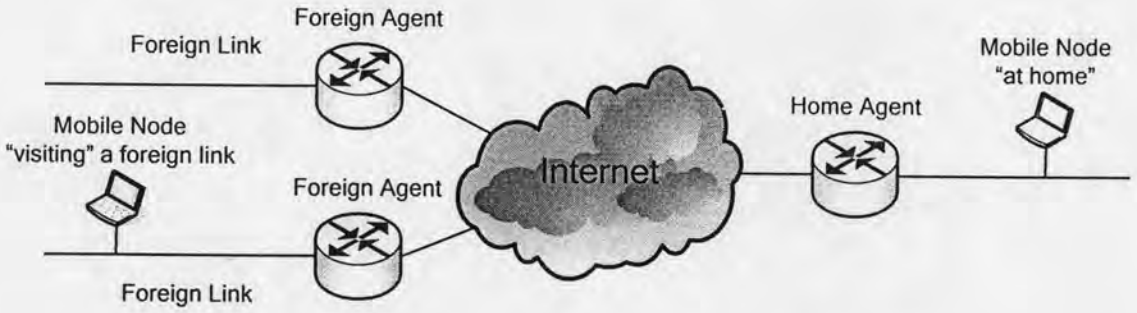

Figure 2.1 Mobile IP entities and relationship.

In Mobile IP, the MN uses two main methods to detect whether it has moved to another network or not. The first method of movement detection is by using Lifetime field within the Internet Control Message Protocol (ICMP) Router Advertisement portion of the Agent Advertisement. Here, when the MN has registered with one FA and fails to listen to an advertisement from that FA within the specified lifetime, the MN then assumes that it has moved to another network and registers with the next FA from which it has received another Agent Advertisement. The second method uses the network prefixes. The MN uses the network prefixes in the Agent Advertisement message to check whether it has moved to a new network or not. If the MN receives the same network prefixes as in its record, the MN deduces that it is still located in the same network. If the network prefixes are different, the MN concludes that it has moved to a new network and starts the registration process.

The MN registers its recent location with the HA during Registration [3]. The MN operating away from home network will register its new CoA every time it changes its point of attachment. Registration is also utilized by the MN to request forwarding services from the FA, to renew a registration which is due to expire, and to deregister when the MN goes back to the HA network. The MN, FA and HA

exchange information through registration messages which is valid for a specified lifetime. The MN conducts Registration by exchanging Registration Request and Registration Reply messages with the HA through current FA where the MN is now located. Using these messages, the HA can create and modify the mobility binding information of that MN, such as new lifetime and new CoA. Other scenarios of registration such as registration without FA if the MN uses Co-located CoA and direct registration when the MN returns to its HA are also possible.

A Registration Request message is first sent by the MN to the FA to start the Registration process. The MN uses the information within Agent Advertisement message to build the Registration Request message. Foreign Agent processes this message by applying a sequence of validity checks. If the message fails to pass the check, the FA rejects the registration by sending Registration Reply message with indicating the cause of rejection. If the Registration Request message is okay, the FA records certain information that is useful for routing of signaling and data packets. The FA then forwards the Registration Request to the HA. The HA also performs a set of validity checks when it receives the Registration Request. If the message passes the check, the HA updates the information of the MN in the routing table and later sends a Registration Reply message to the FA to inform that the registration is successful. If the registration is not successful, the HA does not update the information of the MN in its routing table and sends a Registration Reply with the reason of failure. The Registration Reply message sent by the HA takes the reverse path of the Registration Request message. The FA processes the Registration Reply by also conducting a set of validity check. If the security check is successful the FA updates its list of visiting MNs and delivers the Registration Reply message to the MN. When the MN receives that message, it performs a set of security check and sees whether the registration is accepted or not. If it is accepted, the MN adjusts its routing table to the current link and continues communicating. The MN can try to fix the error that caused the rejection of the Registration Request message and resends the message. If the MN does not receive the reply for a specified of time, it resends the Registration Request messages until it receives the Registration Reply message. Figure 2.2 illustrates the Registration process.

When a node in the internet, called a Correspondent Node (CN), sends data packets to the MN, the data packets are always delivered to the home network of the MN. The HA then intercepts the data packets. If the MN is in the home network, the data packets are routed with normal network prefix routing. In this case, no special procedures are needed to deliver the data packets to the MN. However, if the MN is in the foreign network, a tunnel [3] is then set up by the HA to the CoA of the MN to route the data packets. Before sending the data packets through the tunnel, the HA encapsulates the data packets by adding the CoA as the part of header to the packets

so that the packets can reach the endpoint of the tunnel. At the tunnel endpoint, the FA decapsulates the data packets to recover the original packets and delivers that data packets to the MN. The default tunnel mode is IP Encapsulation within IP Encapsulation. In this type of encapsulation, an Internet Protocol packet is put inside the payload portion of another Internet Protocol packet. The header of the encapsulated packet contains the information that is used to route the packet to the endpoint of the tunnel. Optionally, Generic Routing Encapsulation (GRE) and Minimal Encapsulation within IP may be used.

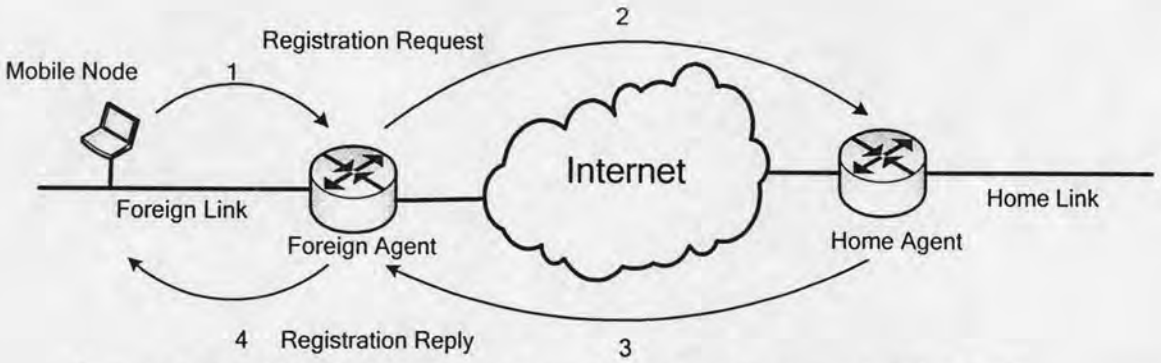

Figure 2.2 Mobile Node registers through the Foreign Agent in Mobile IP.

In the reverse direction, the MN delivers the data packets directly to their destination using standard Internet Protocol routing mechanisms, not necessarily sends them through the HA. The MN sends data packets using its Home Internet Protocol Address as the source address within the Internet Protocol packets. This keeps the information in the CN's record that the MN is located in its home network although in the real condition the MN is located in the foreign network. Although the MN moves from one FA network to another, the CN sends the packet with Home Internet Protocol Address as the destination address. Figure 2.3 shows the routing of data to and from the MN when it is in a foreign network and has conducted Registration process through the FA.

Security aspect is very important in Mobile IP since mobile computing environment is very vulnerable to many security problems such as passive eavesdropping and active replay attacks [3]. The MN and HA conduct authentication to Registration Request and Registration Reply messages by using Hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) as the default algorithm. The receiver of the message compares the authenticator value it computes over the registration messages over the value in the extension to verify the authenticity. The FA must also support authentication using HMAC-MD5 algorithm. Replay protection using Identification field in registration messages is used by the HA

to prevent the attacker replay the registration messages. The MN and HA implement timestamp-based or nonce-based for replay protection. Using the timestamp-based method, the node which is generating the message includes the recent time of day, and the node that is receiving the message verifies that this timestamp is close enough to its own time of day. If nonce-based method is applied, node A inserts a new random number in every message to node B and checks whether node B returns that same number in its message to node A.

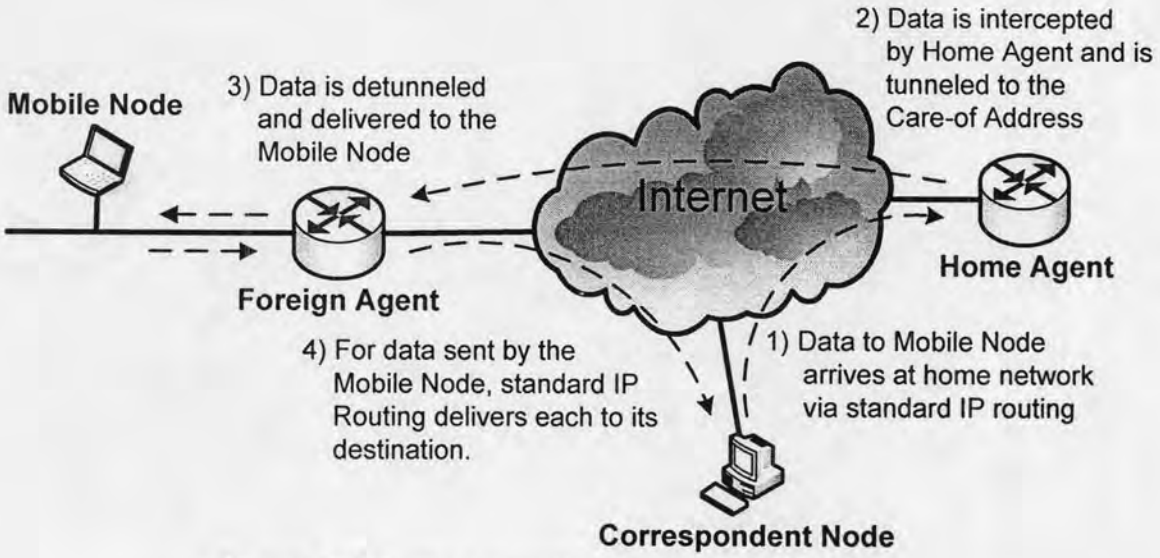

Figure 2.3 Routing operation in Mobile IP v4 [3].

As basic protocol for internet mobility, Mobile IP still suffers a lot of problems. The most outstanding problem facing Mobile IP is that of security [2]. However, other technical problems such as triangle routing that causes routing inefficiencies, inefficient direct routing that is measured in number of hops and end-to-end delay, inefficient HA notification since the MN has to notify its HA during each handover, ingress filtering that causes some data loss, encapsulation overhead, high handover latency, and high signaling load also have serious impact on the overall Mobile IP performances [2] [4]. These problems have resulted in the development of extensions and modifications to the classical Mobile IP as well as in the development of alternative approaches.

2.2 Paging Extensions for Mobile IP (Paging Mobile IP)

Currently, Mobile IP supports registration but not paging [4]. Paging is widely used in cellular systems when there is a call destined for the mobile. To make an easier mobility management, a group of cells construct a paging area under the control

of the same Mobile Switching Center (MSC) in cellular system. When there is a call for the mobile, the MSC sends paging messages to all base stations in the same paging area. Every base station then broadcasts the paging message in its own cell to search for the precise position of the mobile. After receiving the paging response from the mobile, the system knows the position of the mobile and can continue to establish the call.

Paging Mobile IP [4] adapts paging to Mobile IP by differentiating mobile users that are actively communicating or idle and introduces a concept of data session. An active MN is a MN which has just sent or received data. An active timer for a period of time is reset and restarted in the MN and FA each time the MN sends or receives data. When the active timer expires, the MN enters the idle state. The active time period forms a data session since more than one packet may be received or sent by the MN during an active timer period. Paging Mobile IP only needs to conduct paging process to find the MN on the first packet of the data session.

Paging Mobile IP extends the Mobile IP Agent Advertisement message to contain a "P bit". Paging Mobile IP assumes the use of FA which sets the "P" bit in the Agent Advertisement message to support paging and that the MN registers through them. When one MN receives Agent Advertisement message, that MN checks whether that message supports paging or not by looking at the "P bit". There is also a "P bit" in the Registration Request message. In Paging Mobile IP, an active MN registers when it changes its point of attachment from one FA to another. It acts exactly the same manner as in Mobile IP. An idle MN also registers when it moves to a new paging area. An idle MN, however, does not register when moving within the same paging area.

If a CN wants to send packets to the MN, it will first send the packets to the HA. The HA then delivers the packets to the MN's registered FA. The registered FA first finds whether it has any information in the record for the MN. If a record exists, then the registered FA checks whether the MN supports paging or not. If the MN supports paging, the registered FA checks the operational state of the MN. If the MN is in active state, the registered FA then decapsulates the packets and forwards the incoming packets to the MN. If the MN is in idle mode, the registered FA buffers incoming packets and then sends Paging Request messages to all other FAs that reside in the same paging area, as well as broadcasts the Paging Request message on its own network to search for the MN. When the MN receives the Paging Request message and finds that that message is destined for it, the MN checks whether it has moved from the last registered FA. If the MN finds that it is still located in the same cell it registered before, the MN sends Paging Reply message to the FA. If the MN has moved to new cell, it registers with HA through the current FA. After receiving the Registration Reply message, the MN sends Paging Reply message back to the FA it

had previously registered with through its current FA to inform the MN's current location to the previously registered FA. When the previously registered FA receives Paging Reply message, that FA forwards any buffered packets toward the MN through the current FA. After receiving the Registration Request from the MN, HA changes the destination of the data packets from the last registered FA to the current FA.

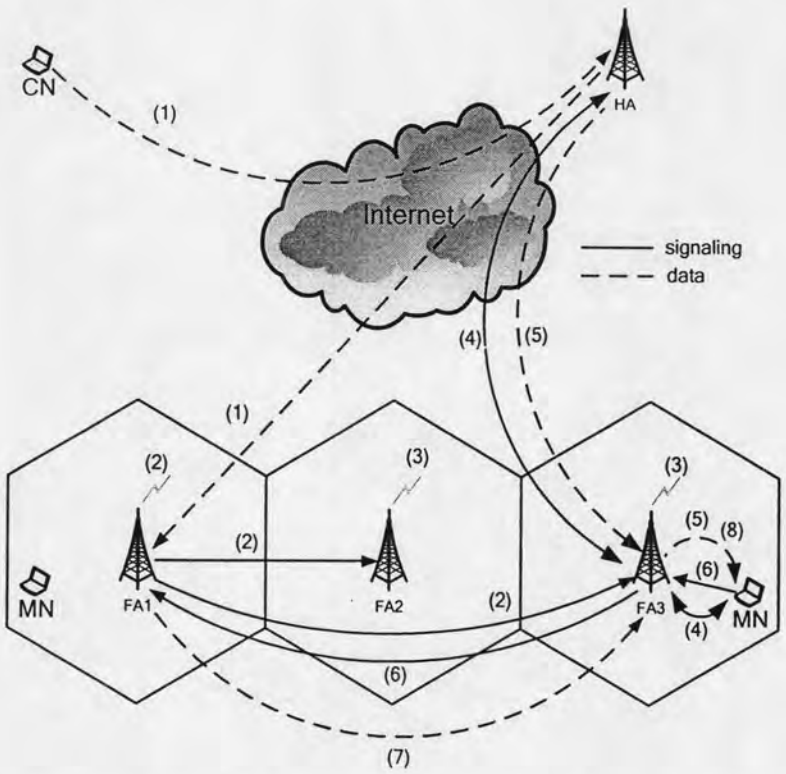

Figure 2.4 An example of paging scenario in Paging Mobile IP [4].

Figure 2.4 illustrates a simple paging scenario where Foreign Agents FA1, FA2, and FA3 form a paging area. An idle Mobile Node (MN) moves from the Foreign Agent FA1's cell to the Foreign Agent FA3's cell without registration. The Mobile Node's Care-of Address (CoA) record maintained at the Home Agent (HA) points to the Foreign Agent FA1. In this scenario, a Correspondent Node (CN) wants to send data packets (1) to the Mobile Node. The Home Agent (HA) encapsulates the packets and tunnels those packets to the Foreign Agent FA1. After Foreign Agent FA1 receives packets destined to the Mobile Node, the Foreign Agent FA1 checks whether it has a record for the Mobile Node. If Foreign Agent FA1 has a record, then it determines whether the Mobile Node supports paging or not. If this is the case, then Foreign Agent FA1 checks the state of the Mobile Node. In this scenario, the Mobile Node is in an idle state. As a result, the Foreign Agent FA1 starts to buffer packets and sends Paging Request messages (2). These Paging Request messages are

broadcast in Foreign Agent FA1's cell and unicast to Foreign Agents FA2 and FA3. Following this, Foreign Agents FA2 and FA3 broadcast the Paging Request messages (3) in their cells. The Mobile Node receives the Paging Request message (which includes its Home Address) in the Foreign Agent's FA3's cell (4) and registers its location with the Home Agent. The Home Agent starts forwarding data packets (5) toward the Foreign Agent FA3 and Mobile Node after the registration process is complete. In addition to action (4), Mobile Node sends a Paging Reply message (6) to Foreign Agent FA3. Foreign Agent FA3 forwards the Paging Reply message to the Paging Foreign Agent FA1. Foreign Agent FA1 forwards any buffered packets toward Foreign Agent FA3 (7) and deletes the record of the Mobile Node. Following this, Foreign Agent FA3 forwards data packets (8) to the Mobile Node.

2.2.1 Messages in Paging Extensions for Mobile IP

Paging Mobile IP uses more messages than the base Mobile IP. These messages are used for some purposes such as to indicate that MN or FA supports paging and to conduct paging process. Paging Area ID extension, as shown in Figure 2.5, is a new ICMP router discovery message extension. This Paging Are ID extension is used in non-overlapping paging area construction scheme. It should be added in the Agent Advertisement message, and periodically broadcast on the network.

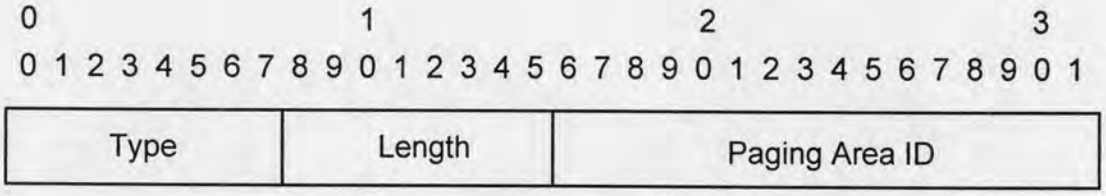

Figure 2.5 Paging Area Identification extensions.

Paging Request message is a new control message sent by registered FA to find the precise location of MN. The length of this message is 2 + 4*N, where N is the number of paged MNs. Length does not cover the type, length, and extensions fields. Sequence number is the count number of Paging Request messages sent to the MN. It is used to distinguish the Paging Request messages. If the same Paging Request message is sent to the same MN more than once, the sequence number is the same. Figure 2.6 illustrates the format of Paging Request message.

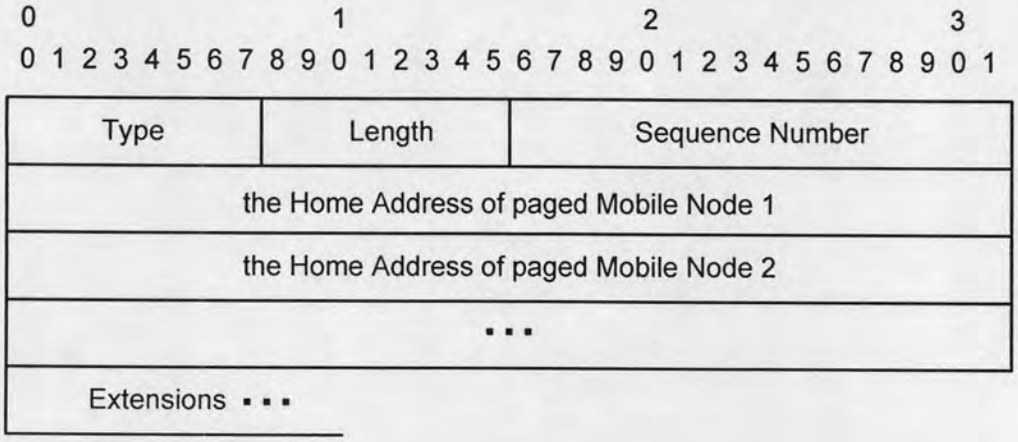

Figure 2.6 Paging Request message format.

Paging Reply message is another new control message in Paging Mobile IP. MN sends this message to the registered FA through the current FA to inform the exact location of the MN. The length of this message is 2 + 8*N, where N is the number of responding MNs. Length does not cover the type, length and extensions field. Paging Reply message format is shown in Figure 2.7.

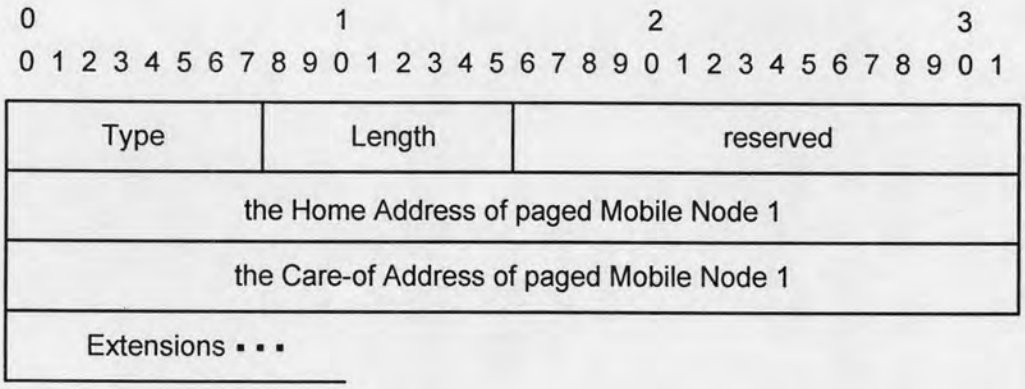

Figure 2.7 Paging Reply message format.

Paging Mobile IP also still uses two messages in the base Mobile IP with minor modifications. Registration Request message and Mobility Agent Advertisement extension are modified to support paging. Paging Mobile IP changes one of the reserved bits in the Registration Request message in Mobile IP to the "P bit" which indicates if the MN supports the paging function or not. A P bit of '1' means that the MN supports paging and a P bit of '0' means that the MN does not support paging. Modified Registration Request message format is illustrated in Figure 2.8.

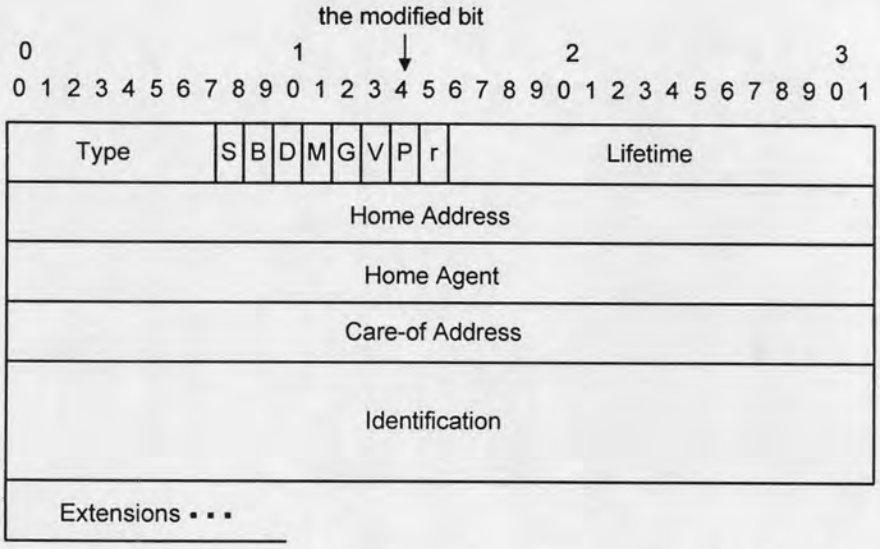

Figure 2.8 Registration Request message in Paging Mobile IP.

Paging Mobile IP changes one of the reserved bits in the Agent Advertisement used in Mobile IP to be "P bit" which indicates whether the FA supports the paging function or not. A P bit of "1" means that the FA supports paging and a P bit of "0" means the FA does not support paging. Figure 2.9 displays the modified Agent Advertisement message.

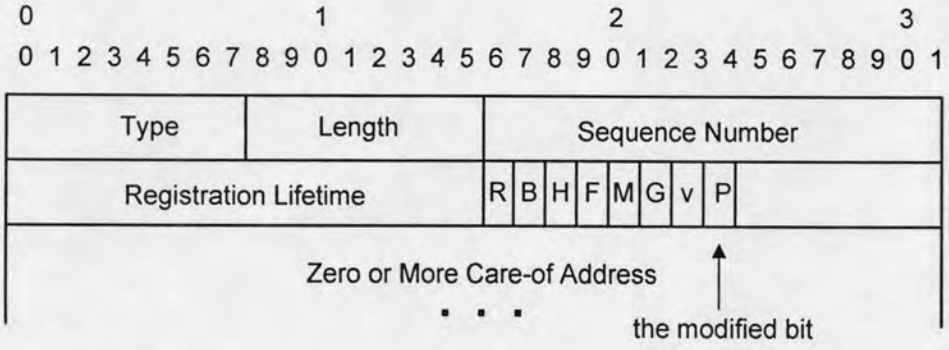

Figure 2.9 Mobility Agent Advertisement extensions in Paging Mobile IP.

2.3 Mobile IPv4 Regional Registration

Mobile IP Regional Registration [6] is an extension to the Mobile IP that is proposed to improve the performance in term of signaling load to the home network and the signaling delay related to handoff process. Gateway Foreign Agent (GFA) is a new entity in Mobile IP Regional Registration. GFA is a specialized router that essentially acts as a local proxy for the HA. GFA is located between FA and HA. To the HA, GFA appears as if the MN's temporary of address is that of the GFA. Two or

more FAs are administered under this entity within the same visited domain. The FA advertises the GFA's address in the Agent Advertisement message periodically. The network model of Mobile IP Regional Registration is shown in Figure 2.10.

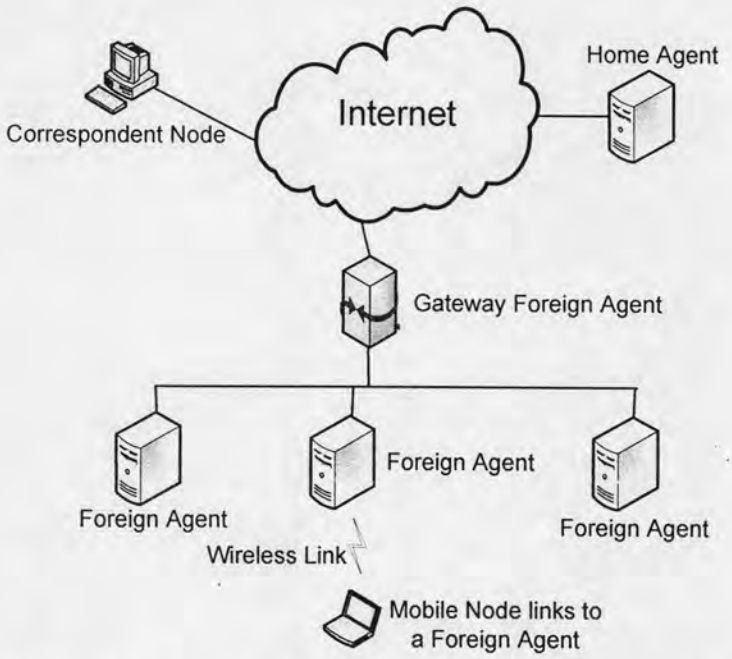

Figure 2.10 Mobile IP Regional Registration network model.

MN carries out home registration with the HA when the MN enters the visited domain for the first time, when the MN changes its GFA, and when the MN's registration lifetime almost expires. The MN registers the GFA's address as its CoA to the HA by exchanging Registration Request and Registration Reply messages with the HA. The MN inserts the GFA's address in the Registration Request message and relays that message to the FA. When the FA receives this message, it finds the GFA to which the message should be relayed. The FA adds its own address in the message and sends the message to GFA. The GFA then forwards the Registration Request message to the HA. The HA then sends Registration Reply message to MN via GFA and FA as the response of Registration Request message. The HA will keep GFA address as the MN's CoA as long as the MN moves within the same GFA domain. Figure 2.11 demonstrates the signaling message flow for home registration.

When moving from one FA to another within the same domain under one GFA, the MN does not need to register to the HA. Instead, the MN performs regional registration with the GFA to register its new FA CoA by using a new pair of registration messages. Regional Registration Request and Regional Registration Reply messages are used for intra-site signaling within a domain by the MN, FA, and GFA for regional registration purposes. When the MN receives Agent Advertisement

message from the new FA, the MN performs regional registration with this FA and GFA. The MN transmits a Regional Registration Request to the GFA via the new FA. Based on the information in this message, the GFA updates the MN's current point of attachment in its visitor list. The GFA then sends a Regional Registration Reply to the MN via the new FA. Figure 2.12 indicates the Regional Registration process when a MN changes the FA under the same GFA.

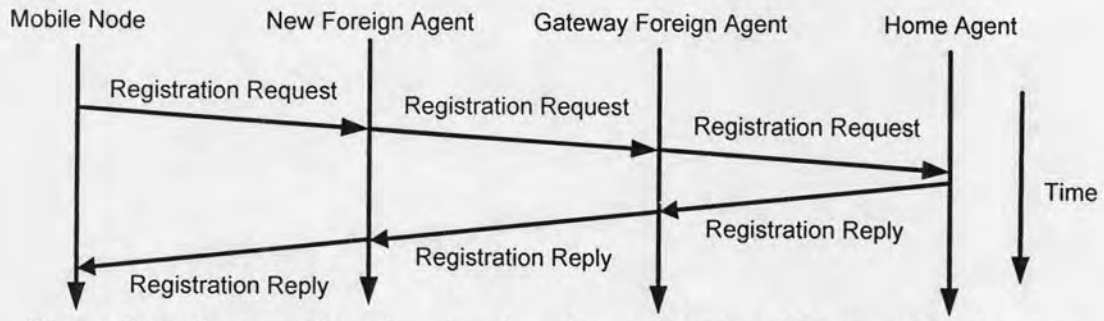

Figure 2.11 Home registration signaling flow in Mobile IP Regional Registration.

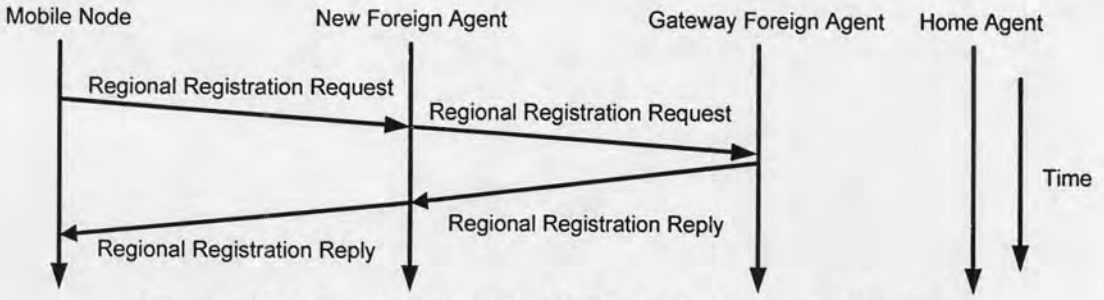

Figure 2.12 Signaling flow in Mobile IP Regional Registration.

2.4 Internet Protocol Multicast

Internet Protocol version 4 uses three fundamental methods for transmitting data packets over the network: unicast, broadcast, and multicast [1]. Unicast traffic is sent to a single point of destination such as a host computer, laptop, web server, or a particular end user. Broadcast traffic is delivered to all users in the network. Multicast traffic is sent to a specific subset of the network users or a group of users. In multicast, participants of the communication must be identified and the traffic must be sent to their specific locations. Multicast can utilize the available bandwidth efficiently since the source does not send the traffic to unnecessary destinations. Several applications in the internet such as data casting, video and audio transmissions and training seminars depend on multicast technology.

There are several processes that must take place to successfully establish multicast communication. The first step is the identification of receivers. All of the hosts that want to receive the multicast packets must inform themselves to the network. This is called registration process and it is facilitated with a unique set of Internet Protocol addresses, also known as Internet Class D Addresses, which has range of 224.0.0.1 through 239.255.255.255. This range of address is reserved specifically for multicast communication. The Internet Protocol multicast packets also contain the Internet Protocol destination addresses within this range. The receiver registers with a particular group to receive multicast traffic. The node sends special messages to multicast router, which is a router that has the capability to route multicast packets, to be a member of the group. Internet Group Management Protocol (IGMP) specifies the messages that are used to join multicast groups. Specifically, IGMP Host Membership Reports are sent by nodes that want to join multicast groups. IGMP is considered to be the part of the network layer. These messages are transmitted within the payload part of IP packets. To send multicast packets, a node simply assigns a specific group Multicast Address as its destination address of the packets. It is possible that a node sends the multicast packets without being a member of the destination multicast groups.

Multicast groups are often denoted by "G," and sources are indicated with the abbreviation "S." Together, a group and source combination can be represented by the notation (S, G). To represent specific groups or sources, notation such as (S_1, G_1) can be used. If there are multiple sources for one multicast group, notation like (*, G_1) is used to indicate any possible source for a particular multicast group. Once receivers join the respective groups, the network must deliver the multicast traffic to the correct stations. Multicast routers use a special multicast routing protocol such as Protocol Independent Multicast-Dense Mode (PIM-DM), Protocol Independent Multicast-Sparse Mode (PIM-SM), Core Based Trees (CBT), and Distance Vector Multicast Routing Protocol (DVMRP) in order to exchange the information about the individual members of each group. This information is then used to decide the appropriate forwarding paths to all registered receivers. Each multicast router computes a delivery tree that describes how multicast packets are to be routed to members of each group. Multicast routing delivers packets using special algorithms which prevent packets from being duplicated unless they absolutely have to be at some network point. Therefore, data packets can be received in multiple locations simultaneously. Every multicast routing has its own unique strengths and weaknesses.

On the foreign link, one MN can be either a sender or a receiver of multicast packets. As a sender, the MN must not send multicast packets directly using its Home Address; otherwise, multicast routers will fail to send the packets to all groups of receivers. The MN has two choices in this case. First, the MN can send it to the HA.

Alternatively, a MN with Collocated CoA can use that address as the Internet Protocol source address of its multicast packets and transmit them directly on the foreign link. As a receiver, the MN also has two options to receive multicast packets. The first option, the MN joins the multicast delivery tree by way of the HA. In this option, the MN tunnels IGMP packets to the HA. In another choice, the MN joins the multicast delivery tree by way of a multicast router on a foreign link. The MN directly sends the IGMP Host Membership Reports on the foreign link.

2.4.1 Protocol Independent Multicast - Sparse Mode

There are several multicast routing protocols. Each of them has its own unique characteristics. Protocol Independent Multicast-Sparse Mode (PIM-SM) [11] is one of these multicast routing protocols. This multicast routing protocol was developed in the late 1990s. The name Protocol Independent Multicast is derived from the fact that this routing protocol is not dependent upon any specific routing protocol. Instead, it takes benefit of the existing routing tables in order to forward multicast data. PIM-SM is suitable for internet since it lowers the overhead and bandwidth requirements for multicast data streams. Here, the routers must specifically request a particular multicast stream before the data is forwarded to them. This protocol exists between routers and does not involve the source and the destination. Similar to any other routing protocol, PIM-SM also shares many of common characteristics such as discovery messages, topology information, and error detection.

PIM-SM routers periodically generate "Hello" messages to discover and maintain sessions with neighbors. After neighbors are discovered, PIM-SM routers can indicate their intention to join specific multicast groups. This is accomplished by having a downstream router send an explicit PIM-SM "join" message to the upstream router. The "join" message will specify the group and the source that the router wants to join. The upstream routers can then forward multicast information to the downstream devices. PIM-SM, like most other multicast routing protocols, implements forwarding trees for each multicast group. These trees are called Rendezvous Point Trees (RPT) since they rely on a central router called a rendezvous point. The routers involved in PIM-SM networks must keep track of the state of various other routers, as well as the trees, to reach all of the receivers. Stateful information must be maintained for every multicast group. This can have some severe scalability implications since all routers must dedicate substantial resources to these processes. In order to offload the majority of the routers, PIM-SM has centralized some of these functions by using a router called the rendezvous point (RP). Each multicast group has its own rendezvous point that is responsible for forwarding information from the source to all of the receivers. In essence, the RP is the root of the RPT. The diagram in Figure 2.13 shows an example of a typical RPT. The multicast

source on the left transmits data to the First Hop Router (FHR). The FHR knows the location of the RP for that particular group, so it will forward the data to the RP. The RP will be the root of the RPT, so it will then distribute the multicast data to all of the registered receivers.

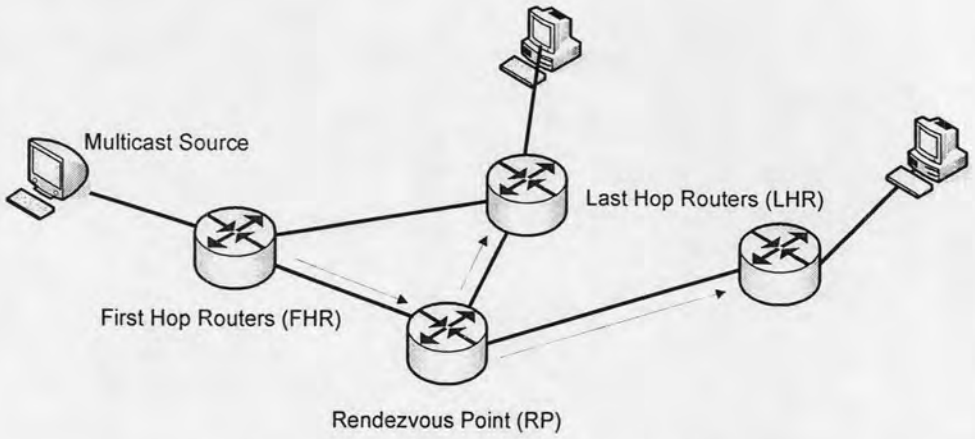

Figure 2.13 Typical Rendezvous Point Tree.

In order to join the tree in which the FHR will use for transmitting data packets to the RP, the FHR sends a "register" message to the RP. The register message is a unicast message addressed directly to the RP. The multicast data from the source is encapsulated in the register message so that the RP can forward the data while adding the source to the tree. These packets are called "register-encapsulated" packets, and they continue to be sent until the RP sends a "register stop" message to the FHR. After receiving a "stop" command from the RP, the FHR will continue to transmit standard multicast packets along the RPT.

While sending multicast data from the first hop router to the RP, it is highly possible that an intermediary router that acts as a LHR will be encountered. If that happens, it would be inefficient to send the multicast data to the RP and then have the RP transmit the data back to the intermediary router. Therefore, the intermediate routers are able to directly deliver the multicast packets to their registered clients, in addition to forwarding a copy to the RP. Finally, when a LHR no longer requires multicast data from a particular group, it sends a "prune" message to the RP. That router will be deleted from the RPT.

2.5 Low Latency Handoff in Mobile IP version 4 using Post-Registation Handoff Method

Low Latency handoff [8] has been proposed to minimize handoff latency and the number of lost packets by Internet Engineering Task Force. It utilizes Link Layer information to start handoff. Facilities of Link Layer information, such as signal strength, bit error rate, and signal to noise ratio, are used by the MN to detect whether the MN has entered a new network or still resides in the old network. Using Link Layer information, the MN can detect the new connectivity with new FA faster than using Network Layer information in Mobile IP. There are two types of Low Latency handoff: Pre-Registration Handoff and Post-Registration Handoff. Here, Post-Registration Handoff is discussed.

Post-Registration handoff scheme uses Link Layer trigger to set up a Bi-directional Edge Tunnel (BET) that allows the MN to continue using its old CoA while it is on the new FA subnet. The scheme is based on a network-initiated handoff model by means that the MN is not involved in performing the handoff process until the actual Link Layer connection with the new FA is completed. In Post-Registration handoff method, instead of making a new registration with the new FA, the MN defers the Network Layer registration while maintaining the connection using the BET to tunnel the packets from the old FA to the new FA.

The Post-Registration concept utilizes the old FA to be the mobility anchor point for the MN, called the anchor FA. When the MN moves from the old FA to the new FA, rather than performing signaling over the wireless link to register to new FA, the MN can defer the Network Layer handoff and continue using it's anchor FA (that is the old FA in this case) as shown in Figure 2.14. After the BET is established, the traffic is tunneled from the old FA to the new FA so that the MN continues to receive service through the BET without registration to the new FA. At sometime in the future, the MN will eventually register to the new FA. The signaling time diagram is shown in Figure 2.15.

Two network-initiated handoffs are defined: source trigger and target trigger handoffs. Here, target trigger received at the new FA is described. The new FA receives Link Layer Target Trigger informing that the MN is about to associate with it. The new FA then sends Handoff Request to the old FA. The old FA then replies with Handoff Reply message to new FA. This establishes the BET between the old FA and the new FA. The MN loses the connection with the old FA when the Link Layer Link Down is received at the old FA. The MN is the fully connected to the new FA when the Link Layer Link Up is received at the new FA.

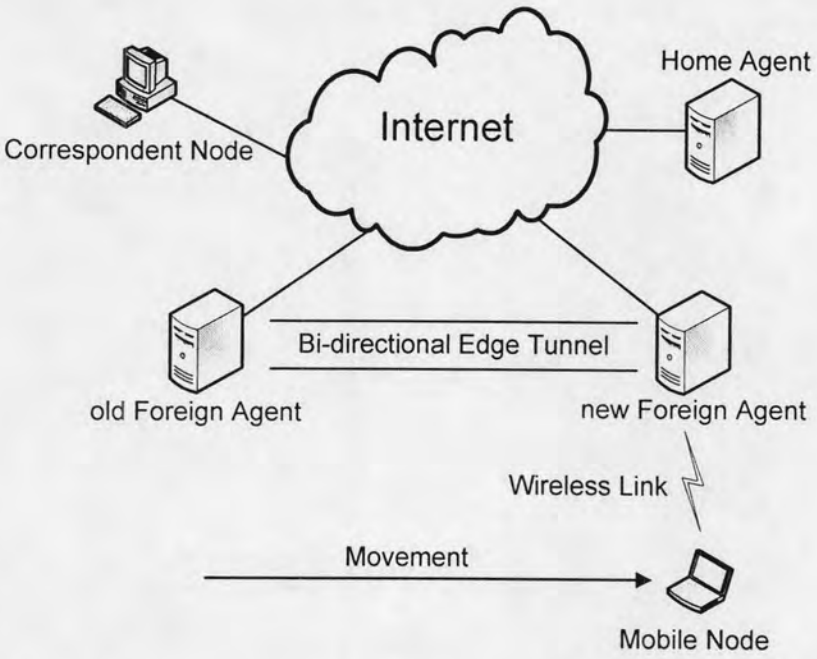

Figure 2.14 Post-Registration concept in low latency Mobile IP v4 handoff.

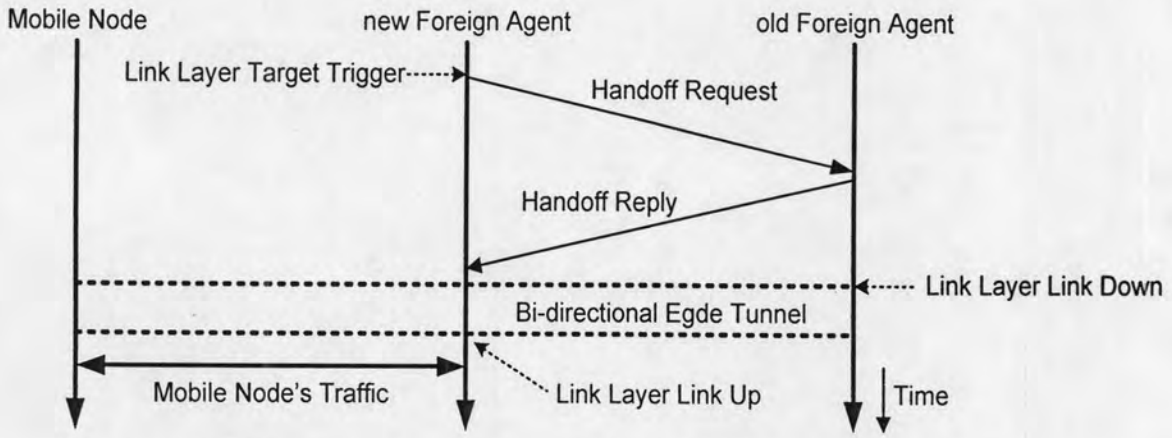

Figure 2.15 Signaling time diagram in Post-Registration environment.

2.6 Related Works

As mentioned before, Mobile IP still has many problems. One of them is the limited capability of Mobile IP to support the environment, in which the MN changes its point of attachment to the network so frequently that Mobile IP introduces significant overhead in terms of delay, number of packet lost, and signaling load [12]. This problem especially occurs when Mobile IP has to support real time services, such as Internet telephony and video conferencing, while it still has to achieve low latency and minimum lost packet during handoffs [13]. Many works have been proposed to solve these problems.

Reference [7] combined Mobile IP Regional Registration with Paging Mobile IP. In this scheme, when there are packets sent to a MN, the packets are forwarded by the HA to the GFA to which the MN has registered. The GFA then checks whether the MN supports paging or not. If the MN supports paging, the GFA checks the operational state of the MN in its record. If the MN is in active mode, the GFA encapsulates the packets and forwards them to current FA where the MN is now located. The FA then decapsulates packets and forwards them to MN. If the MN is in idle mode, the GFA buffers incoming packets and sends Paging Request messages to all FAs that reside in the same paging area under the same GFA. When the MN receives Paging Request message, it registers to GFA. After receiving Regional Registration Reply message, the MN sends a Paging Reply message back to GFA and the GFA then delivers the buffered and incoming packets to the MN. Figure 2.16 shows the signaling time diagram when there are packets sent to an idle MN.

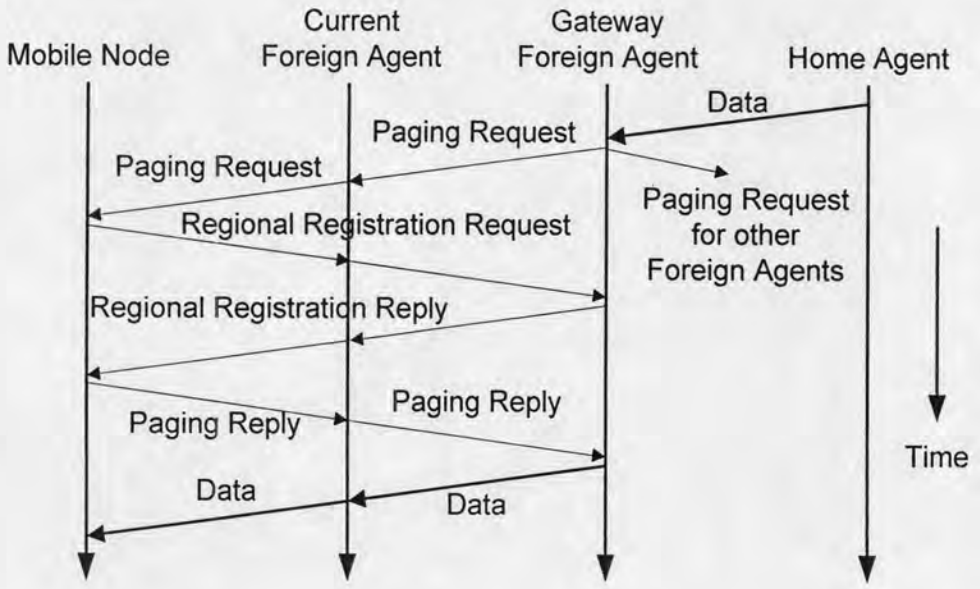

Figure 2.16 Signaling time diagram when there are packets sent to idle Mobile Node in [7].

Reference [5] improved the performance of Paging Mobile IP by reducing the number of lost packets and handoff latency by using the main idea of Post-Registration (Low Latency handoff) [8]. This is done because Paging Mobile IP still uses basic Mobile IP registration procedure, in which the registration can take a long delay if the distance between the MN and its HA is large. Registration delay method is proposed in two phases, which are when the MN is in the active state and when there are incoming packets destined to the MN. Post-Registration scheme is used during active state to reduce the movement detection time. In Paging Mobile IP, the current network is detected when the MN receives Agent Advertisement message in

Network Layer periodically every one second. Using Post-Registration method, where the Link Layer beacon is sent every 100 ms, allows the MN to detect that it has moved to another FA area faster than that of Network Layer in the Paging Mobile IP algorithm. When there are packets destined to the MN, the MN defers the registration process and keeps using the registered FA's Care-of Address while the MN is on the current FA's subnet and receives packets through the BET. BET is established between the registered FA and the current FA. Then, the MN can obtain these packets fast before the MN registers to the HA.

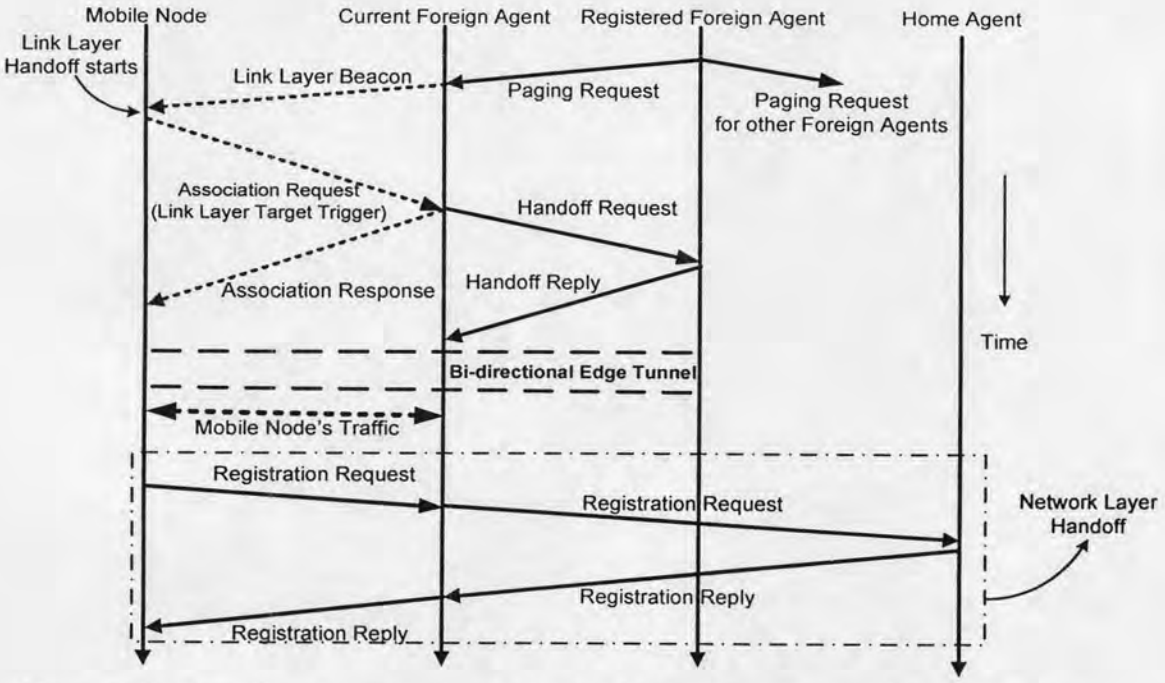

Figure 2.17 Signaling time diagram while the Mobile Node is entering active state in [5].

When there are packets destined for the MN, these packets are always sent to HA. The HA then forwards the packets to the registered FA. If the registered FA has the information of the MN, it checks whether the MN supports paging. If the MN supports paging, the FA checks the state of the MN. If the MN is in the active state, the FA decapsulates the packets, forwards them to the MN, and enters the Post Registration scheme. If the MN is in idle state, the registered FA buffers the packets and sends Paging Request messages to all FAs that reside in the same paging area and broadcast Link Layer beacon to search for the MN. Every FA that receives the Paging Request also broadcasts Link Layer beacon in its own cell. When the MN receives the Link Layer beacon, it associates with the current FA by sending Association Request message. This message has the function as Link Layer Target Trigger for the FA. In return, the FA sends Association Response message to the MN. Association Request

message will trigger the current FA to send Handoff Request message to the registered FA. The registered FA then replies with Handoff Reply message to form the BET between the registered FA and current FA to forward the buffered data packets in the registered FA. Sometime in the future, when the MN receives Agent Advertisement message from the present FA, the MN registers to the HA and the data packets will be sent to the MN via the new FA. Figure 2.17 shows the signaling time diagram of Reference [5] while the MN is entering the active state.

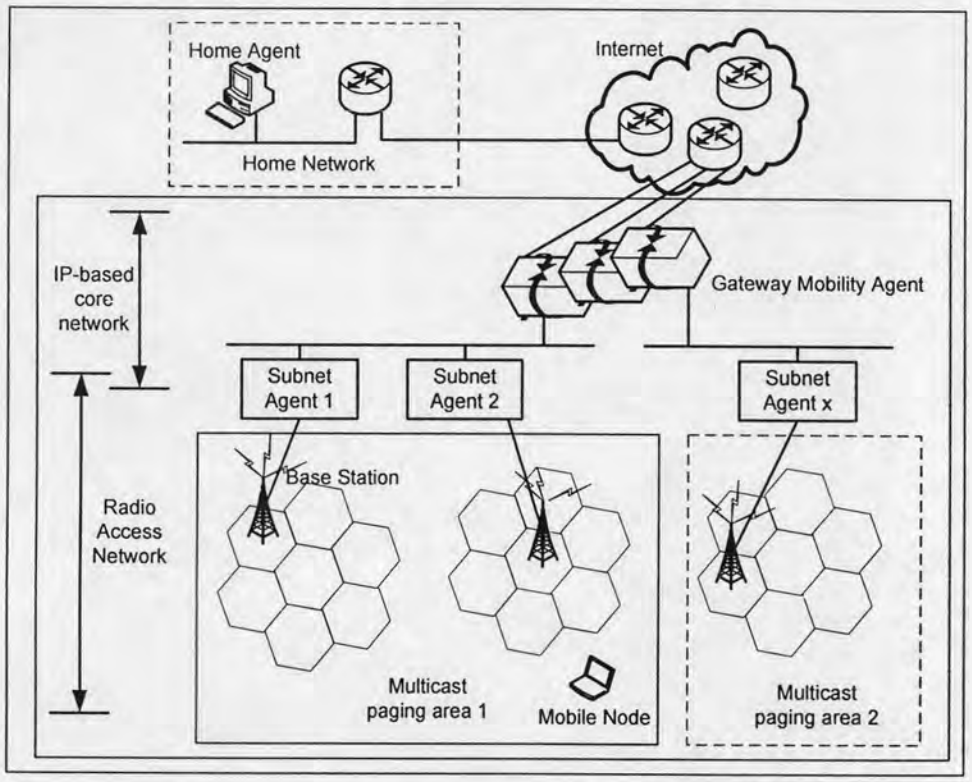

Figure 2.18 Network configuration of Micro-Mobile IP [9].

Micro-Mobile IP [9] is an extension to the Mobile IP Regional Registration. The motivation is that the Mobile IP Regional Registration lacks support for fast handoffs as well as for paging. Micro-Mobile IP implements the same hierarchical structure as Mobile IP Regional Registration. The network architecture is based on a two-level hierarchy. Figure 2.18 illustrates the configuration of Micro-Mobile IP. To achieve low-latency handoff, Micro-Mobile IP employs proactive handoff. Here, the MN receives Link Layer handoff trigger and subsequently reads the FA advertisement through the target access point. The MN returns to the serving access point, sends a registration with the CoA set to the target FA and requests bi-casting of Internet Protocol packets. The MN then completes Link Layer handoff. For paging purposes, idle state is governed by the lifetime timer, while the overall binding information, such as the CoA and Home Address, is held within the MN, Gateway Mobility Agent

(GMA), and HA. The paging mechanism relies on manually configured Subnet Agent (SA) paging groups. When there is a packet for an idle MN, the GMA where the MN is now located immediately begins to buffer all packets destined to that MN. The GMA uses multicast to send Page Solicitation messages, which are broadcast over access points. The paged MN responds by sending a Registration Request message. The Registration Request message creates binding information of the MN in the new SA as well as updates the MN binding information in the GMA. The GMA then sends a Registration Reply message. Following this, the GMA forwards the buffered and incoming packets to the MN via the current SA.

Reference [12] proposed a fast and efficient handoff scheme that supports the handoff of MN that crosses wireless cell boundaries frequently. They adopted a Domain Foreign Agent (DFA) concept to hide the mobility of MNs within the foreign domain from the HA. No location update to the HA is needed when the MN is moving within the domain of DFA. This approach eliminates any location update traffic going across the wide-area network. Multicast is employed as the packet forwarding mechanism from the DFA to the Base Stations (BS) in the vicinity of the MN. When a MN enters the DFA domain and registers with it, the DFA assigns a multicast address unique for the MN in the domain. The MN notifies the present BS to subscribe to this multicast group because the multicast packets are forwarded by the DFA to this group. Serving BS then tells all physically adjacent BSs to subscribe to the same group. There is only one BS that forwards data to the MN, other BSs in the same group buffer the packets. The buffered packets are forwarded to the MN if the MN moves to another BS area. Figure 2.19 shows the flowchart of their proposal.

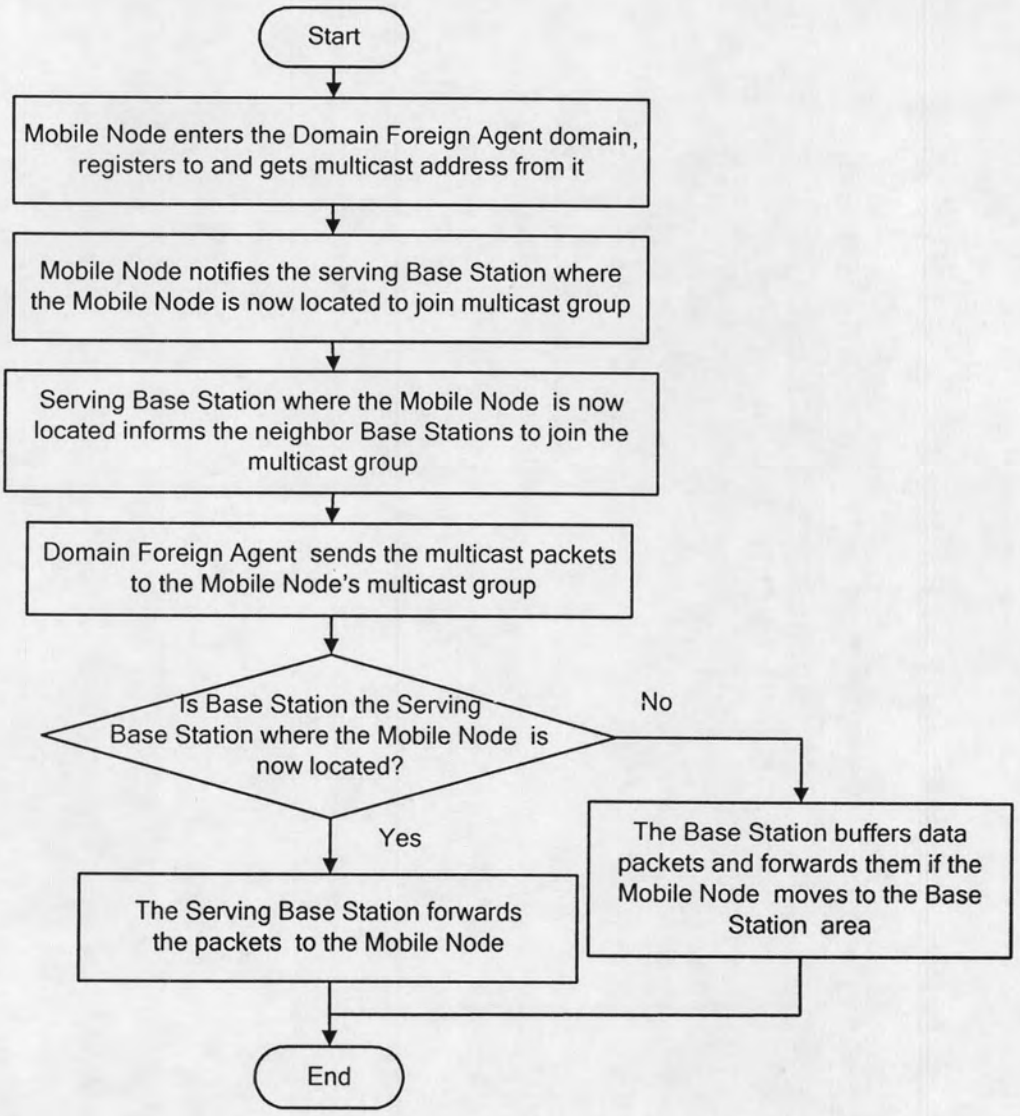

Figure 2.19 Flowchart of Mobicast protocol.