CHAPTER 5

ROUTE OPTIMIZATION IN MOBILE IP

5.1 INTRODUCTION

The convergence of wireless and IP network has led to the need for IP to handle mobility. The Mobile IP protocol was developed to facilitate IP mobility. However, it has a number of shortcomings for dynamically auto-configured networks. Mobility protocols like MIP with location registers and Session Initiation Protocol (SIP) have been developed to address some of its shortcomings. Micro-mobility protocols like Cellular IP and HAWAII have been developed to support fast seamless hand-off.

Mobile IPv4 (Perkins 2002) describes how a Mobile Node (MN) can perform IPv4- layer hand-off between subnets served by different Foreign Agents (FAs). In certain cases, the latency involved in hand-off can be above the threshold required for the support of delay-sensitive or real-time services. This research work presents EACS protocol supports layer-2 hand-off which triggers the layer-3 hand-off to achieve low-latency MIPv4 hand-off during movements between FAs. The proposed route optimization technique allows greater support for real-time services on MIPv4 network by minimizing the period of latency time. During this time an MN is unable to send or receive IPv4 packets due to the delay in the MIPv4 registration process. One or more of these techniques may be required to achieve fast Mobile IPv4 hand-offs over different wireless technologies (e.g., WLAN, Cellular, WiMAX, etc.). Each wireless technology has different layer-2 hand-off procedures and the
best low-latency technique for each scenario should be used to optimize the hand-off performance.

5.2 OVERVIEW OF MOBILE IP

Mobile IP (Perkins and Johnson 2000) has been developed in the IETF standard for mobility management of IP. That is, Mobile IP is a network layer solution for mobility management. The wireless network in the Mobile IP architecture has three basic elements: the Home Agent (HA), the Foreign Agent (FA) and the MN. Even though there are differences in details, the two versions of Mobile IP share the same key idea. The MN registers its location, that is, the Care of Address (CoA) to be used in the visited network with the HA. Any packet heading for the MN can be forwarded to the MN using tunnelling. A problem with Mobile IP is large hand-off latency. This large latency may adversely affect application QoS during hand-off.

Every MN has a home address that is used and routable in the home network of the MN. Correspondent Node (CN) is a communicating node with the MN. The main objective of Mobile IP is to enable the CN and the MN to communicate continuously even while the MN is away from its Home Network (HN). An important feature of Mobile IP is that the CN may not be aware that the MN is roaming during their communication. That is, the CN may send packets whose destination IP address is the HN of the MN no matter where the MN is located. Figure 5.1 shows the network architecture with Mobile IP. When an MN is away from its HN and visiting an FN, the MN is attached to the FA serving the visited network.
Figure 5.1 Mobile IP architecture

An FA is a router and the main functionality of the FA is to provide the list of temporary addresses that can be used by the visiting MNs in the visited network. Such temporary addresses are called CoA. The FA periodically broadcasts the advertisement messages that contain the list of CoAs available from the FA. When an MN wants to be connected to the network via the FA, the MN selects one of the CoA from the advertisement message and starts the registration procedure.

The main objective of the registration procedure is to let the HA of the MN know the selected CoA of the MN. The HA maintains a record of the CoA of each MN served by the HA. In Mobile IPv6, the registration is called binding because, it binds a CoA with an MN. The binding table is a logical storage of the binding records. The binding table is similar to the Home
Location Register of the cellular network in which it stores information about MNs’ current locations.

There are two types of CoA: FA-located CoA and co-located CoA. The FA-located CoA is an address of the FA and the co-located CoA is an IP address which is valid in the visited network and assigned to the MN for temporary use during its visit. A temporary IP address assigned through DHCP is a kind of co-located CoA. Figure 5.2 shows the registration procedure of Mobile IP. After selecting a CoA from the FA advertisement message, the MN sends a Registration Request to the FA. The Registration Request message contains the home address and the selected CoA of the MN and the HA address. The FA forwards the message to the HA of the MN.

**Figure 5.2 MIP hand-off message flows**
Then the HA updates the binding record of the MN with the new CoA and sends a Registration Reply to the FA. The FA also maintains a binding table for visiting MNs. The binding table is also updated with the CoA and the home address of the MN. Then the FA forwards the Registration Reply message to the MN.

Once the registration procedure is completed, the user traffic for the MN is transferred as follows. The CN sends packets with the MN’s home address as the destination IP address. Then the packets arrive in the HN, in particular, in the subnet where the MN’s home address is valid. Then the HA intercepts the packets and encapsulates them with another IP header, where the destination address is the CoA of the MN and the source address is the HA address. The HA sends the encapsulated packets and those packets are transferred to the FA corresponding to the CoA. The FA decapsulates the packets by removing the external header and forwards only the original packets to the MN.

The packets are transferred from the HA to the FA using IP encapsulation and is called tunnelling. The arrows from CN to HA, HA to FA, and FA to MN show the user traffic from the CN to the MN as shown in Figure 5.1. The arrow from HA to FA is different from the other two because tunnelling is used in this portion. It is also said that there is a tunnel between the HA and the FA in this case. The starting end of a tunnel is the node encapsulating packets and the finishing end of a tunnel is the node decapsulating packets. Obviously, the tunnel between the HA and the FA is established during the registration procedure described above.
When the MN sends packets to the CN, the packets can be transferred to the CN by normal IP routing. Since the IP routers look up only the destination address of the packet for routing, the packets from the MN to CN is not encapsulated.

In that case, such routers in the visited network discard the packets from the MN because the home address of the MN is not topologically correct. A solution for this case is to establish a tunnel between the FA and the HA for the packets from the MN. Such a tunnel is called a reverse tunnel. When the MN selects a co-located CoA, the CoA is assigned to the MN for temporary use. The tunnel starting at the HA ends at the MN rather than the FA in this case, that is, the MN decapsulate the packets encapsulated by the HA.

As shown in Figure 5.1, the user traffic from the CN to the MN traverses a network path via the HA with base Mobile IPv4. This is called ‘triangular routing’ because most likely the route is not the shortest path from the CN to the MN. It is a consequence of the Mobile IPv4 design that the CN is not aware of the MN’s mobility. It is a good characteristic in the sense that it makes it easy to deploy Mobile IPv4 since nothing needs to be done in the CN to support mobility of MNs. However, using the shortest path is preferable when the user traffic is isochronous. Route Optimization (Perkins and Johnson 2000) was introduced so that the user traffic from the CN to the MN follows the shortest path. The idea is that the HA informs the CN of the MN’s CoA and the CN then encapsulates its own packets and sends them to MN’s CoA. That is, the CN becomes the end point of the tunnel. Route Optimization is a separate protocol for Mobile IPv4 for optimising the route between CN and MN.
5.3 RELATED MOBILITY MANAGEMENT TECHNIQUES

Some wireless link layers are able to maintain traffic flow between the old AP and the MN while a new CoA is established through the new AP. This process is called make-before-break handover (Hartstein et al 2000 and Corson et al 2002). This is different from soft handover supported by CDMA (for example 3GPP2 2002). Since in soft handover, the IP layer never sees the backward link as such, it cannot utilize it for maintaining traffic flow during the CoA change. If the link layer provides make-before-break handover support, no change is required in the default Mobile IP subnet movement algorithm, since the MN can continue receiving packets through the old link until the routing change becomes effective on the HA. For the more typical break-before-make handover case, where the old link is broken before the new one is completely up, additional support for fast handover may be necessary. One technique to reduce packet loss is to buffer traffic while the link switch and routing changes are underway.

Proposals have been made to buffer at the AP (Balakrishnan et al 1995) and at the FA (Seshan and Katz 1997). Buffering at the AP requires the AP to perform proxy Address Resolution Protocol (ARP) to maintain the illusion that the MN is still on the subnet after it has moved. The process of opening up a security hole with an attacker should try to intercept the traffic. Buffering at the old FA requires the FA to buffer all traffic using a sliding window and download the buffer to the Mobile Node. The FA at that time receives a Previous FA Notification message (Perkins 2001) from the MN on the new subnet.

In general, the buffering algorithms do not directly address the source of handover latency in standard Mobile IP handover, but rather attempts to mitigate it. While results for TCP traffic have been good,
buffering may introduce artifact into streaming media and real-time traffic. Excessively large buffers of streaming media or real-time traffic can cause "ringing" on slow links after the handover. This effect of the handover is dissipated. However, a limited amount of buffering may be useful in conjunction with link synchronous approaches for packet drops which cannot be eliminated, such as complete loss of network layer service during switching of the link.

Multicasting packets from the HA to Foreign Agents surrounding the FA on which the MN is located has been proposed as another technique for reducing packet loss during handover (Seshan and Katz 1997). As in the buffering approaches, the Foreign Agents are required to buffer the multicast traffic, and the MN requesting the buffer where the Mobile IP subnet movement algorithm is complete. When multicast approaches can work in routing domains, multicast routing protocols are enabled. The use of multicast is generally not possible on the Internet because routers in the internet disable multicast routing. In addition, currently deployed multicast transport protocols are unreliable, and thus this scheme would require converting the traffic using reliable protocols such as TCP to an unreliable protocol for the link between the HA and Foreign Agent, breaking the end to end connection.

Eva et al (2001) proposed a Regional Registration mechanism, a HA like Regional Registration Agent (RRA) in the local access network tunnels traffic between the MN’s local CoA of the FA. A regional CoA is maintained by the RRA. When the MN moves between subnets, it needs to report only the change to the RRA and not to HA. Because the RRA is topologically nearer, the registration updates the signalling latency, and thus the number of dropped packets should be less than for signalling of HA.
When the MN moves between RRAs, it obtains a new regional CoA and reports this to the HA. Thus, Regional Registration can reduce the number of packet drop.

An optimized hand-off algorithm that uses link mechanisms specific to 802.11 was described by Sharma et al (2004). The authors performed an informal analysis for sources of latency. Their solution, however, is to utilize link specific mechanisms without changing Mobile IPv4 rather than to modify the Mobile IPv4 protocol as the link synchronous mechanisms.

Finally, Campbell et al (2002) proposed Mobile IP mobility management to movements across large areas of network topology and used a specialized routing protocol for movement in smaller topological areas. These routing protocols are typically called micro-mobility protocols because they handle mobility in a small area of network topology. Micro-mobility protocols typically depend on limited propagation of host routes and may utilize link layer information to trigger host route propagation. Although these protocols have been studied extensively and show some promise, they do require specialized routers over a larger chunk of the network topology that is required by MIPv4. This requirement may serve as a deterrent to widespread deployment. MIPv4 only requires that the first hop router to (the FA) be specialized.

The most fundamental host controlled network-level protocols for supporting mobile hosts are the family of Mobile IP protocols MIPv4 (Perkins 2002) and MIPv6 (Johnson et al 2004). There has been recent work on various enhancements to the existing IP mobility protocols Hierarchical Mobile IP (HMIPv6) (Soliman et al 2005) and Mobile IPv4 Regional Registration (Fogelstroem et al 2006) are examples of such protocol enhancements that attempt to reduce signaling latencies based on localized mobility agents.
5.4 MIP STRENGTHS AND SHORTCOMINGS

MIPv4 is the standard scheme for IP mobility management MIP has several strengths:

- Transparency to upper layers MIP is designed as an overlay over the IP layer in the protocol stack. Therefore, its operation is transparent to upper layers.
- No modifications are needed in the CN.
- Therefore, existing IP nodes can be CN without modification.

However, basic MIP has some shortcomings:

- **Routing efficiency problems** - Having to route through the HA, is an inefficiency, known as “triangular routing”. However, route optimization enhancement has been introduced to fix this problem, but this requires CN modification (Perkins 2000).

- **Overhead problems** - Encapsulated packets are at least 8-12 bytes larger than the original packets. There is also a signaling overhead from the MIP registration request and replies.

- **Hand-off latency problems** - In addition to the hand-off latency related to the physical and link layers of the MN links, MIP signaling could add significant latency.

- **Survivability problem** - The NA is a single point of failure in MIP routing. In a single point of contact, the HA is unavailable, packets which will not be routed correctly to a roaming MN.
To overcome the above shortcomings, route optimization technique between the CN and MN is introduced.

5.5 HAND-OFF LATENCY WITH MIPv4

The hand-off procedure with MIPv4 consists of two phases namely, movement detection and registration. Movement detection occurs when the MN detects that has lost the connection to the old FA (oFA) and the connection to the new FA (nFA) has been established or the MN has moved from one subnet to another subnet. The hand-off message flow is shown in Figure 5.3. The layer-3 hand-off control relies only on the advertisement messages for movement detection.

There are two types of layer-2 hand-off, break-before-make hand-off and make-before-break hand-off. With the make-before-hand-off, the MN can communicate over the old link, as well as over the new link during the hand-off, and thus the MN can continue communication with the CN without losing any user traffic. The MN may receive advertisements over both links simultaneously and handover from the old FA to the new FA seamlessly. There is no hand-off latency during the hand-off process.

In the break-before-make hand-off, the old link is terminated first and then the new link is established. This is the case for GPRS and 802.11 WLAN. The MN loses connection to the old FA as soon as the old link is terminated. The registration information held at the old FA and the HA becomes obsolete. User traffic for the CN cannot be transferred over the most recent link from this moment. The link layer hand-off is a break-before-make hand-off, as soon as the layer-2 hand-off starts; the MN loses communication with the CN and thus the hand-off latency starts. Only when the MN completes the registration with the HA with the new CoA from the new FA,
the MN re-establishes communication with the CN. Therefore, the whole hand-off procedure contributes to the hand-off latency as shown in Figure 5.3.

Then the MIPv4 hand-off latency becomes (T_hoff)

\[ T_{hoff} = T_{l2\_hand-off} + T_{l3\_hand-off} \] (5.1)

Layer-2 handoff latency is \( T_{l2\_hand-off} \) is the sum of detection (\( T_{l2\_detection} \)), searching (\( T_{l2\_searching} \)) and re-association (\( T_{l2\_reassociation} \))

\[ T_{l2\_hand-off} = T_{l2\_detection} + T_{l2\_searching} + T_{l2\_reassociation} \] (5.2)

\[ T_{l3\_hand-off} = T_{mip\_agentdiscovery} + T_{mip\_registration} \] (5.3)

![Figure 5.3 Hand-off process in MIPv4](image-url)
When base Mobile IP runs over the 802.11b WLAN operating in the infrastructure mode, it has several components contributing to the hand-off latency, as shown in Figure 5.3. A typical 802.11b interface card operates on one channel at a time. The 802.11b specification has defined 13 channels. When the signal quality of the link between the MN and the current AP (the AP with which the MN is associated) falls below a certain threshold, the 802.11b interface card starts a search for new APs.

During the search, the 802.11b interface scans the other channels and the data traffic between the current AP and the MN is interrupted during the scanning. If there is an AP whose signal strength is strong enough, the 802.11b interface initiates the authentication and association procedures. The delay components 1 and 2 in Figure 5.3 represent the search period and the authentication and association period, whose sum is the layer-2 hand-off latency. During the layer-2 hand-off latency, all user traffic of the MN is stopped and the MN cannot receive the advertisement messages from the old FA. The delay component 3 is for the period from when the Mobile IP protocol determines to do a hand-off to an advertisement message which is received from the new FA. The latency due to movement detection is the sum of the three delay components. The delay component 4 is for the registration procedure.

The sum of the four delay components results in the hand-off latency that occurs when base Mobile IP operates in the 802.11 infrastructure mode. The key ideas proposed for reducing the hand-off latency are the following:

- Reducing the delay due to 802.11 channel scanning.
- Reducing the delay due to IP layer movement detection.
- Reducing the delay due to the Mobile IP registration procedure.
If IP layer hand-off must be controlled without any information about layer-2 hand-off, the two methods of movement detection specified in Mobile IP would have to be used. But, it can be determined by the need for an IP hand-off by taking advantage of cross layer hand-off control for IP and link layer hand-offs. The EACS protocol provides information of mapping between APs and FAs (or equally ARs). So, when the MN knows the MAC address of the target AP for layer-2 hand-off, it can find out whether the MN should register a new CoA or not and thus IP layer movement detection is done instantly as the layer-2 hand-off target is decided. The active scanning is done in less than 33ms by using the proposed pre-hand-off initiation algorithm.

5.6 PROPOSED ROUTE OPTIMIZATION FOR MOBILITY MANAGEMENT (RMIP)

The ECAS protocol provides the following functionality,

- Identifying or discovering the candidates of the next hand-off target.
- Collecting and representing the information of the candidates.

The key internal outcome of the protocol is to build the dynamic channel scanning table at each access router. The first task of the protocol is to build the channel scanning dynamic table correctly and maintain it efficiently. In particular, maintaining the integrity of the information in the table is important to enable various applications of the information. The types of the attributes to be in the table are open and thus new types of attributes can be defined and added. The key problem in building the table is to find out the IP address of the neighbouring access routers. Once two neighbouring access routers know the IP address of each other, they will communicate with each other over the wired network and exchange all the attribute information.
Since there can be multiple APs associated with an access router, the hand-off target candidates should be specified up to the AP Layer-2 ID. So the discovery process identifies the information pair (access router IP address, AP Layer-2 ID).

The EACS protocol provides means to update the dynamic channel scanning table when the information in the table becomes obsolete. For instance, when an AR is uninstalled, the relevant table entries are removed automatically in the neighbouring ARs. Once when each AR builds its table, the AR can provide the information in the table to the MNs, or the mobility management system can use the information. An MN may need just a part of the information in the EACS protocol to enable efficient handover. The protocol allows the MN to specify the required information when it requests the channel scanning table information from the AR.

A movement between two wireless subnets can be decomposed into two operations: the layer-2 handover, which is the change of APs at the layer-2 level, and the layer-3 handover, which is the change of the default access router for the MN and the establishment of a new path between the MN and its correspondents. The problem is that the MIP mechanisms are triggered only after the layer-2 handover ends; the MN first attaches to a new point of attachment at the layer-2 level. The MN may discover that it is attached to a new subnet by the Router Advertisement sent by the new access router. It configures a new IP address, verifies that this new address is unique on the link and then updates its localization.

To enhance these operations, the MN has to begin the layer-3 handover before the layer-2 handover ends. To begin the layer-3 handover in advance, the MN can anticipate its movement by the layer-2 triggers. A layer-2 trigger is based on the link layer protocol. It contains information on the physical connection and the link layer identification of the different
entities (the new AP’s MAC address for example). The EACS protocol initiates the layer-2 trigger, when the wireless link quality is below the threshold minimum value. The purpose of link layer trigger is to allow the MN to choose the best AP according to several parameters, like, RSS, number of MNs associated with the AP and the proposed capacity-based association.

The conventional RSS-based association MN continuously measures the strength of the received signal(s) from its AP(s). This signal strength may indicate that it is about to lose the connection with its current AP. A low level of the received signal triggers the scanning of all APs in the MN range to let it compare the strength of the received signal of the available APs. Different signal strength thresholds are distinguished to anticipate the redirection of flow between MN interfaces.

When the received signal strength of the current AP goes below -72 dBm, then the MN starts sending probe request to the AP and identifies its target AP based on various parameters, including RSS and the current throughput of the AP. Due to pre-initiated hand-off process, the MN is able to identify its candidate router and AP before the signal strength goes below -82dBm. The threshold minimum and threshold maximum points are discussed in chapter 2. During layer-2 hand-off process the MN is able to identify its target AP, ARs MAC address. The next point of attachment is updated in the new AR where MN is yet to attach. The next point of attachment is updated in the HA, but the packets are sent from the CN directly to the new AR before MN is assigned with new CoA.

The problem of triangular routing is eliminated. The router is updated with the new route information about the MN. The credential details are updated in the new AP as well as the new AR. The intermediate routes are updated with the binding update messages. When the signal strength is below the minimum threshold value, MN identifies the next candidate AP and AR.
from the dynamic channel scanning table using the probe request message. Before it reaches the maximum threshold value, it updates the next best candidate details in the intermediate router. The packets are routed directly to the new AR. The context information flow between the MN and AP includes the following elements.

1. MN’s MAC address, BSS ID
2. MN’s data frame sequence number

The layer-2-route update occurs when the MN moves between APs which are located within the same subnet. The layer-2 broadcast route update is sent to the new AP with MN’s MAC address as the source address. The broadcast message updates the intermediate ARs and dynamic channel scanning table for layer-2 two routing process. The layer-3-route update happens when the MN moves between APs that are located in different subnets.

5.7 SIMULATION RESULTS

The simulation scenario consists of four APs and 10 MNs. The distance between every consecutive AP is 500M and the moving speed of MN varies from 10 m/s to 40 m/s. The file size varies from 9200 Kb to 7800 Kb with the buffer size of 522 bytes. The sending data rate is 64 kbps from the CN to the MN. The experiment is repeated for conventional scanning process and for EACS protocol-based scanning process. The simulation study is conducted using Ns2 simulator to demonstrate the performance difference with regard to hand-off latency with and without route optimization. The traffic delay on TCP and UDP flows is shown in Figure 5.4. The TCP flow with different mobility speed is shown in Table 5.1 for standard MIP and the proposed Route Optimization - based method.
Figure 5.4 The hand-off latencies in UDP flow

(a) UDP delay in MIP

(b) UDP delay in RMIP
The CBR traffic consists of 1024 bytes of UDP packets at a constant rate of 100 packets/second which are sent from the CN to MN. The MN moves from one AP to another AP and triggers hand-off. The latency is collected as the performance metric to compare the proposed RMIP and standard 802.11 hand-off. Figures 5.4 and 5.5 show the UDP and TCP performance in both regular 802.11 and proposed centralized RMIP system. The horizontal axis is the packet sequence number and the vertical axis is the UDP end-to-end delay in seconds. In the regular 802.11 hand-off situation, a significant increase of end-to-end latency before the completion of hand-off as well as packet loss due to buffer overflow and packet drops are seen. In this simulation, a total of 65 UDP packets are lost during the hand-off in the regular 802.11 systems. Comparatively, the centrally controlled RMIP system completes hand-off within milliseconds, which are trivial compared to 10 ms packet interval and 2.7 ms average transmission delay.

The TCP performance in regular 802.11 and Mobile AP is shown in Figure 5.5. It is observed that the TCP connection using the regular 802.11 hand-off scheme is disrupted for 1.60 seconds from 42.13 to 43.73 second, of which the 802.11 re-association process incurred a latency of around 650 ms. Such delay is significant for multimedia or real time applications that are sensitive to delays. In the RMIP, the hand-off process took 0.985 ms, which barely affects the TCP stream.
A notable phenomenon in the simulations is that the hand-off starts at different time instants in RMIP and regular 802.11 systems. The regular 802.11 hand-off mechanisms provided by Ns2 adopts a “lazy” scheme in which the MN does not initiate the hand-off process until the RSS value is below a certain low threshold, even if there are APs that have better RSS with that MN. In the RMIP system, the hand-off begins when the central switch receives a better RSS report from a new AP about the MS than the currently associated AP. Therefore, the regular 802.11 system started hand-off at 42.1280 second, while the RMIP system started hand-off at time 23.0003 second. Such phenomenon is proved desirable in providing the best wireless connections to the MN in the world of multimedia in the next generation wireless networks.

The simulation results are conducted for varying the speed of the mobile device. The result for various speed and the throughputs are observed for MIP and the proposed RMIP. The average throughput at different speed is
shown in Table 5.1. It is observed that the average throughput is improved by 22.593%. This solution allows packets to be routed directly from the CN to the MN’s CoA.

Table 5.1  Comparison of throughput at different speed using MIP and RMIP

<table>
<thead>
<tr>
<th>Speed in M/Sec</th>
<th>Bytes transferred</th>
<th>Travel time in Sec</th>
<th>Avg Throughput in kB/s in MIPv4</th>
<th>Bytes transferred</th>
<th>Travel time in Sec</th>
<th>Avg Throughput in kB/s in RMIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>78500</td>
<td>396</td>
<td>196.97</td>
<td>84400</td>
<td>402</td>
<td>222.67</td>
</tr>
<tr>
<td>20</td>
<td>33100</td>
<td>196</td>
<td>162.172</td>
<td>37400</td>
<td>201</td>
<td>190.12</td>
</tr>
<tr>
<td>30</td>
<td>16600</td>
<td>126</td>
<td>128.645</td>
<td>19500</td>
<td>133</td>
<td>150.05</td>
</tr>
<tr>
<td>40</td>
<td>9200</td>
<td>95</td>
<td>92</td>
<td>11500</td>
<td>99</td>
<td>107.32</td>
</tr>
</tbody>
</table>

The number of packet drop is compared with conventional MIP and the proposed RMIP is shown in Figure 5.6. The network efficiency and utilization have been improved by eliminating the triangular routing. The proposed RMIP is reliable for real-time communications and provides high throughput with minimized latency time.
5.8 SUMMARY

The EACS protocol enables efficient and intelligent mobility management in the wireless internet over heterogeneous wireless networks. The primary role of the EACS protocol is to provide appropriate information about neighbouring base stations that can be used in hand-off target selection. It is a complementary protocol to Mobile IP and other mobility management protocols. The EACS protocol requires each AR to know the IP address of the neighbouring ARs and the layer-2 address of the neighbouring base stations. The hand-off based discovery mechanism allows distributed and dynamic discovery in a scalable manner. RMIP reduces traffic disruptions experienced in the MIP schemes by exchanging MN and AP link quality information between APs. The proposed RMIP scheme achieves seamless roaming by transferring the MN-AP context to the best connected AP around the vicinity of MN thereby eliminating the need for MN to re-associate with other APs.