# A Micro-Mobility Management Scheme for Handover and Roaming

**Debabala Swain** *debabala.swain@rediffmail.com*
*Dept.of Computer Science*
*CUTM*
*Bhubaneswar, India*

**Siba Prasada Panigrahi** *siba_panigrahy15@rediffmail.com*
*Dept of EEE*
*GITA*
*Bhubaneswar, India*

**Prasanta Kumar Patra**
*Dept. of Computer Science* *hodcomputer@yahoo.co.in*
*CET*
*Bhubaneswar, India*

**Abstract**

Even though the PMIP provides mobility solutions, there are many issues of user identity, mobility context of users from a home network to the visiting network, the assignment of home address to a user terminal in a visiting network, identification of the user terminal's mobility, and identification of MPA and HA. In this paper, we propose a new mechanism with proxy mobile IPv4, as a mobility solution in networks. In this mechanism, during mobile node access authentication, MPA exchanges registration messages with the HA (Home Agent) to set up a suitable routing and tunneling for packets from/to the MN. In this method, the authentication request of the mobile node is passed through the NAS or AP of visiting network, this is then passed to the AAA (Authentication Authorization and Accounting) server, and the authentication server checks the realm and does start authentication procedure at the time of initialing authorizing module of the mobile terminal. It also initiates the mobility extension module, where the AAA server initiates MPA of the access network, which also informs the AAA server of the home network with information on the mobility extensions and request of the mobility parameters of the user terminal. The home AAA server interacts with the HA and collects mobile node parameters, as well as sending back details as a reply request to the visiting AAA server. After the mobility context transfer, the MPA conducts a mobility registration to the HA for that particular mobile node. Later in this paper, we will provide sequence of message exchanges during a mobility session of a user mobile node during handover.

**Keywords**: Handover, Roaming, Mobility Management

## 1. INTRODUCTION

The mobility management in the access networks is provided by the mobile IP for the seamless continuity of the services during handover and roaming. The demands for accessing services at high data rates while on the move, anyplace and anytime, resulted in numerous research efforts to integrate heterogeneous wireless and mobile networks. However, when the handover happens, the contention-based medium access mechanism which is mainly used in WLAN is invoked and introduces unbounded transmission delay due to idle time periods and retransmission because of collision during the handover. If this technique is expanded to use in a micro-cellular network such as connected WLAN micro-cells, contention-based mechanism, therefore, should not be used to handle the MT's handover, especially for vehicular users who change access point every few seconds [1]. IP Mobility management protocols are divided into two kinds of category: host-based and network-based mobility protocol. Issues and challenges in mobility management identified and discussed in [2]. Recently, a unified IP Multimedia Subsystem (IMS) authentication architecture that extends the scope of IMS by allowing it to offer users different IMS-based services even beyond their own domain has been proposed in [3]. But, all these research activities resulted in various heterogeneous architectures where the interworking was performed at different levels in the network. Also, integration at the UMTS radio access level for seamless session continuity proposed in [4]. But, proposed integration is a technology specific solution. However, in this article, we evaluate micro mobility.

The Proxy Mobile IP (PMIP) [5] solution based on Mobile IP approach; handles mobility management inside access networks. Therefore network entities will require more capability than in the standard Mobile IP. The Foreign Agent is no longer capable to handle the mobility management in this new scenario, so we need to enhance its capabilities with the Mobility Proxy mechanism. This new entity called Mobile Proxy Agent replaces Foreign Agent in the visiting network. It also handles mobility registration with the Home Agent. This change is most significant since the Mobile Node now lies outside the mobility registration procedure. In fact, Mobile Node is not aware of its movement, access networks deceives the host to believe that it is stationary in its Home Network. Since the Mobile Node does not need either movement detection or agent registration, the agent advertisements are no longer necessary.

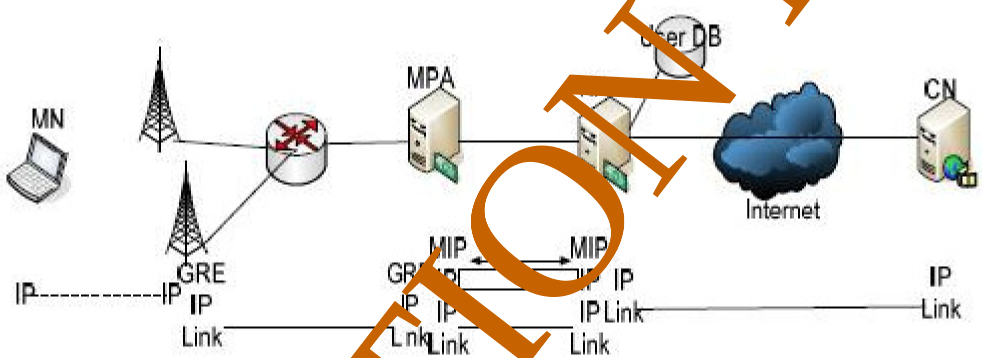


**FIGURE 1:** Proposed PMIP model

This paper addresses some of the requirements and features to be satisfied for PMIP to provide mobility management:

- Support Unmodified Hosts: As noted above, the protocol supports mobility to nodes that does not have capability of mobility.
- Air link consumption: Mobility-related signaling over the air-link is eliminated. Considering that Network Address Translation (NAT) is ubiquitous in IPv4 networks, a mobile node needs to send keep alive at short intervals to properly maintain NAT states. This can be performed by the MPA in the network which does not consume any air-link bandwidth. The Agent Advertisement is also eliminated in the protocol.
- Support the Heterogeneous Wireless Link Network: One aspect is how to adopt the scheme to an access technology. Since Proxy Mobile IPv4 is based on a heterogeneous mobility protocol, it can be used for any type of access network.
- The other aspect is how to support mobility across different access technologies. As long as the MPA can use the same NAI to identify the MN for various access networks, roaming between them is possible.
- Support the IPv4 and IPv6: As IPv6 increases in popularity, the host will likely be dual stack.

## 2. PROPOSED SOLUTION FOR PMIP WITH INTEGRATED AAA ARCHITECTURE OF THE 3GPP AND WIRELESS NETWORKS

In this new mechanism, mobility registration of a user terminal is performed by visiting access networks and a home access network. The user terminal does general authentication by visiting access networks with the help of an EAP (Extensive Authentication Protocol) mechanism. The visiting access networks receive the authentication request from a user terminal through the NAS or AP of the network. The AAA server of visiting network and home networks are modified so that they can communicate with the HA and MPA of their respective networks. New mobility extensions are developed in AAA server to support mobility management, which adds to its present services. These extensions provide mobility context transfer from home access networks, registering the user terminal for mobility at the time of authentication. The visiting network initiates authentication and the mobility extension method whenever it receives a request from the NAS or AP of the access network. During initiation of mobility extensions, the AAA mobility extension process collects data when NAS/AP requests authentication. The AAA mobility process sends mobility user details request to the home network and the AAA server of the terminal with newly specified attributes of proxy mobile IP. The Home AAA server does receive a request for the mobility user details request as well as the authentication. The home AAA server distinguishes a proxy mobile IP packet from other codes and attributes of the received packet. If the packets need to be a proxy from an intermediate AAA server, then that server adds the proxy attribute to the received packet and sends it to the destination AAA server. If ever the user terminal belongs to the current network, then the AAA server sends a mobility registration request to HA.

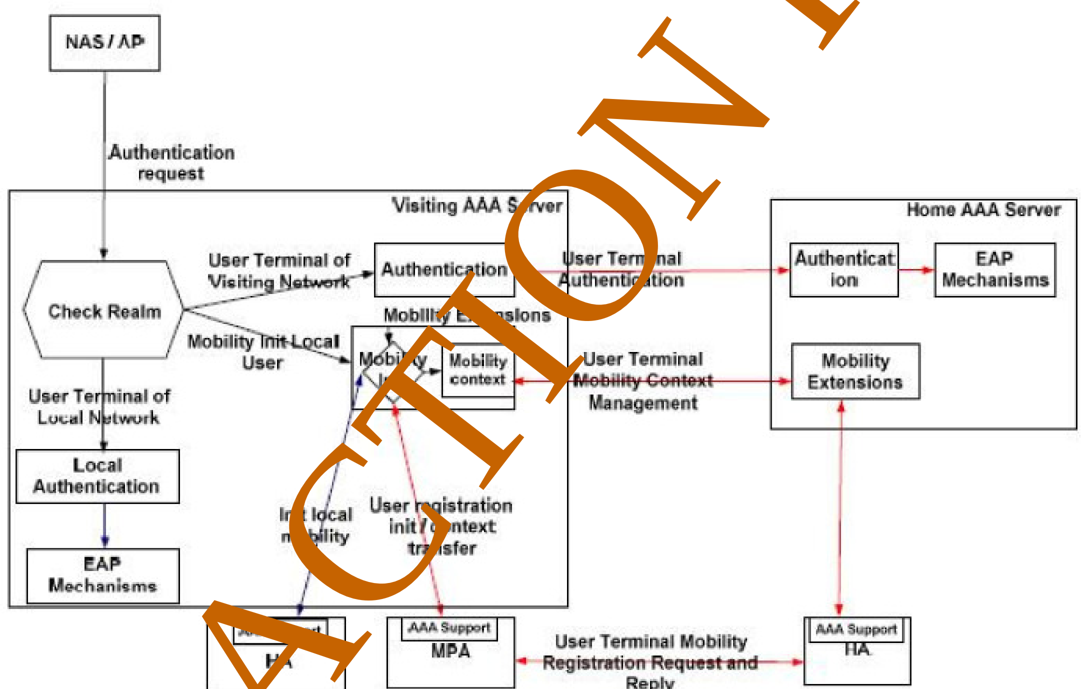


**FIGURE 2:** Sequence diagram of PMIP Architecture

After receiving the request for mobility user details packet from the visiting AAA server, the home AAA server investigates any information available in the packet and collects user identity from the request packet. After processing the request, the mobility extension method prepares user detail request packet to the HA of the access network. This packet contains details of user id and parameters. The HA receives a request, and with a user ID of request it extract the information of its SID, keys, home address and home agent address from the database of the HA. The HA then sends back a reply to the AAA of home network with the above mentioned data. The AAA server receives a reply and processes the information, and sends back a reply message to the visiting AAA server. The visiting AAA server receives a reply from home server and processes it, storing the data of the user in a temporary database. After processing the reply message, the AAA server sends a mobility registration request to the MPA associated with that particular NAS or AP. This request contains the details about user ID, SPI, keys, home address and home agent address. When the MPA receives the packet it starts the mobility registration of a user with details from the AAA server.

MPA initiates a mobility registration request of a user terminal with HA using details provided by visiting AAA server. Registration involves the user SPI and the shared key mechanisms with the key available from the AAA server to the MPA. After successful registration of the user with the HA, the MPA will modify the DHCP server configuration with the user terminal's details. These modifications contain details of MAC address and home address of the user in the DHCP server. After successful authentication of the user terminal it initiates a DHCP request for an IP address. The AP/NAS of the visiting network forwards the request to the DHCP server. With the MAC address of the user terminal modified, the DHCP server sends a reply to user's terminal with its home address. The user terminal receives the reply and configures the IP address to the home address. Necessary modification has to be done by the visiting network to accommodate the terminal with the ARP, etc. When the user terminal is in it home domain, the HA registers the terminal and sends the modified DHCP request to the DHCP server and acknowledges the home AAA server of successful registration of a user terminal. The Proxy Mobile IP with the AAA server mobility architecture is shown in Figure 1.

**2.1 AAA Mobility Extensions for PMIP Integrated Architecture**

In this section we describe the detailed architecture of AAA with mobility extensions to provide mobility management during user mobility in different access networks and technology. In this process, the existing AAA architecture is modified to accommodate proxy mobile IP. In general, authentication information of users is passed through the authenticator, and then this information is passed through the NAS or AP of the access networks. An AAA server authenticates the access networks for the AP or NAS initially, and then processes the user authentication request depending on the realm of the user. In this new method, the mobility management of a user can be initiated during the authentication process. In this process, due to parallel operation of authentication and mobility management, the overall latency of a user during the handover and initial access can be reduced.

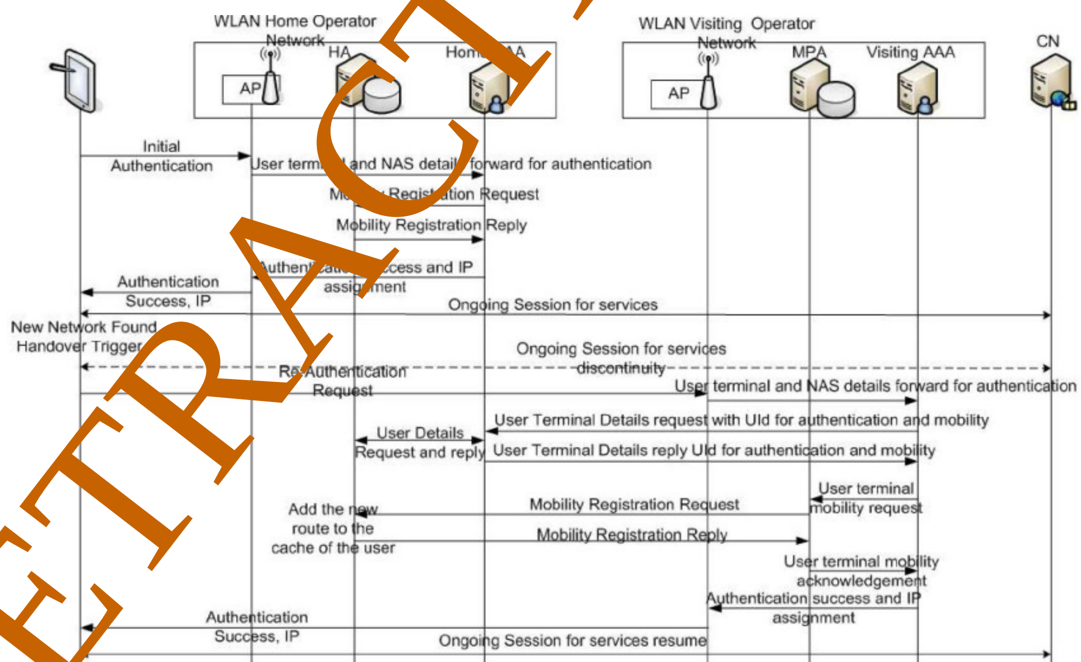


**FIGURE 3:** AAA mobility extensions sequence Diagram

When there is an authentication request for a user terminal from an NAS or AP, the AAA server initiate authentication module and mobility modules, and processes the user's details by identifying the NAI of the user terminal request. From the NAS or AP request information, such as MAC address of user terminal, NAS details are processed for further procedures. The AAA is modified, with new attributes and codes being added for supporting the PMIP modules. As mentioned previously in the proposed solution section with new extensions, the AAA of the home network can communicate with a visiting network, and can provide mobility context management. With these mobility extensions, the AAA server can communicate with the MPA and HA of the access networks.

On the other side, the visiting AAA server communicates with the home network AAA server, after receiving an authentication request using the mobility extensions, with user information being available from the authentication request from the user's terminal. The visiting server sends a mobility user details request using ID and NAI of the authentication request to the home AAA server. When the home network receives a request packet, the AAA server processes the information of the user from request. It then sends a request to the HA with the new mobility extension, requesting details of the user. After receiving the request packet and processing user details from its internal database, the HA sends back a reply packet with home address, key, SPI and home agent address to the home AAA server. The home AAA server sends back a reply to the visiting AAA server with user details as the reply. After receiving this reply from the home AAA server, the visiting AAA server processes the information of the user and sends a request for mobility registration request with new attributes to the MPA. The MPA receives the user terminal data, sent by the visiting AAA server, and temporarily stores it in a local database. The MPA, with available user information, starts registering with the HA. After registration request and reply message exchange with HA, the MPA sends reply of success or the failure of mobility registration of user to visiting AAA server. Figure 2 describes the AAA mobility architecture.

### 2.2 PMIP Operation With New Mobility Extensions in MPA and HA

MPA exchanges registration messages with the HA to set up a proper routing and tunneling packets from/to MN. The MN broadcasts messages containing an MN's Network Access Identifier (NAI) to request authentication/authorization, and the AP transfers the request to the local AAA server (visiting AAA). If the MN is away from home, it is clear that the MN is out of the local authentication database.

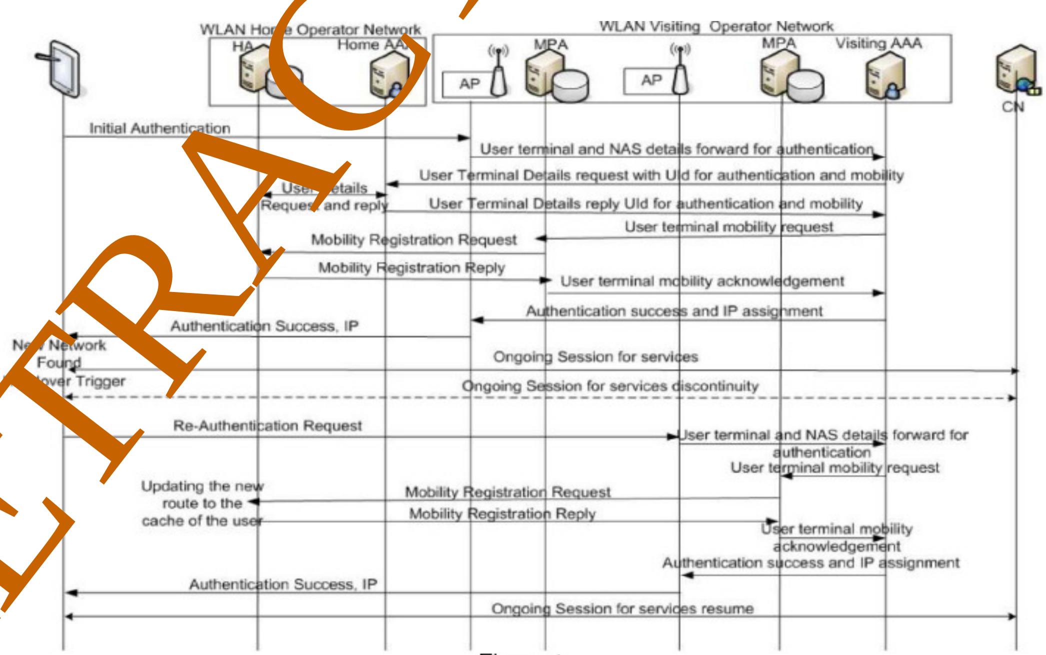


Figure 4

Mobility extensions using MPA and HA

However, the local AAA server can use the NAI to identify the MN's Home Network, and then the authentication/authorization, along with mobility user details, will request a message to be transferred by the visiting AAA to the home AAA Server (AAAH) in the Home Network.

Along with the authenticating validation, the AAAH searches for information of the MN stored in the HA, containing MN's HA, NAI, and SPI. If the MN is back to its Home Network, then the local AAA server sends a message to the HA to deregister the MN instead of searching for the data. The MN's information will be transferred to the visiting AAA, which will deliver it to the MPA with the AP's MAC address included. Triggered by the AAA server, the MPA exchanges messages with the HA to demand Mobility Registration and Tunneling.

After successful registration, the MPA sends a message to inform the DHCP server about the MN's arrival. It forces the DHCP server to update the configuration file with the Mobile Node information. Finally, the MPA informs the AAA visiting about the successful registration. The Authentication Accept message is sent to the NAS, granting network access to the MN. After authentication success, the MN sends a Binding DHCPDISCOVER to request the IP address. This message is formatted as described by the DHCP protocol (the CIADDR field is filled with the MN's IP). By searching for information of the Mobile Node, in the configuration, the DHCP server replies with a DHCPOFFER message in which the YIADDR field is filled with the MN's Home Address and the default gateway address, being the MPA's. Next, the MN and DHCP server exchange the DHCPREQUEST and DHCPREPLY to complete this procedure. The MN is then ready to connect to the network with its Home Address.

## 3 MICRO MOBILITY

In this scenario mobility is performed in same administrative domain and same access technology, we have observed two sub scenarios where the proposed architecture addresses this issue.

### 3.1 User Terminal Mobility in Home Administrative Domain on Same Access Technology

In this scenario access network has multiple APs, and user terminal moves from one AP to another AP. During initial authentication of user, AAA server does authenticate user and assists HA for mobility registration of user terminal. When user terminal senses other APs of access network and triggers the handover with re-authentication procedure, upon receiving request from new AP, the AAA server sends mobility registration request to MPA associated with AP. MPA and HA does the mobility registration of the user terminal and sends acknowledgement to AAA server. Upon successfully authentication and registering terminal in HA, it provides access and home IP address of user terminal to AP for providing access to user terminal. The message exchange is shown in Figure 3.

### 3.2 User Terminal Mobility in Visiting Administrative Domain on Same Access Technology

In this scenario, user terminal moves on same interface from one AP to another in visiting operator network. The user terminal is authenticated and registered in HA with the help of home AAA and visiting AAA servers. When user terminal identifies new AP it triggers the handover and does re-authentication procedures. Upon receiving request from new AP visiting AAA identifies user from previous registration and sends mobility registration request to new MPA with previous details. MPA does register the user terminal with HA and sends acknowledgement to visiting AAA server to complete handover procedure, the whole procedure is shown in message sequence in Figure 4.

### 3.3 Enhancing the Proposed Solution Using Network Selection Procedure for Seamless Mobility.

To enhance proposed architecture we used network selection procedures combined with this architecture to use context management between the networks. Using this process access networks can create mobility context even before user terminal does initiate access to visiting network. In this process user terminal can communicates with home network using present connected network and negotiate best suitable network to connect during handover. After selecting best suitable network with the assistance of terminal, home network initiate context transfer and creating mobility context with the future visiting network.

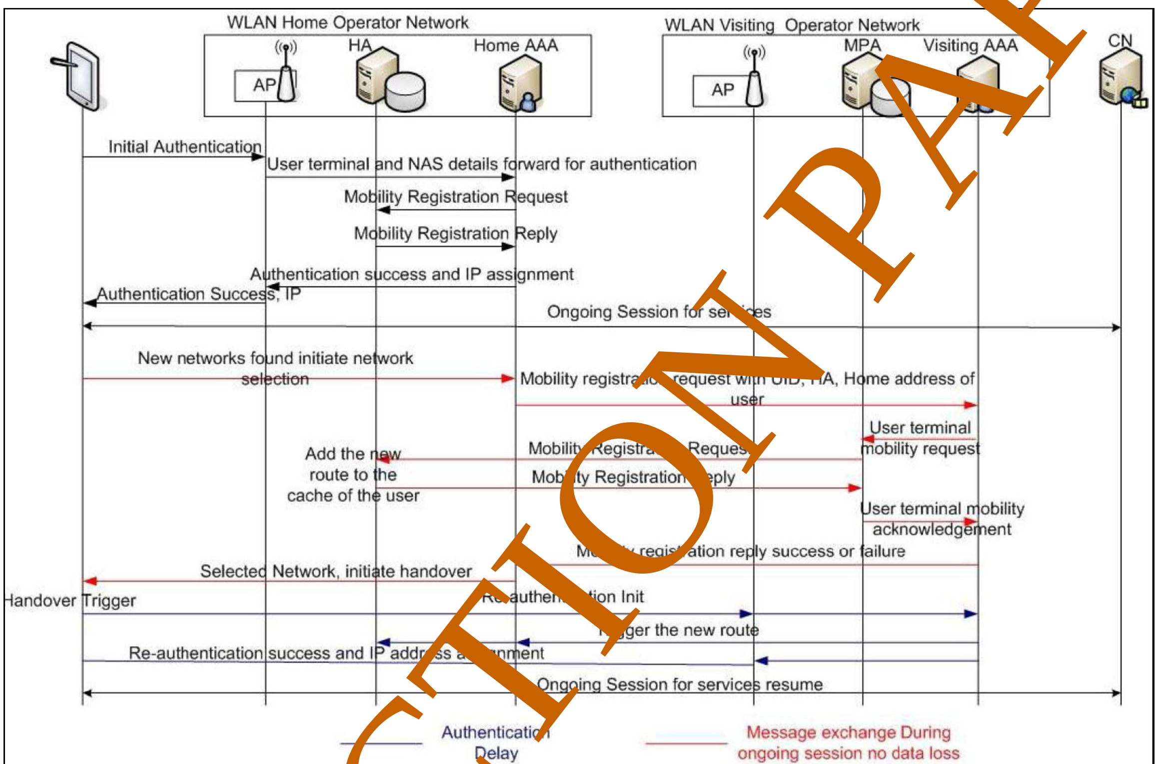


**FIGURE 5:** Mobility management using Micro mobility model

Using AAA mobility extensions proposed in this architecture AAA of home network sends a mobility registration request to visiting AAA server with UID of the terminal and mobility context details in the request. After receiving request from home AAA server, visiting AAA server collects data and sends registration request to MPA of visiting network. After receiving request for mobility registration MPA collects user details and initiates registration request to HA of home access network. After successful registration user details of new route are cached in HA and MPA and a tunnel is established between them. When user or home AAA server does the handover triggering, HA does update route upon receiving the RU (route update) request from home AAA server. In this way maintaining multiple tunnels with future visiting networks of user and triggering with the help of home AAA server seamless mobility is achieved.

The whole message exchange sequence diagram is shown in Figure 5. During implementation of this procedure in a test bed we observed zero latency for multi homing handover and for horizontal handover we obtained small latency delay due to re-authentication procedure.

## 4 NEW PMIP AND AAA MOBILITY EXTENSION DEVELOPMENT AND TEST-BED SETUP

### 4.1 PMIP and AAA Software Architecture

To implement proposed architecture we developed AAA server and PMIP in house using existing open source software. We have developed software architecture to implement mobility extensions for AAA server. In this architecture AAA server can receive a request from NAS or from another AAA server. From NAS it can receive authentication request and from AAA server it can receive mobility user detail request. Upon receiving mobility registration request, extensions model respond with the reply of user details. Software architecture of AAA as shown in Figure 6, the AAA server can send requests and reply accordingly to incoming requests with the different components. For implementing the PMIP we used dynamics mobile IP architecture and modified to our requirements. We converted FA to an MPA, modified HA and MPA to accept any requests from AAA server and sending reply accordingly. In this architecture MPA can perform registration requests to HA upon request from AAA server and sends acknowledgement as success or failure. New packet formats and codes are added in MPA and HA to implement the proposed architecture.

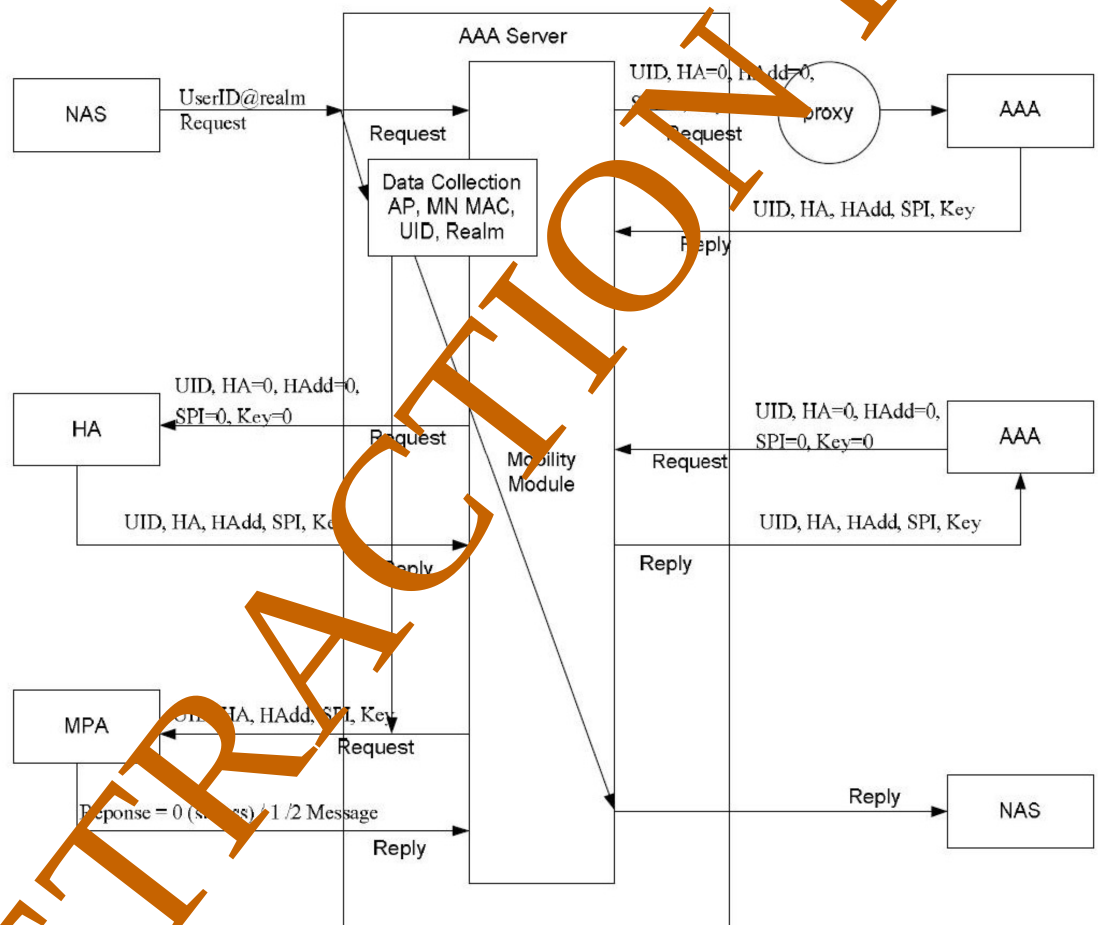


**FIGURE 6:** Software Architecture for PMIP Architecture

### 4.2 AAA Mobility Extension and PMIP Packet Formats

We have developed new AAA mobility extensions and new codes and packet formats for developing and demonstrating the capabilities of new mechanisms proposed in this architecture. The AAA server builds Mobility User Detail Request message from Access Request or EAP

Request from the NAS or AP. Remark that intermediate AAA servers just pass through this step adding Proxy Attribute and forwarding the Request.

#### 4.2.1 AAA Mobility User Detail Request Format:

Note: the codes and the attributes in this document are taken as reference these can be changed according to the IANA consideration; in this case we used available values for developing the prototype, we can change these values if there are any issues.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|         Length (2 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   Authenticator (16 bytes)                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Code: (1 byte) Mobility_User_Detail_Request = 60.
Identifier: (1 byte) number to match the Request/Reply.
Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes. In the case that there is only mobility attribute, length = 350.

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

Attributes: Mobility Attribute:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |         Length (2 bytes)        | User's ID (1B)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   User's ID (256 bytes)
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     HA address (4 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Home address (4 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SPI (1 byte)  |        Key (64 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = (1 byte) Mobility_Request_Attribute = 193.
Length (2 bytes) = Length of the message = 332.
User's ID: (256 bytes) extracted from the name of the user (ex: userID@realm).
HA address: (4 bytes) Home Agent's IP address, filled with Zeros.
Home Address: (4 bytes) Mobile Node's Home Address, filled with Zeros.
SPI: 1 byte, filled with Zeros.

Key: (64 bytes) public key of the HA, filled with Zeros.
The AAAH will reply with a Mobility Response.

**HA/MPA Consultation**

If AAA home server receives Mobility user detail request from a visiting server, the AAAH sends message to HA to fill the information required in the Mobility Request Attribute (fields that are filled with Zeros). Remark that the AAAH sends the HA Consultation message only by being triggered by the Mobility user detail Request; the Access Request forces the AAAH to deregister the MN.

H1: Create a message from AAAH to the HA demanding for the necessary information:

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Code (1byte)  |Identifier (1B)|      Length (2 bytes)         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     User's ID (256 bytes)                     |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |            Access Point's MAC address (6 bytes)               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   AP's MAC address (cont)     |  MN's MAC address (6 bytes)   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 MN's MAC address (continue)                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  Home Address (4 bytes)                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   HA address (4 bytes)                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | SPI (1 byte) |              Key (64 bytes)                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Key (continue)                           |
   |                                                               |
```

Code (1 byte) = HA_Consultation_Request = 63.
Identifier: (1 byte) number to match Request/Response.
Length (2 bytes) = total length of the message = 343
AP and MN's MAC address: These fields are practically used in the message from AAA to MPA. In the message from AAA to HA, these fields are filled with Zeros, and the HA just ignores it. But these fields SHOULD appear in the HA Consultation Message to identify the format of messages AAA-HA and AAA-MPA. It is very useful since the HA and MPA in the same network are usually installed in the same server. This identification simplifies the treatment of message in the HA/MPA server.

Other fields are copied from the Mobility Attribute of the authentication request.
H2: HA looks for the required information in its database, save the AP and MAC address fields. If the information can't be found (this may be due to the modification of the administrator), HA will pass this phase, so that the message will be left Zeros. That allows the AAAH to detect the failure.

H3: HA sends back the reply to the AAA after filling the request's required fields and setting Code = HA_Consultation_Response = 64.

H4: The AAAH replies the visiting AAA with a Mobility user detail Response, which is either an Accept or Reject message. The format of these messages is as same as the request, with different code and attributes.

If the message from HA is not filled with Zeros (successful verification), the AAAH reply to the AAAF with Mobility Accept message which is copied from the Mobility Request whose the Attributes filled by the data retrieved from HA. The Code field for this message is: Code = Mobility_Accept = 61.

If the data from HA is filled with Zeros, the AAAH MUST reply the visiting AAA with a Mobility user detail Reject message, with Code = Mobility user Reject = 62. The Mobility Reject message doesn't contain the Mobility_Attribute, and may include Reply-Massage Attribute which contains the error message shown to the user [6]:

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type = 18 |    Length     |  Text ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type: 18 for Reply-Message.
Length: length of the attribute, including Type and Length field.
Text: The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. If the registration failed, this field is filled with the message extracted from the MPA Mobility Registration Reply.

**Mobility Registration**
After receiving the Mobility Accept message, the visiting AAA makes MPA handle the Mobility Registration procedure. The MPA exchanges messages with HA and DHCP server, then informs visiting AAA about the result (success or failure). The Mobility registration Reject causes the AAAF to send the Reject message to the NAS and terminate the whole procedure.

MR1: Visiting AAA sends a MPA Mobility Registration Request message to MPA: the format is as same as HA Consultation message:

Type (1 byte) = MPA_Mobility_Registration_Request = 65.
Identifier: (1 byte) number to match Request/Response.
Length (2 bytes) = total length of the message = 343.
Other fields same AP and MN's MAC address are copied from the Mobility Attributes of the Registration Response.
MR6: MPA Mobility Registration Reply to visiting AAA:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type (1 byte)| Identifier(1B)|     Length (2 bytes)          |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|                    User's ID (256 bytes)                      |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Access Point's MAC address (6 bytes)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AP's MAC address  (cont)     |     MN's MAC address          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 MN's MAC address (continue)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Home Address (4 bytes)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 HA address (4 bytes)                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SPI (1 byte) |             Key (64 bytes)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Key (continue)                             |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The MPA sends back the reply to the AAA after successful communication with the DHCP server, or if it detects any error (registration unsuccessful, DHCP server refusal to register the Mobile Node, or requests cannot reach the destination). In this latter the MPA sends a reject message to the AAA server (reply with response = 1 or 2).

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) | Identifier(1B)|   Length (2 bytes)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Response (1B) |          Message
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = MPA_Mobility_Registration_Reply = 66
Response = 0 if successful, = 1 if unsuccessful with message, = 2 if unsuccessful without message.

In the unsuccessful case (Response != 0), AAA will sends an Access_Reject message to the NAS. Otherwise, if the Response Code = 1, the text in the Message field can be used in the Reply-Message Attribute in the Mobility Registration Reject message.

MIP Registration
For the convenience of use of Client Mobile (Mobile IPv4) and Proxy Mobile IP simultaneously, the MPA and HA should use the Mobility Registration Request as specified as in RFC3344.

HA reply with Mobility Registration Reply, formatted as specified in RFC3344.

MR4: MPA sends DHCP Mobility Registration Request to DHCP server:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |     Identifier (1 byte)      |  Length (1B)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      MAC address (6 bytes)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   MAC address (continue)      |  Home Address (4 bytes)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Home Address (continue)    |  Action (1B)  | MPA's MAC add |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               MPA's MAC address (continue) (6 bytes)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| MPA's MAC add |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = DHCP_Mobility_Registration = 67
Identifier: match Request/Response
Length = 21: length of the message, including the Type and Identifier fields
MAC address: MN's MAC address
Home Address = MN's Home Address.
Action: (1 byte) = 0 - binding update: the DHCP server updates its configuration file with the MN's new entry:

MN's MAC address --- MN's IP address --- Default Gateway = MPA's MAC address

If Action = 1 - remove entry: cause the DHCP server to remove the MN's entry in its configuration file. This action is used in the Registration Revocation Procedure. As receiving the message from the MPA, the DHCP server updates its configuration with the information supplied by the MPA. Since then, as soon as the DHCP server receives the (Binding) DHCPDSICOVER message from the MN, it will exchange the messages with the MN granting the MN keep its Home Address; also indicates the MPA as MN's default gateway.

MR5: DHCP Mobility Registration Reply to MPA
The message is formatted as same as the reply from MPA to AAA

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) | Identifier(1B)|      Length (2 bytes)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Response (1B) |          Message
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = DHCP_Mobility_Registration_Reply = 68
Length = length of the message including the Type and Identifier fields
Response Code = 0: accept, = 1 reject with message, = 2 reject without message.

If the response Code is other than 0, the MPA MUST response with the AAA with MPA Mobility Registration Reply whose Response and Message fields copied from DHCP Mobility Registration Reply message.

Message: this message will be used in the response from MPA to AAA.

### 4.3 Test bed Setup

This section describes testbed setup for implementing solutions proposed in this architecture. As mentioned earlier we have developed mobility extensions for AAA server using FreeRadius [7], and PMIP using parts of Dynamics mobile IP [8] with our implementation. The proposed testbed composed of 3GPP, WLAN and WIMAX Networks. We used Infinet's preWIMAX equipment, operating at the frequency of 5.4 GHZ for WIMAX network, WLAN access consists of Linksys WRT54 and Cisco AirNet AP350. The 3GPP network used in this case is EDGE network operated by the French network operator Bouyges Telecom courtesy of MVNO Transatel. The user terminal used in the testbed is DELL Latitude410 using Centrino for wireless with option GT 7.2 ready MAX data card for 3GPP access. Most of our testing for different scenario we have used WIMAX and WLAN due to complexity of EDGE network as we have limited control of the production network provided by MVNO Transatel for us. To validate the solution we used basic testing like vertical handover where the client is equipped with multiple interfaces to validate the solution for multi homing scenarios. As we mentioned earlier horizontal handover is limited for EDGE in our case because of the control of the access network.

The implemented scenario is shown in Figure 7. We have deployed a VPN with cellular network where authentication and data is routed through the cellular network to local testbed. The user terminal is configured with AT commands using PAP for authentication. When user terminal dials for connection, authentication information of user terminal is routed through GGSN to the local authentication in the test bed, the modified AAA server does the authentication and assigns the address using IP pool mechanism, and in parallel mobility context is created for MPA and HA using AAA server.

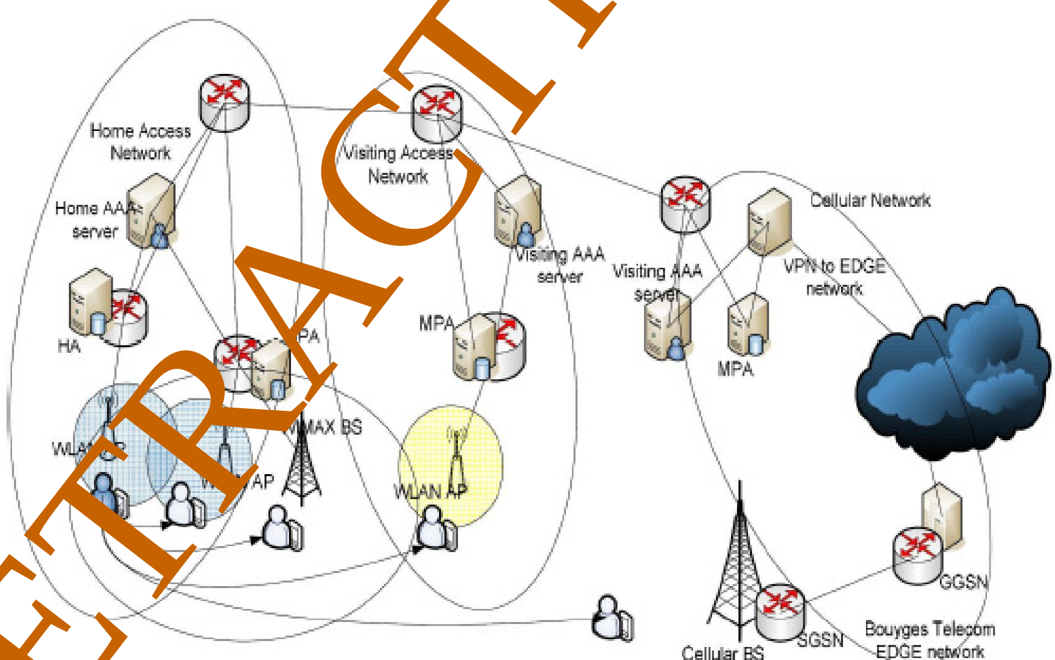


**FIGURE 7:** Test-Bed set up for proposed model

We have deployed EAP authentication mechanism for authentication in WLAN and WIMAX networks. A user terminal tries to connect access networks using WPA supplicant [9], it is configured with user id with NAI and security mechanisms essential for EAP TLS mechanisms. Once the authentication is initiated in access networks, APs and BS sends authentication request to AAA servers, and AAA initiates authentication and mobility context for user terminal. A GUI is developed on terminal to maintain interfaces and control access management along different access networks.

## 5 RESULTS

As mentioned in architecture the AAA server does authentication and mobility in parallel when there is a request from the user terminal in test-bed. Using this test-bed we have achieved mobility of user with low latency and seamless mobility in some scenarios. Multi homing, horizontal handover and roaming is performed efficiently using this mechanism. Various scenarios of mobility have been tested using this test-bed. Deployment and extending to the new access networks and operator is very efficient as the modifications are made at network side without any client conscious. The modifications on the network side can be made with additional patches with existing deployments. For testing purposes we have used experimental codes and attribute value pairs these can be extended to the vendor specific or using IANA status can be standardized.

We have observed an overall latency of the user terminal involved during roaming from one network to another on the same technology is around 2.4 sec for WLAN, 3.6 seconds for WIMAX, and 16 seconds for 3G networks, due to re-authentication and mobility management. In 3G networks we have observed high latency due to delay of routing messages from bouyges telecom network to our test bed. For multi homing scenario we observed latency of 18 milliseconds as we have implemented multiple interface scenarios, where a user terminal connects to multiple networks and the management of the mobility is performed by triggering route update message in HA of the user terminal. In the next paragraph we have attached a log of our radius servers in home and visiting networks where the whole procedure is depicted. For more details about logs, ethereal results refer to [10].

### 5.1 Comparison With Existing Mobility Models

In this section different mobility protocols are compared with the available results and support for access networks with experimental results and simulation results. As we mentioned in last section we have built test bed to perform mobility in different interworking scenarios of mobility using mobility protocols. We take the following result of CMIP, HMIP and PMIP from the test bed and the result of HAWAII and Cellular IP from other sources [11]. The Table 1 shows the different performance results for mobility protocols.

In the test for CMIP and HMIP, we take the result from mobility registration procedure only. Macro-mobility handoff time is counted from moment that MN starts to the end of the handoff; and micro-mobility handoff time is counted from the moment that we switch network connection (changing access point). In fact, using manual switch is little different from real time test in which the MN starts handoff if it moves out of the first access point's cover, since in the later case's handoff time depends largely on network scanning and selecting software used in the MN. We can observe that the CMIP has very high macro-mobility latency, which dues to Agent Discovery phase. We admit that the test bed is so simple as compared to the architecture implemented HAWAII and Cellular IP that the different networks are adjacent, and therefore cannot have a proper comparison among these protocols. The test is purely on latency issue, we don't count on packet loss and robustness. However, the result is persuading enough to prove the advantage of PMIP.

Proxy Mobile IP is advantageous over other mobility protocols over security, since the information is exchanged among the network entities with authenticated mechanism. More precisely, the advantage of PMIP over other protocols comes from the fact that the information exchanged in registration procedure can be generated for each session, i.e., HA can generate necessary information used for each registration session. Hence, outside AAA authentication, no key is actually stored for mobility registration.

The proposed mechanism for mobility management in this paper is compatible and interoperable with the existing converging networks. We have studied different interworking methods to implement our solution for completing the seamless converging puzzle at the mobility management layer. We interrogated different interworking mechanisms such as Seamless Converged Communications Across Networks (SCCAN), Unlicensed Mobile Access (UMA), Interworking- Wireless LAN (I-WLAN), Media Independent Handover (MIH) IEEE 802.21. The proposed solution can be adapted in these mechanisms to provide seamless services at the mobility layer.

| Protocols | Support for Micro mobility | Handover latency Micro mobility | Access Networks Support | Security | Legend |
|---|---|---|---|---|---|
| CMIP | -- | Non | WLAN/WIMAX | + | ++Strong advantage |
| HMIP | ++ | 138ms* | WLAN/WIMAX | - | +Advantage |
| HAWAII | ++ | 150ms* | WLAN/WIMAX | - | -Drawback |
| Cellular IP | + | 300ms* | WLAN/WIMAX/ Cellular Mobile Network | + | --Strong drawback<br>*not include network selection and authentication |
| PMIP | ++ | 70ms*** | WLAN/WIMAX/ Cellular Mobile Network | ++ | **include authentication and manual network selection latency<br>***include re-authentication |

**TABLE 1:** Comparison of mobility protocols with PMIP

### 5.2 Issues of IPv6 Migrations

Due to low IP address space available for ever increasing terminals there is a need of IPv6 in the near future to deliver the services. NETLMM is an IETF working group working in PMIPv6 [12, 13], Specification of PMIPv6 is still in the infancy stage, there are several issues which has to be addressed to obtain the mobility solution. Issues of Mobile IPv6 and PMIPv6 interactions, AAA support for PMIP, MPA discovery in the access networks, handover and route optimizations, Path Management and Failure Detection, Inter access handover support and multi homing scenario handover are still open in the WG. Using AAA mobility extensions and PMIPv6 supporting AAA extensions as proposed in the architecture, issues mentioned above are solved. As part of our future work we are developing dual stack PMIPv4 and PMIPv6 for mobility support in heterogeneous networks.

## 6 CONCLUSION

Post handover techniques are intended to reduce latency during roaming and handover in heterogeneous networks. As a part of this we have proposed security authentication and mobility management to optimize handover and roaming. Extending existing infrastructure such as AAA in this case is more efficient than proposing new protocols and infrastructure. As a part of it security and mobility extensions are proposed. Using the security mechanisms we estimated the latency obtained in this method is far less than any conventional methods available in the literature. The authentication keying material created dynamically, by this way the theft presentational and security vulnerabilities are reduced. The mechanisms presented are applicable to WLAN, WIMAX and cellular networks and utilizing with RII architecture the solution provides the flexibility to operate in any interworking scenarios of roaming and handover.

Proxy Mobile IP is a development of Mobile IP, where the registration is processed by the network entities. Hence, the Mobile Node does not require a Mobile IP stack to roam over the network without losing its IP address, so this can be applied to unchanged devices. Using this proposed mechanism, authentication and mobility management of users during the access is performed in parallel; in this way, latency during the authentication and re-authentication is reduced. In this mechanism, using context management the control of users can be maintained according to the access networks. Fast and seamless handover is achieved in various deployment and mobility scenarios using these mechanisms. Extending and upgrading existing networks can be performed efficiently, as no new hardware is added to the existing architectures. Multi homing scenarios, different interworking architectures of WLAN, WIMAX and 3G are addressed using the proposed mechanisms.

## 7 REFERENCES


[1] Thanh Hoa Phan, Gaute Lambertsen, Takahiko Yamada, Seamless handover supported by parallel polling and dynamic multicast group in connected WLAN micro-cell system, *Computer Communications*, *Volume 35, Issue 1*, *1 January 2012*, *Pages 89-99.*

[2] Ibrahim Al-Surmi, Mohamed Othman, Borhanuddin Mohd Ali, Mobility management for IP-based next generation mobile networks: Review, challenge and perspective, *Journal of Network and Computer Applications*, *Volume 35, Issue 1*, *January 2012*, *Pages 295-315.*

[3] Salekul Islam, Jean-Charles Grégoire, Multi-domain authentication for IMS services, *Computer Networks*, *Volume 55, Issue 12*, *25 August 2011*, *Pages 2689-2704.*

[4] Natasa Vulic, Sonia M. Heemstra de Groot, Ignas G.M.M. Niemegeers, Vertical handovers among different wireless technologies in a UMTS radio access-based integrated architecture, *Computer Networks*, *Volume 55, Issue 7*, *16 May 2011*, *Pages 1533-1548.*

[5] Leung K., Dommety G., Yegani P, Chowdhury K, "Mobility Management using Proxy Mobile IPv4," IETF RFC, January 2007.

[6] Adoba. B, "IANA Considerations for RADIUS," IETF RFC 2869, July 2003.

[7] Freeradius. [Online]. http://freeradius.org/

[8] Dynamics mobile IP. [Online]. http://dynamics.sourceforge.net/

[9] S. Parkvall, "Long-term 3G Evolution – Radio Access," Ericsson Research Report.

[10] Detailed results and logs of testbed implementations. [Online].http://193.54.225.196/pmip

[11] Vollero. L and Cacace. F, "Managing mobility and adaptation in upcoming 802.21 enabled devices," in *4th international workshop on wireless mobile applications and services on WLAN hotspots*, Los Angeles, CA, USA, September 2006.

[12] Arikko. J and et. al, "Mobility Support in IPv6," IETF RFC 3775, May 2003.

[13] Network-based Localized Mobility Management. [Online]. http://www.ietf.org/html.charters/netlmm-charter.html