Institut Eurecom[1]
Department of Mobile Communications
2229, route des Crêtes
B.P. 193
06904 Sophia Antipolis
FRANCE

Research Report RR-09-225

Combination of ad hoc mobility with IPv6 mobility mechanisms report

January 19th, 2009

Giuliana IAPICHINO
Prof. Christian BONNET

Tel: (+33) 4 93 00 82 52
Fax: (+33) 4 93 00 82 00
Email: {Giuliana.Iapichino, Christian.Bonnet}@eurecom.fr

[1] Institut Eurecom research is partially supported by its industrial members: BMW Group Research & Technology – BMW Group Company, Bouygues Telecom, Cisco Systems, France Telecom , Hitachi, SFR, Sharp, STMicroelectronics, Swisscom, Thales

TABLE OF CONTENTS

LIST OF FIGURES

List of Tables

1 INTRODUCTION

1.1 Scope of the Document

The scope of this document is to combine the most promising IPv6 mobility mechanisms, such as Proxy Mobile IPv6 (PMIPv6) micro-mobility scheme, with an ad hoc mobility solution that can easily interconnect ad hoc heterogeneous access networks with the Internet and provide at the same time an efficient macro-mobility scheme. For this purpose, the Host Identity Protocol (HIP) has been selected.
HIP enhances the original Internet architecture by adding a new layer between the IP and the transport layers. This new layer introduces a new name space consisting of cryptographic identifiers, thereby implementing the so-called identifier/locator split. In the new architecture, the new identifiers are used for naming application level end-points, thereby taking the prior identification role of IP addresses in applications, sockets, TCP connections, and UDP send and receive system calls. IPv6 addresses are still used, but only as names for topological locations in the network.
The combination of PMIPv6 and HIP provides a macro and micro-mobility solution for a heterogeneous ad hoc mesh network deployed at the disaster site and communicating to Internet and the headquarters via satellite. The proposed combination provides an efficient mechanism for intra and inter-technology handover between Public Safety users at the disaster field and it also benefits of secure end-to-end communications inside and outside the disaster area.

1.2 Structure of the Document

The document starts, in section 2, with an overview on IP layer location and handoff management and the analysis on handover latency among different IPv6 micro-mobility mechanisms. An evaluation on PMIPv6 performances over other micro-mobility schemes is also provided.

Section 3 introduces the Host Identity Protocol as an ad hoc mobility solution for ad hoc heterogeneous networks communicating with Internet, in which a common identity space is created in order to facilitate addressing and routing issues. HIP architecture and its mobility and multi-homing features are presented in details.

In section 4 the new proposal for combining the micro-mobility scheme of PMIPv6 and the macro-mobility and multi-homing aspects of HIP is described. The initialization phase together with intra and inter-technology handover phases are provided.

Finally, conclusion and applicability aspects to the advanced hybrid satellite and terrestrial system architecture for emergency mobile communications [17] are presented.

2 IPV6 MOBILITY MANAGEMENT MECHANISMS

Mobility management [1] contains two components: location management and handoff management. Different solutions try to support mobility management in different layers of the TCP/IP protocol stack reference model. IP-based heterogeneous wireless networks can greatly benefit of a network layer solution, which provides mobility-related features at IP layer without relying on or making assumption about the underlying wireless access technologies.

Location Management

Location management enables the system to track the location of Mobile Nodes (MNs) between consecutive communications, discovering their current points of attachment to the system. It includes two major tasks: *location registration* (or *location update*) and *data delivery*.

During the first step, the MN periodically notifies the network of its access point, allowing the system to authenticate the MN and to update relevant location databases with its up-to-date location information. The second task consists of determining the serving location directory of the receiving MN and locating its visiting cell/subnet.

Handoff Management

Handoff management is the process by which the system maintains a user's connection as the MT continues to move and change its access point to the network. It involves three stages: *initialization*, *new connection generation* and *data flow control*.

During initialization, the user, the network agent or changing network conditions identify the need for handoff. In the second stage, the network must find new resources for the handoff connection and perform any additional routing operations. During the final step, the delivery of the data from the old connection path to the new connection path is maintained according to agreed-upon service guarantees.

The handoff process can be intrasystem or intersystem. The first type, also called *horizontal handoff*, occurs when the user moves within a service area (or cell) and experiences signal strength deterioration below a certain threshold that results in the transfer of the user's services to new radio channels of appropriate strength at the same base station. The intersystem handoff or *vertical handoff* arises when the user is moving out of the serving network and enters another overlaying network, when it is connected to a particular network but chooses to be handed off to another network for its future service needs, or when it distributes the overall network load among different systems to optimize the performance of each individual network.

2.1 IP Layer Location Management

In the Internet, a node is identified by an IP address that uniquely identifies its point of attachment to the Internet and packets are routed to the node based on this address. Therefore, a node must be located on the network indicated by its IP address in order to receive data. This prohibits the node from moving and remaining able to receive packets using the base IP protocol. Network layer mobility management solutions are used to manage node mobility between different domains or between different subnets inside the domain [2]. IP mobility management can be broadly classified into two schemes: *macro-mobility* and *micro-mobility*, as shown in Figure 1.

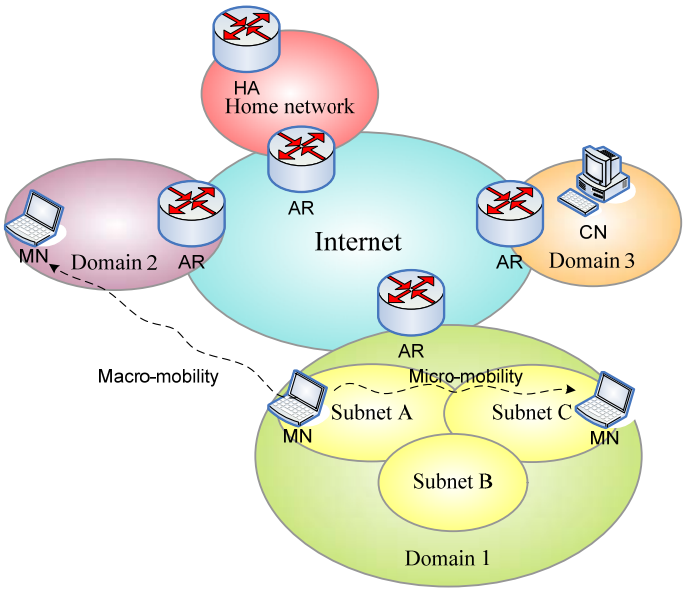

Figure 1. IP mobility schemes

2.1.1 MACRO-MOBILITY

Macro-mobility is the movement of mobile nodes between two subnets in two different network domains. The most known standard for IP mobility support is Mobile IP [3], which is the best and the most frequently adopted solution for supporting IP macro-mobility. Two versions of Mobile IP have been standardized on the Internet: Mobile IPv4 (MIPv4) [4] and Mobile IPv6 (MIPv6) [5].

MIPv6 involves three functional entities:

- Mobile Node (MN): a host or router, which changes its access point from one subnet to another without changing its home IP address.
- Home Agent (HA): a router located on a mobile node home network.
- Correspondent Node (CN): a host or router which communicates with the MN; it can be either a stationary node or a mobile node.

In MIPv6 each MN is always identified by its Home Address (HoA), regardless of its current point of attachment to the Internet. While a MN is attached to a foreign link away from home, it is addressable at its Care-of Address (CoA), an IP address associated with the MN that has the subnet prefix of a particular foreign link. The MN can acquire its CoA through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. As long as the MN stays in this location, packets addressed to this CoA are routed to the MN. The MN may also accept packets from several CoAs, such as when it is moving but still reachable at the previous link. The association between MN's HoA and CoA is known as a "binding" for the MN. The MN performs this binding registration by sending a Binding Update message to the HA, which replies by returning a Binding Acknowledgement message.

One of the main advantages of MIPv6 over MIPv4 is the *route optimization,* which allows direct communication between MN and CN without going through the HA. It requires that the MN registers its current binding at the CN. Packets from the CN can be routed directly to the MN's CoA. When sending a packet to any IPv6 destination, the CN checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the MN by way of the CoA indicated in this binding.

2.1.2 MICRO-MOBILITY

Micro-mobility is the movement of MNs between two subnets within the same domain. Although MIPv6 is a mature standard for IP macro-mobility support and solve many problems such as triangle routing, security and limited IP address space, addressed in MIPv4, it still reveals some problems in the case of micro-mobility support. Hierarchical Mobile IPv6 (HMIPv6) [6] is an extension to MIPv6 to improve local mobility handling, reducing significantly the signalling and the handover delay between MN, CN and HA.

HMIPv6 is based on the functionalities of a new node called Mobility Anchor Point (MAP), a router located in the network visited by the MN and used by the MN as a local HA. A MN entering a MAP domain receives Router Advertisement messages containing information on one or more local MAPs. The MN can bind its current location (on-link CoA) with an address on the MAP's subnet (Regional Care-of Address (RCoA)). Acting as a local HA, the MAP receives all packets on behalf of the MN it is serving and encapsulates and forwards them directly to the MN's current address. If the MN changes its current address within a local MAP domain (on-link Care-of Address (LCoA)), it only needs to register the new address with the MAP. Hence, only the RCoA needs to be registered with CNs and the HA. The RCoA does not change as long as the MN moves within a MAP domain. This makes the MN's mobility transparent to the CN it is communicating with.

HMIPv6 is a *host-based* mobility management protocol, as it requires MN's participation in mobility related signalling. On the contrary, in a *network-based* mobility management approach, like in PMIPv6 [7], the serving network handles the mobility management on behalf of the MN.

The two approaches for micro-mobility have different impact on deployment and performance points of view:

- Host-based network layer approaches require protocol stack modification of the MN in order to support them, causing increased complexity on the MN. Network-based approaches support unmodified MNs, accelerating their practical deployment.
- Host-based approaches imply tunneling overhead as well as significant number of mobility-related signaling message exchanges via wireless links due to the MN's involvement in the mobility signaling. On the other side, with a network-based solution, an efficient use of wireless resources can result in the enhancement of network scalability and handover latency.

2.1.2.1 Proxy Mobile IPv6

The IETF has recommended a Network-based approach to Localized Mobility Management, called NETLMM, based on Proxy Mobile IPv6. PMIPv6 is an extension of MIPv6 as it reuses its signalling and many concept such as HA functionalities. As PMIPv6 is designed to provide network-based mobility management support to a MN in a topologically localized domain, its innovative point is that it exempts the MN from participating in any mobility-related signalling and proxy mobility agents in the serving network perform mobility-related signalling on behalf of the MN.

Once the MN enters a PMIPv6 domain and performs access authentication, the serving network ensures that the MN believes it is always on its home network and can obtain its HoA on any access network. The serving network assigns a unique home network prefix to each MN whenever they move within the PMIPv6 domain. Thus, for MNs the entire PMIPv6 domain appears as their home network.

As shown in Figure 2, this mechanism is possible thanks to two core functional entities in the NETLMM infrastructure:

- *Local Mobility Anchor (LMA)*: it is similar to HA in MIPv6. LMA is responsible for maintaining the MN's reachability state and it is the topological anchor point for the MN's home network prefix. LMA includes a binding cache entry for each currently registered MN with MN-Identifier, the MN's home network prefix, a flag indicating the proxy registration and the interface identifier of the bidirectional tunnel between the LMA and MAG.
- *Mobile Access Gateway (MAG)*: it is the entity that performs the mobility management on behalf of the MN and it resides on the access link where the MN is anchored. The MAG is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA. Moreover, the MAG establishes a tunnel with the LMA for enabling the MN to use an address from its home network prefix and emulates the MN's home network on the access network for each MN.

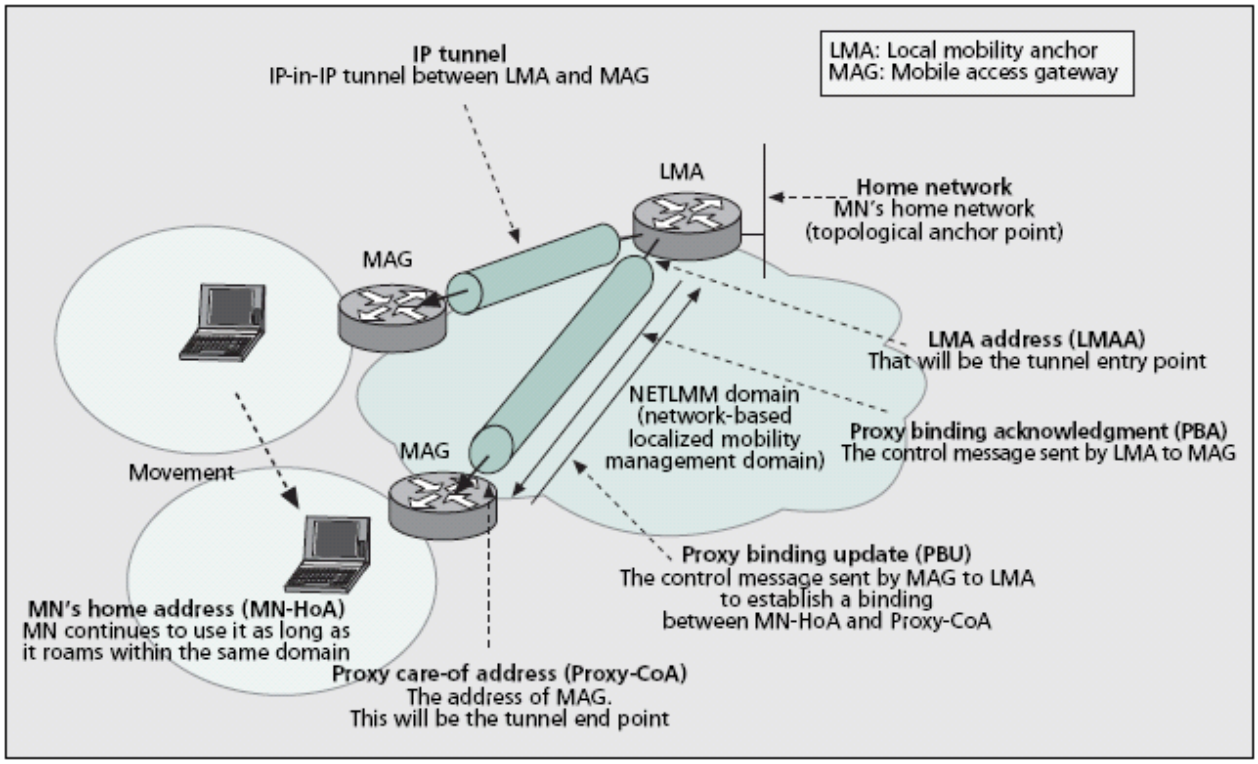

Figure 2. Overview of PMIPv6

The main steps in the PMIPv6 mobility management scheme are described hereafter and shown in Figure 3:

- MN attachment: once a MN enters a PMIPv6 domain and attaches to an access link, the MAG on that access link performs the access authentication procedure with a policy server using the MN's profile, which contains MN-Identifier, LMA address and other related configuration parameters;
- Proxy Binding exchange: the MAG sends to the LMA a Proxy Binding Update (PBU) message on behalf of the MN including the MN-Identifier. Upon accepting the message, the LMA replies with a Proxy Binding Acknowledgment (PBA) message including the MN's home network prefix. With this procedure the LMA creates a Binding Cache entry for the MN and a bi-directional tunnel between the LMA and the MAG is set up;
- Address Configuration procedure: at this point the MAG has all the required information for emulating the MN's home link. It sends Router Advertisement message to the MN on the access link advertising the MN's home network prefix as the hosted on-link-prefix. On receiving this message, the MN configures its interface either using stateful or stateless address configuration modes. Finally the MN ends up with an address from its home network prefix that it can use while moving in the PMIPv6 domain.

The LMA, being the topological anchor point for the MN's home network prefix, receives all packets sent to the MN by any CN and forwards them to the MAG through the bi-directional tunnel. The MAG on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the MN. The MAG typically acts as a default router on the access link. It intercepts any packet that the MN sends to any CN and sends them to its LMA through the bi-directional tunnel. The LMA on the other end of the tunnel, after receiving the packet, removes the outer header and routes the packet to the destination.

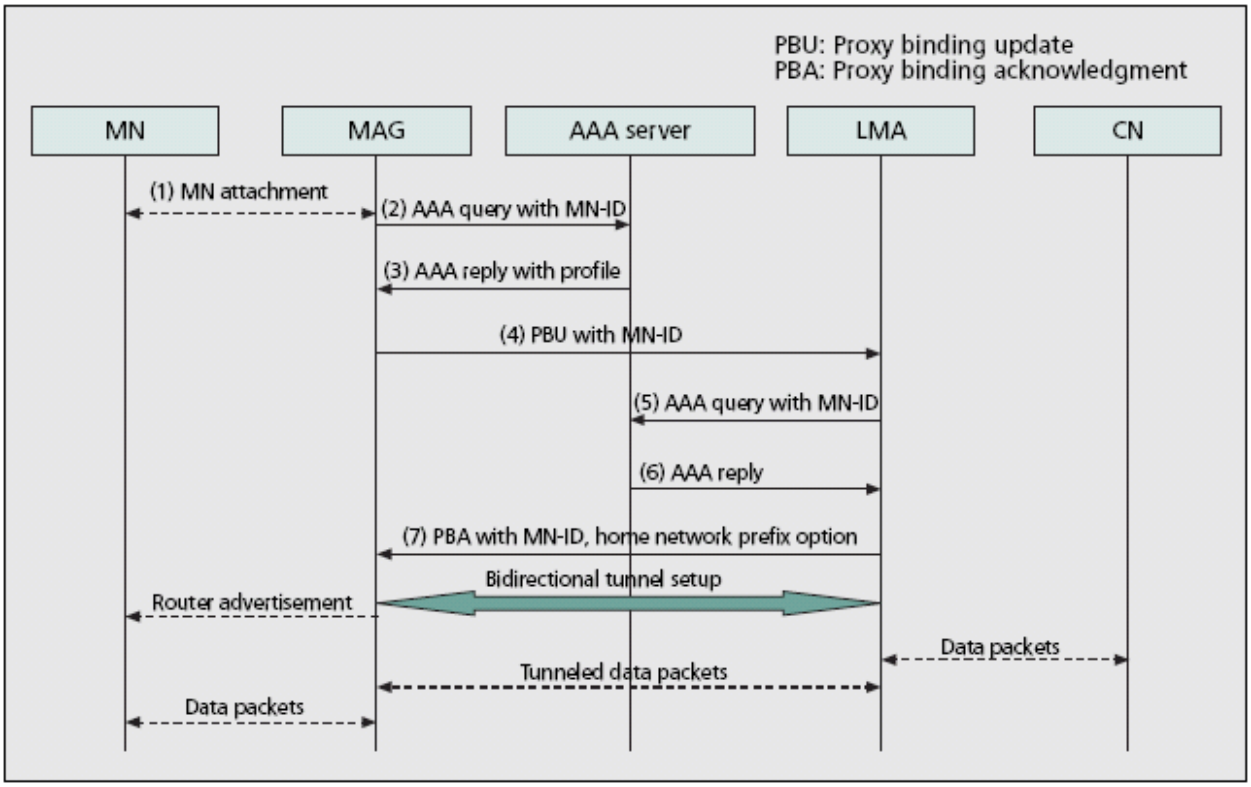

Figure 3. Message flow in PMIPv6

2.2 IP layer handoff management and analysis

Handover latency is one of the most critical factors for the next-generation all-IP mobile networks. In order to demonstrate the efficiency of PMIPv6 under this point of view, it is interesting to compare it not only with the location management protocols as MIPv6 and HMIPv6, but also with the specific enhancement of MIPv6 for reducing the handover delay: Fast Handover for MIPv6 (FMIPv6) [8].

FMIPv6 is an extension of MIPv6 and provides the mobility support for the MN under the assistance of enhanced Access Routers (ARs). FMIPv6 configures the New CoA (NCoA) based on the link layer information in advance to shorten the handover delay, and it also setup the tunnel between Previous AR (PAR) and New AR (NAR) to minimize the packet loss during the handover. There are two types of FMIPv6, predictive and reactive FMIPv6, depending on the fact that the Fast Binding Update (FBU) is sent directly by the MN to the PAR or through the NAR.

Figure 4 summarizes the handover procedure of MIPv6, predictive and reactive FMIPv6, HMIPv6 and PMIPv6.

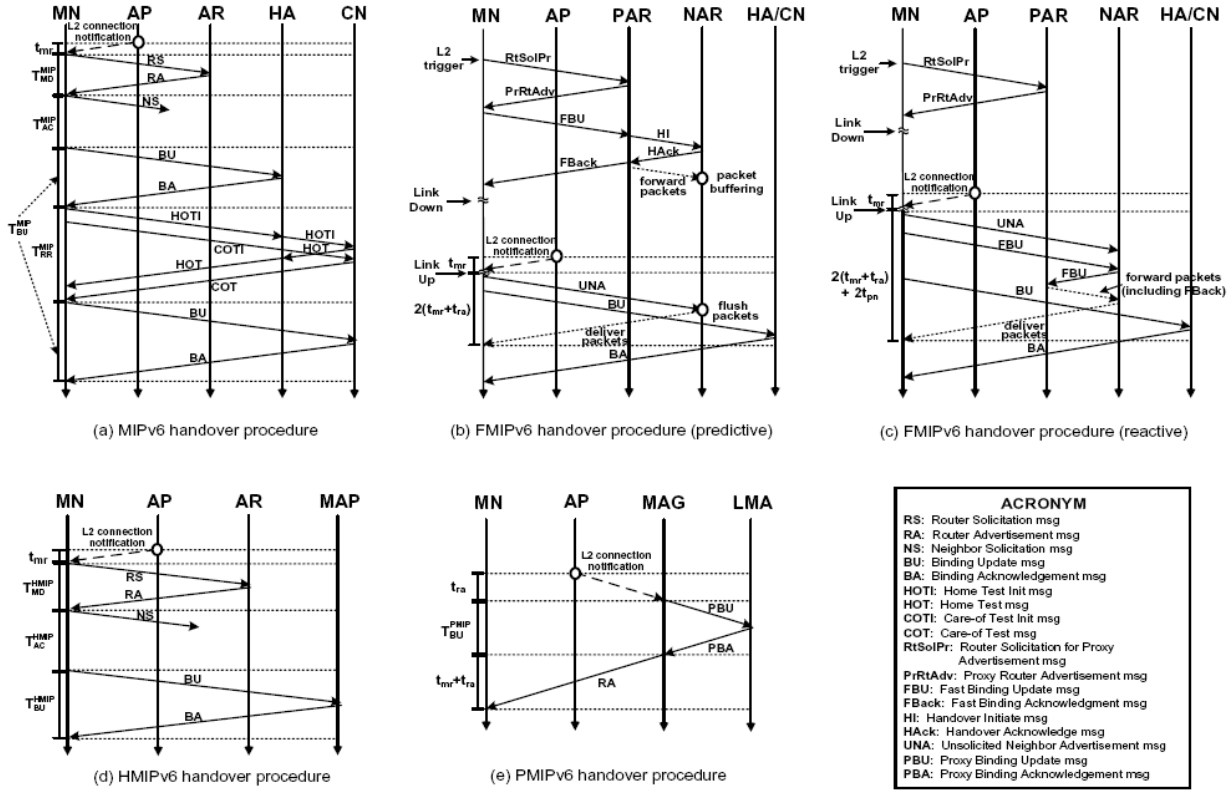

Figure 4. Handover procedure for each protocol.

The handover latency [10] is defined as the time that elapses between the moment in which the L2 handover completes at the AP and the moment the MN receives the first packet after moving to the new point-of-attachment. It can be expressed as

$$T_{HO} = T_{L2} + T_{MD} + T_{AC} + T_{AAA} + T_{BU}$$

where T_{L2} represents the delay due to layer 2 signalling, T_{MD} the movement detection delay, T_{AC} the address configuration delay, T_{AAA} the delay involved in performing the AAA procedure and T_{BU} the binding update delay. It is assumed that, for all the protocols, the MN is allowed to access a service provider's network after the AAA procedure is completed, so T_{AAA} is not considered in the analysis.

The following notation is used for the analysis as shown in Figure 5:

- The delay between the MN and the AP is t_{mr}, which is the time necessary for a packet to be sent between the MN and the AP through a wireless link.
- The delay between the AP and the AR/MAG is t_{ra}, which is the time between the AP and the AR/MAG connected to the AP.
- The delay between the AR/MAG and the MAP/LMA (i.e., the delay between AR and MAP in HMIPv6 or between MAG and LMA in PMIPv6) is t_{am}.
- The delay between the AR/MAG and the HA is t_{ah}.
- The delay between the AR/MAG and the CN, not via the HA is t_{ac}.
- The delay between the HA and the CN is t_{hc}.
- The delay between NAR and PAR is $t_{pn.}$

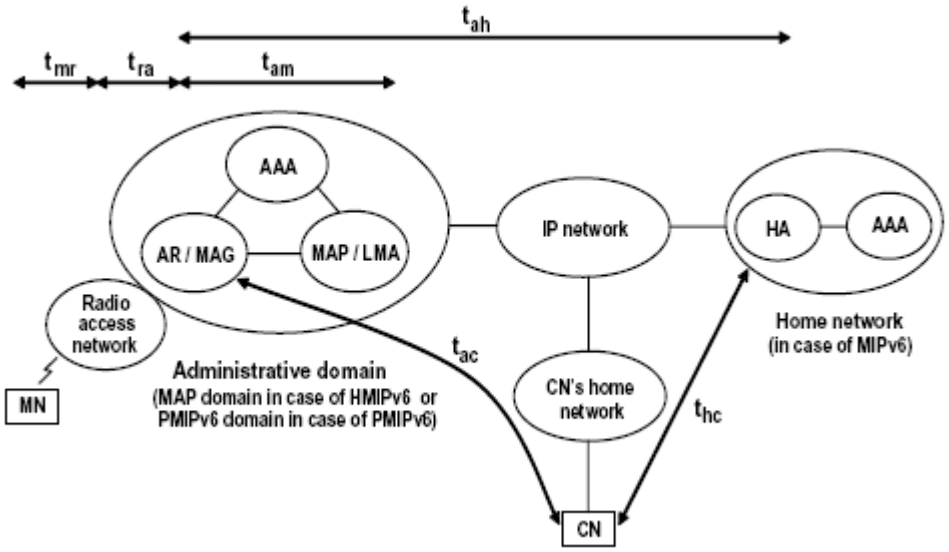

Figure 5. Network model for performance analysis

It is interesting to analyse the handover latency for each protocol:

- MIPv6:
  a) T_{L2} is equivalent to t_{mr};
  b) T_{MD} is calculated considering the delay due to the reception of an unsolicited RA message. Each router that supports mobility is configured with a *MinRtrAdvInterval (MinInt)* and *MaxRtrAdvInterval (MaxInt)*. The mean time between unsolicited RA messages is expressed as *(MinInt + MaxInt)/2* so the T_{MD} is half of that, thus *(MinInt + MaxInt)/4*;
  c) T_{AC} is due to the duplicate address detection (DAD) process and can be expressed as $R \times D$, where R is *RetransTimer* and D is the *DuplAddrDetectTransmit*;
  d) T_{BU} includes the time of the binding update delay to the HA (i.e., $2(t_{mr}+ t_{ra}+ t_{ah})$), the binding update delay to the CN (i.e., $2(t_{mr}+ t_{ra}+ t_{ac})$) and the delay for the return routability (i.e., $2(t_{mr}+ t_{ra}+ t_{ah}+ t_{hc})$).

$$T_{HO}^{MIPv6} = t_{mr} + \frac{MinInt + MaxInt}{4} + R \times D + 2\left(t_{mr} + t_{ra} + t_{ah}\right) + 2\left(t_{mr} + t_{ra} + t_{ac}\right) + 2\left(t_{mr} + t_{ra} + t_{ah} + t_{hc}\right)$$
$$= \frac{MinInt + MaxInt}{4} + R \times D + 7t_{mr} + 6t_{ra} + 4t_{ah} + 2\left(t_{ac} + t_{hc}\right)$$

- HMIPv6:
  a) T_{L2} is equivalent to t_{mr};
  b) T_{MD} is calculated as in MIPv6;
  c) T_{AC} is calculated as in MIPv6;
  d) T_{BU} includes the time of the binding update delay from MN to the MAP (i.e., $2(t_{mr}+ t_{ra}+ t_{am})$).

$$T_{HO}^{HMIPv6} = t_{mr} + \frac{MinInt + MaxInt}{4} + R \times D + 2\left(t_{mr} + t_{ra} + t_{am}\right) = \frac{MinInt + MaxInt}{4} + R \times D + 3t_{mr} + 2\left(t_{ra} + t_{am}\right)$$

- FMIPv6:
  a) T_{L2} is equivalent to t_{mr};
  b) T_{MD} is null as the IP-level movement detection does not occur during the handover procedure;
  c) T_{AC} is null as the MN is informed of the NAR's network prefix via the PAR and can validate the uniqueness of the prospective CoA on the NAR prior to the MN's movement;
  d) T_{BU} is due to the Unsolicited Neighbor Advertisement (UNA) message sent by the MN to the NAR in order to quickly announce the MN's attachment to the NAR. Depending on the preactive or reactive mode, T_{BU} is equivalent to $2(t_{mr} + t_{ra})$ or to $2(t_{mr} + t_{ra} + t_{pn})$.

$$T_{HO}^{FMIPv6-pre} = t_{mr} + 2\left(t_{mr} + t_{ra}\right) = 3t_{mr} + 2t_{ra}$$
$$T_{HO}^{FMIPv6-rea} = t_{mr} + 2\left(t_{mr} + t_{ra} + t_{pn}\right) = 3t_{mr} + 2\left(t_{ra} + t_{pn}\right)$$

- PMIPv6:
  a) T_{L2} is equivalent to t_{ra};
  b) T_{MD} is null as the IP-level movement detection does not occur.
  c) T_{AC} is null as it occurs only when the MN enters a PMIPv6 domain, then the MN keeps the same address inside the domain;
  d) T_{BU} is composed of the sum of the proxy binding update delay between the MAG and the LMA $2t_{am}$ and the packet delivery delay from the MAG to the MN $t_{mr} + t_{ra}$.

$$T_{HO}^{PMIPv6} = t_{ra} + 2t_{am} + t_{mr} + t_{ra} = 2t_{ra} + 2t_{am} + t_{mr}$$

Based on the previous analysis and on the values in Table 1 [9], in which it is assumed a low bandwidth wireless link between the MN and the AR, it is possible to show the following numerical results.

t_{mr}	t_{ra}	t_{am}= t_{hc}	t_{ah}= t_{ac}	t_{pn}	MinInt	MaxInt	R	D
10 ms	2 ms	20 ms	40 ms	5 ms	30 ms	70 ms	1000ms	1

Table 1. Parameters used for the performance analysis

Figure 6 shows that the handover latency gets larger as the wireless link delay increases for all the protocols. In particular, MIPv6 first and then also HMIPv6 are the most affected protocols as they require the largest number of messages exchanged over the wireless link. We can also see that, for small t_{mr}, FMIPv6-pre has lowest handover latency, but as t_{mr} increases, PMIPv6 performs better.

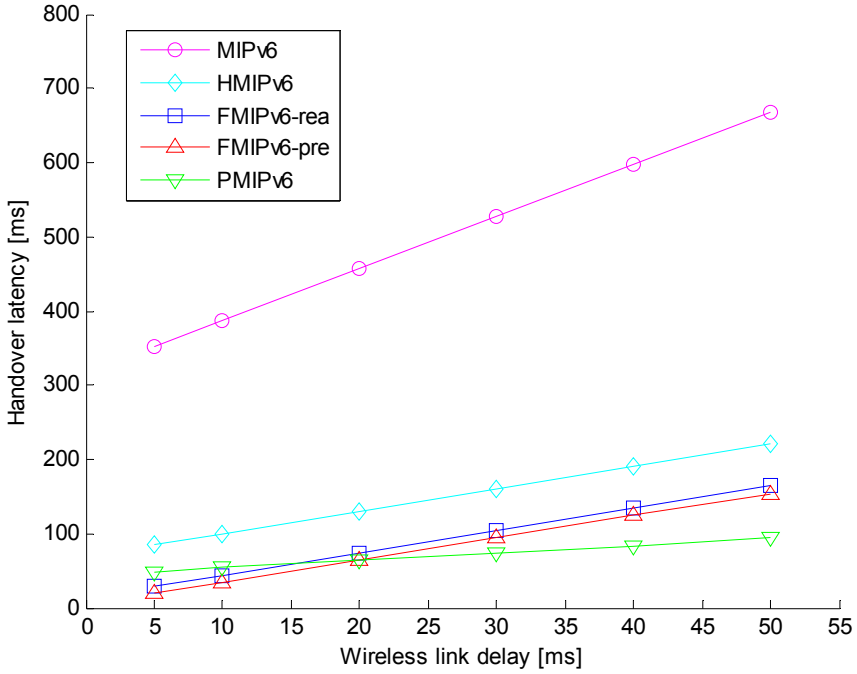

Figure 6. Handover latency vs. wireless link delay

Figure 7 evaluates the impact of T_{MD} over the handover latency. The IP-level movement detection affects only MIPv6 and HMIPv6, as in PMIPv6 the same IP address is kept by the MN in the PMIP domain and in FMIPv6 the MN is informed of the NAR's network prefix before its movement.

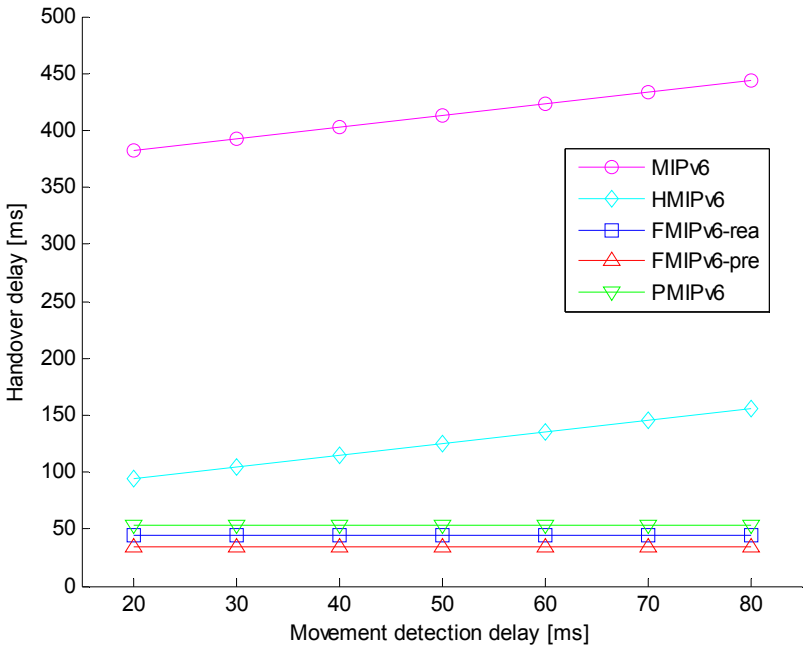

Figure 7. Handover delay vs. movement detection delay

Figure 8 evaluates the impact of $(t_{mr} + t_{ra} + t_{ac})$ over the handover latency. In particular, we focus on investigating the change of t_{ac}, keeping the other two parameters fixed to the values in Table 1. Only for MIPv6 the handover latency increases with the increasing of the delay between MN and CN, as MIPv6 requires the binding update to the CN as well as the HA whenever the MN moves across subnets. HMIPv6 and PMIPv6 are not affected because MN's movements within the domain as transparent to the outside of the domain.

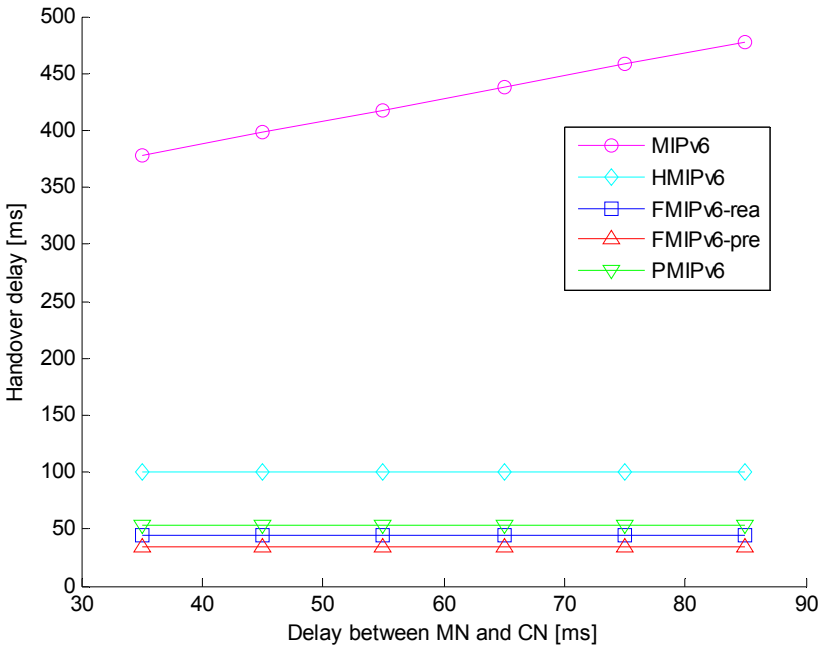

Figure 8. Handover latency vs. delay between MN and CN

Figure 9 shows the impact of $(t_{mr} + t_{ra} + t_{am})$ over the handover latency. We focus the investigation only on the change of t_{am} and, in addition, we suppose $t_{ac} = t_{am} + 20$ ms as it is assumed that the CN is located outside the domain. The handover latency of MIPv6, HMIPv6 and PMIPv6 gets larger as t_{am} increases, while FMIPv6 is not affected. We can see that PMIPv6 performs better than FMIPv6-pre only when the delay between MN and LMA is small.

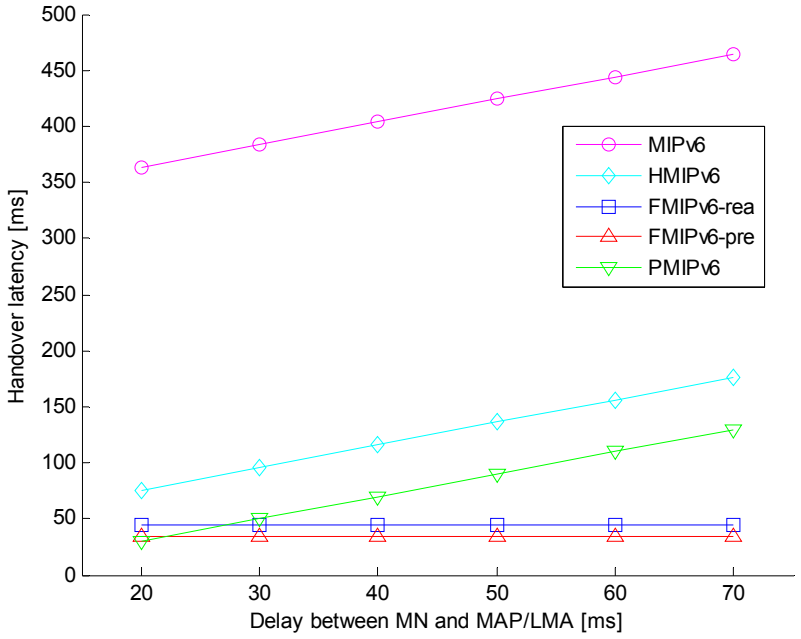

Figure 9. Handover latency vs. delay between MN and MAP/LMA

From the comparative analysis, we can see that the handover latency of PMIPv6 is much lower than those of MIPv6 and HMIPv6, while the handover latency comparison of PMIPv6 and FMIPv6 is dependent on the values of several parameters.
In order to understand better the behaviour of PMIPv6 and FMIPv6-pre in Figure 6 and Figure 9, it is interesting to see under which conditions $T_{HO}^{FMIPv6-pre} \geq T_{HO}^{PMIPv6}$, so then

$$3t_{mr} + 2t_{ra} \geq 2t_{ra} + 2t_{am} + t_{mr}$$
$$t_{mr} \geq t_{am}$$

Thus, the handover latency of PMIPv6 is smaller than the one of FMIPv6-rea only when t_{mr} is greater than $t_{am.}$

3 AD HOC MOBILITY

Ad hoc access networks are *ad hoc networks* that contain one or several nodes that act as gateways to a fixed network, such as the Internet. The Internet uses hierarchical IP addresses as a basis for routing. Many ad hoc networks routing protocols use flat identities. The ad hoc routing protocol may or may not be based on IP. There are many IP based proposals, such as AODV and DSR. In addition, distributed hash tables based on flat addresses have been integrated with MANET routing protocols.

The Host Identity Protocol (HIP) changes the transport level connections by associating them with Host Identities rather than IP addresses. This makes it easier to bridge connections between IP networks and ad hoc access network since the Host Identities can be easily used in many different kinds of networks. In IP networks the creation of a transport session requires the use of the HIP Base Exchange, which creates an association between IP addresses and Host Identities for that session. This association is required, because routing in IP networks requires the address information of the recipient.

In ad hoc networks, hierarchical addressing is not typically used. With HIP both ad hoc networks and the Internet have a common identity space. This leaves us with the problem of doing the necessary translation between identities and IP addresses. In order to be able to communicate both within an ad hoc network and fixed-network hierarchical IP networks, the ad hoc node needs to have a dual stack that supports both the ad hoc networking protocol and the IP protocol. HIP can be implemented to support both, which makes the mapping between ad hoc nodes and IP network nodes easier.

3.1 Host Identity Protocol

Currently the IP address has two functions; it is a *locator* used to route traffic to the destination node and at the same time it serves as the *identifier* of the node. The dual role of the IP address causes some problems. When a mobile node moves to another location in the network topology the IP address of the node changes. The consequence of this is that the information used to route packets to that node is changed. But, as the IP address also serves as the identifier, the identifier is also changed. This means that the same node would have different identifiers depending on where it is positioned in the network. To be useful the identifier to be should remain the same regardless of where the node is located.

Methods for solving the ambiguity problem of the IP address have been presented. There are solutions that attempt to solve the problem using resources and technologies we have now. An example of this is Mobile IP, which tries to fix the problem by assigning multiple IP addresses to a node. This is more like bypassing the problem instead of repairing it. There are also solutions that instead try to separate the identifiers from the routing information by modifying the current architecture. One such proposal is the Host Identity Protocol (HIP) [11].

HIP separates the identifier from the locator with the help of a new entity, the Host Identity (HI). The IP address is still used as the locator while the HI serves as the identifier. The HI is the public key of an asymmetric key-pair. However, because of its length it is not feasible to use it during actual communication. Instead a 128-bit hash of the HI, called the Host Identity Tag (HIT), is used. The length of the HIT allows it to be used instead of an IPv6 address at higher layers. In a HIP capable node, when using HIP, the applications use the HIT as the destination for the packets. The IP address is hidden from the applications and a translation from HIT to IP address must be made at some point in the IP-stack. To handle this translation a new layer is added to the network architecture. In Figure 10 the new architecture, with the new Host Identity layer, is presented. In all layers above the Host Identity layer, a HIT is used instead of an IP address to represent the host. At the Host Identity layer the HIT is translated into an IP address for correct routing in the network (or IP address to HIT when receiving packets). In all layers below the Host Identity layer everything works as in the current architecture. A node learns of the HIT of a peer in the same manner as it would a normal IP address, e.g. via DNS.

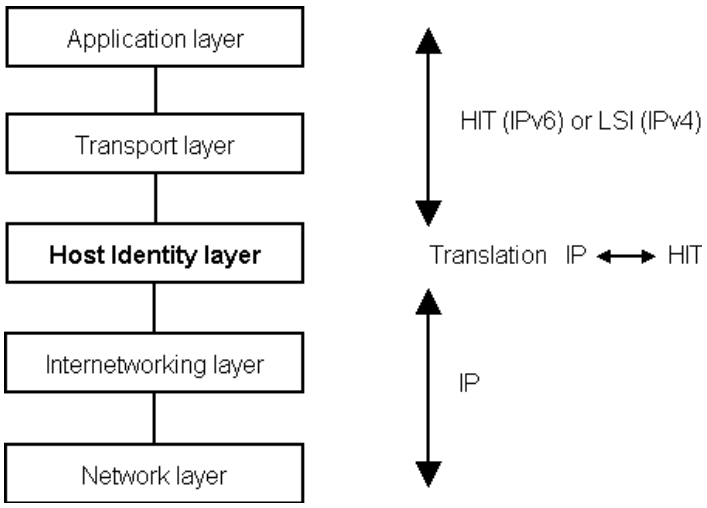

Figure 10. HIP architecture

Before two HIP nodes can communicate with each other using HIP they perform a 4-way handshake called the HIP base exchange. During the base exchange they create a session key, using the Diffie-Hellman (DH) procedure [12], to be used in IPsec Encapsulating Security Payload (ESP) Security Associations (SA). Instead of binding the SAs to IP addresses as the current IPsec defines, the SAs are bound to HITs. Because of this, even if one of the nodes moves and gets a new IP address, the SAs stay valid.
Figure 11 illustrates a HIP negotiation packet before the SA's are established. When the IPsec SA's are established, the packet used for the actual data transfer look like illustrated in Figure 12. However HIP control packets will still look like the packets shown in Figure 11.

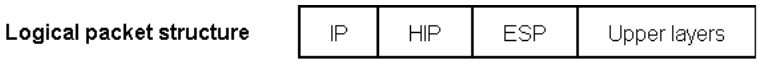

Figure 11. Logical HIP packet structure

Figure 12. Actual HIP data packet structure

3.1.1 HIP BASE EXCHANGE

HIP Base Exchange (BE) is necessary for any HIP-based communication. BE is a four-way handshaking process, that contains a DH key exchange to establish the HIP connection. A session key is created under the DH process. This session key is used to establish a pair of IPSec Security Associations (SA) between hosts during the HIP BE. A cookie mechanism is used in the BE to protect the responder from Denial-of-Service (DoS) threats. The complete process is explained hereafter in details and illustrated in Figure 13.

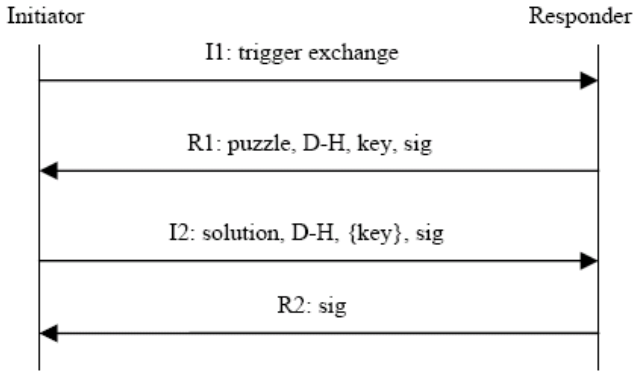

Figure 13. HIP Base Exchange

A BE starts with the initiator sending a trigger packet (I1) to the responder. This packet is a lightweight trigger packet containing only the source HIT and possibly the destination HIT, if known. The intention of the trigger packet is to be a small packet telling the responder: “Let’s talk HIP”. It furthermore is designed to avoid DoS attacks of the receiver, since he can remain stateless and only needs to send a pre-computed packet in response (the R1 packet).

The R1 packet then starts the actual Base Exchange. The packet contains a pre-computed cryptographic puzzle the initiator must solve before continuing the Base Exchange. The R1 generation counter (R1_COUNTER) is used to mark the puzzle and is later on used to validate the puzzle when it is returned by the initiator. The puzzle contains a random number I and the difficulty K. The difficulty K is the number of bits, which the initiator must get to zero. The packet is signed except the random number I, which is zeroed among calculation of the signature.

By zeroing the random number using the signature calculation, it allows the responder to select and set the number I into a pre-computed R1 just prior to sending it.
To distribute IPSec session encryption keys used for the HIP connection, the Base Exchange performs a Diffie-Hellman key exchange. This starts in the R1 packet and continues in the I2 packet. The D-H value is ephemeral but can be reused over a number of connections. As a defense against I1 packet storms, it is possible to use the same D-H value for a period of time by using a small number of different cookies for the D-H value. This opens the above mentioned possibility to pre-compute R1 packets and to deliver them quickly and without increased computational cost.

The I2 packet is the initiators response to the R1 packet. The I2 packet contains the solution to the received puzzle and the unmodified cookie (R1_COUNTER) so the responder easily can validate the puzzle against the correct solution. The solution contains the random number I from R1 and the computed number J consists of the low order K bits of the SHA-1(I | ... | J) that must be zero. If the solution is not correct, the I2 message is dropped. The I2 message also contains the D-H parameter that carries needed information for the responder. The packet is signed by the initiator to check the message confidentiality.

The R2 packet is the last packet of the HIP Base Exchange. It is a HMAC signature of the R2 packet, which ends the handshake.

When the HIP BE is finished two unidirectional IPSec SA's (using IPSec transport mode) are established between the initiator and the responder. They are now able to send encrypted IPsec packets between each other using ordinary IPv6. Furthermore if one of the nodes now changes its IP-address, HIP will inform the other node about this and the connection can continue using the new IP-address.

3.1.2 HIP MOBILITY AND MULTIHOMING

HIP mobility and multi-homing [13] is independent from any protocols and the HIP ESP mobility scheme has been well defined so far.
Since the pair of SAs created by BE are not bounded to the IP address but to the HIT, a host can receive packets that are protected by SA from any IP addresses. After the handover in the lower layers is complete, the MN sends a HIP UPDATE packet with a LOCATOR parameter to its CNs to notify the change of IP address. CN uses the UPDATE packet with an Addressing Check (AC) parameter to request an address check. Once the MN replies to the address check, the handover is complete.
The HIP UPDATE packet is protected by the HIP security mechanism, so it does not need any additional mechanisms to guard against security threats, such as Return Routability in Mobile IP.
Multi-homing allows a host to receive packets from different network interfaces by using one host identity. MIP does not support multi-homing. HIP uses HIP UPDATE packets or HIP BE packets to notify the CN about the additional interface.

Mobility with a single SA pair

A mobile host must sometimes change an IP address bound to an interface. The change of an IP address might be needed due to a change in the advertised IPv6 prefixes on the link, a reconnected PPP link, a new DHCP lease, or an actual movement to another subnet. In order to maintain its communication context, the host must inform its peers about the new IP address.
The simplest scenario in which the mobile host has only one interface, IP address, a single pair of SAs (one inbound, one outbound), and no rekeying occurs on the SAs, is explained hereafter.

The steps of the packet processing are as follows:

- The mobile host is disconnected from the peer host for a brief period of time while it switches from one IP address to another. Upon obtaining a new IP address, the mobile host sends a LOCATOR parameter to the peer host in an UPDATE message. The UPDATE message also contains an ESP_INFO parameter containing the values of the old and new SPIs for a security association. In this case, the OLD SPI and NEW SPI parameters both are set to the value of the preexisting incoming SPI; this ESP_INFO does not trigger a rekeying event but is instead included for possible parameter-inspecting middleboxes on the path. The LOCATOR parameter contains the new IP address and a locator lifetime. The mobile host waits for this UPDATE to be acknowledged, and retransmits if necessary.
- The peer host receives the UPDATE, validates it, and updates any local bindings between the HIP association and the mobile host's destination address. The peer host MUST perform an address verification by placing a nonce in the ECHO_REQUEST parameter of the UPDATE message sent back to the mobile host. It also includes an ESP_INFO parameter with the OLD SPI and NEW SPI parameters both set to the value of the preexisting incoming SPI, and sends this UPDATE (with piggybacked acknowledgment) to the mobile host at its new address. The peer MAY use the new address immediately, but it MUST limit the amount of data it sends to the address until address verification completes.
- The mobile host completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO_RESPONSE. Once the peer host receives this ECHO_RESPONSE, it considers the new address to be verified and can put the address into full use.

While the peer host is verifying the new address, the new address is marked as UNVERIFIED in the interim, and the old address is DEPRECATED. Once the peer host has received a correct reply to its UPDATE challenge, it marks the new address as ACTIVE and removes the old address.

Host multihoming

Consider the case between two hosts, one single-homed and one multihomed. The multihomed host may decide to inform the singlehomed host about its other address. It is recommended that the multihomed host set up a new SA pair for use on this new address. To do this, the multihomed host sends a LOCATOR with an ESP_INFO, indicating the request for a new SA by setting the OLD SPI value to zero, and the NEW SPI value to the newly created incoming SPI. A

Locator Type of "1" is used to associate the new address with the new SPI. The LOCATOR parameter also contains a second Type "1" locator, that of the original address and SPI. To simplify parameter processing and avoid explicit protocol extensions to remove locators, each LOCATOR parameter must list all locators in use on a connection (a complete listing of inbound locators and SPIs for the host). The multihomed host waits for an ESP_INFO (new outbound SA) from the peer and an ACK of its own UPDATE. As in the mobility case, the peer host must perform address verification before actively using the new address.

In multihoming scenarios, it is important that hosts receiving UPDATEs associate them correctly with the destination address used in the packet carrying the UPDATE. When processing inbound LOCATORs that establish new security associations on an interface with multiple addresses, a host uses the destination address of the UPDATE containing the LOCATOR as the local address to which the LOCATOR plus ESP_INFO is targeted. This is because hosts may send UPDATEs with the same (locator) IP address to different peer addresses - this has the effect of creating multiple inbound SAs implicitly affiliated with different peer source addresses.

4 PMIPV6 AND HIP: COMBINING MICRO-MOBILITY WITH ACCESS HETEROGENEITY AND SECURITY

Comparing the most promising macro-mobility solutions (HIP and MIPv6) in a heterogeneous IPv6 network environment, it has been proved that HIP performs better than MIPv6 in terms of handover latency [14], providing also security and multi-homing features.
Several micro-mobility solutions have been proposed for MIPv6 as described in chapter 2. On the contrary, only few micro-mobility proposals have been presented for HIP, which still represent partial solution to the problem and still need improvements to develop all HIP's potentialities.
Those micro-mobility proposals are mainly based on HMIPv6 scheme as in [15] and [16].

In [15], Novaczki et al. propose a Local Rendezvous Server (LRVS), which acts as a Mobile Routing Point (MRP) in the domain – a micro-mobility management scheme enhanced router with a concept similar to the MAP. The MN needs to register itself not only in the RVS but also in the LRVS. When the MN performs a handover, it will notify the LRVS instead of the CN, to redirect all HIP-based communication streams into its new address. Novaczki's scheme is efficient as a macro and micro-mobility solution, but it does not consider the inter-technology and the multi-homing scenarios.
In [16], So and Wang propose a new HIP architecture composed of micro-HIP (mHIP) agents: mHIP gateways and mHIP routers. mHIP agents under the same network domain share a common HIT to represent the whole mHIP domain and can sign messages on behalf of the group. This scheme permits to distribute the load of the LRVS in Novaczki's scheme among mHIP agents and provides a framework in which any number of security scheme can be adopted. It also takes into account the inter-technology and multi-homing issues, but introduces more complexity in the architecture. A modified SPINAT device has to be implemented in the mHIP agents to allow the overlay routing based on SPI. Moreover, the MN registers itself in the mHIP gateway and also registers itself with the HIT of the mHIP gateway in its RVS. This means that each time the MN moves to a new domain, the MN changes the HIT and the macro-mobility of HIP is not supported anymore. Finally, the number of signaling messages traversing the domain is still high as the MN needs to update the mHIP gateway with the new IP address each time the MN moves from a mHIP router to another one.

Considering the success of PMIPv6 on the other micro-mobility solutions for MIPv6, we suggest to implement a PMIPv6-based scheme for HIP micro-mobility.
In the next paragraphs, we introduce our new HIP and PMIPv6 combination, which provides several advantages to both protocols:

- PMIPv6 can benefit of:
    - Security: end-to-end secure associations are maintained between the MN and the CN through HIP scheme, even during MN movements;
    - Inter-technology handover and multi-homing: they are guaranteed by HIP features as applications are not linked to MN's locator (IP address) anymore, but to MN identifier (HIT_MN is used as MN_ID);
- HIP can benefit of:
    - Micro-mobility management of PMIPv6 scheme.

4.1 Initialization

First of all, some assumption has to be done for the proposed scheme, like in So's scheme.
We suppose that all the entities in the PMIPv6 domain (LMA and MAGs), besides their own HIT, are sharing a common HIT (HIT_domain) to represent the whole PMIPv6 domain. We suppose also that each entity can sign messages on behalf of the domain thanks to signature_domain. The MN can verify the signature of the group.

The first part of the initialization phase is quite similar to PMIPv6 initialization [RFC 5213].
When a MN enters a Proxy Mobile IPv6 domain and attaches to an access link, the MAG on that access link, after identifying the MN and acquiring its identity, will determine if the MN is authorized for the network-based mobility management service.

In the first step, a MN attached to the PMIPv6 domain network is detected by the MAG. The MAG sends access request message to Authentication, Authorization and Accounting (AAA) server to obtain the MN identifier (HIT_MN) and profile, together with the Mobility Management Key (MMK).

For updating the LMA about the current location of the MN, the MAG sends a Proxy Binding Update message to the LMA with HIT_MN, the interface_ID and the access technology type (ATT). Upon receiving and checking the validity of this Proxy Binding Update message, the LMA sends a Proxy Binding Acknowledgement message including the MN's home network prefix. It also creates the Binding Cache entry in which registers the HIT_MN, the prefix, the new MN's IP address, the MAG's IP address and sets up its endpoint of the bi-directional tunnel to the MAG.

The MAG on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the LMA and also sets up the forwarding for the mobile node's traffic. At this point, the MAG has all the required information for emulating the MN's home link. It sends Router Advertisement messages to the MN on the access link advertising the MN's home network prefix as the hosted on-link prefix.
The MN, on receiving these Router Advertisement messages on the access link, attempts to configure its interface using either stateful or stateless address configuration modes, based on the modes that are permitted on that access link as indicated in Router Advertisement messages. At the end of a successful address configuration procedure, the MN has one address from its home network prefix.

The MN has to send an UPDATE message to its RVS with the new IP address. Once this message arrives at the MAG it will start the Passive Service Discovery procedure after forwarding the packet. It will send a Service Announcement packet for mobility management to the MN. The message contains the HIT_group and the signature_group. The MN, that is interested in the offered service, can complete the registration process by sending I2 to the MAG. A R2 packet from the MAG will conclude the registration.

An UPDATE message for the CN with the new LOCATOR and ESP_INFO containing the SPI values is also required in the case there is an active connection between the MN and the CN. The

HIP UPDATE packet is signed but not encrypted so that the SPI values can be used by LMA to update the binding cache.

Figure 14 shows in detail the signalling flow for initialization.

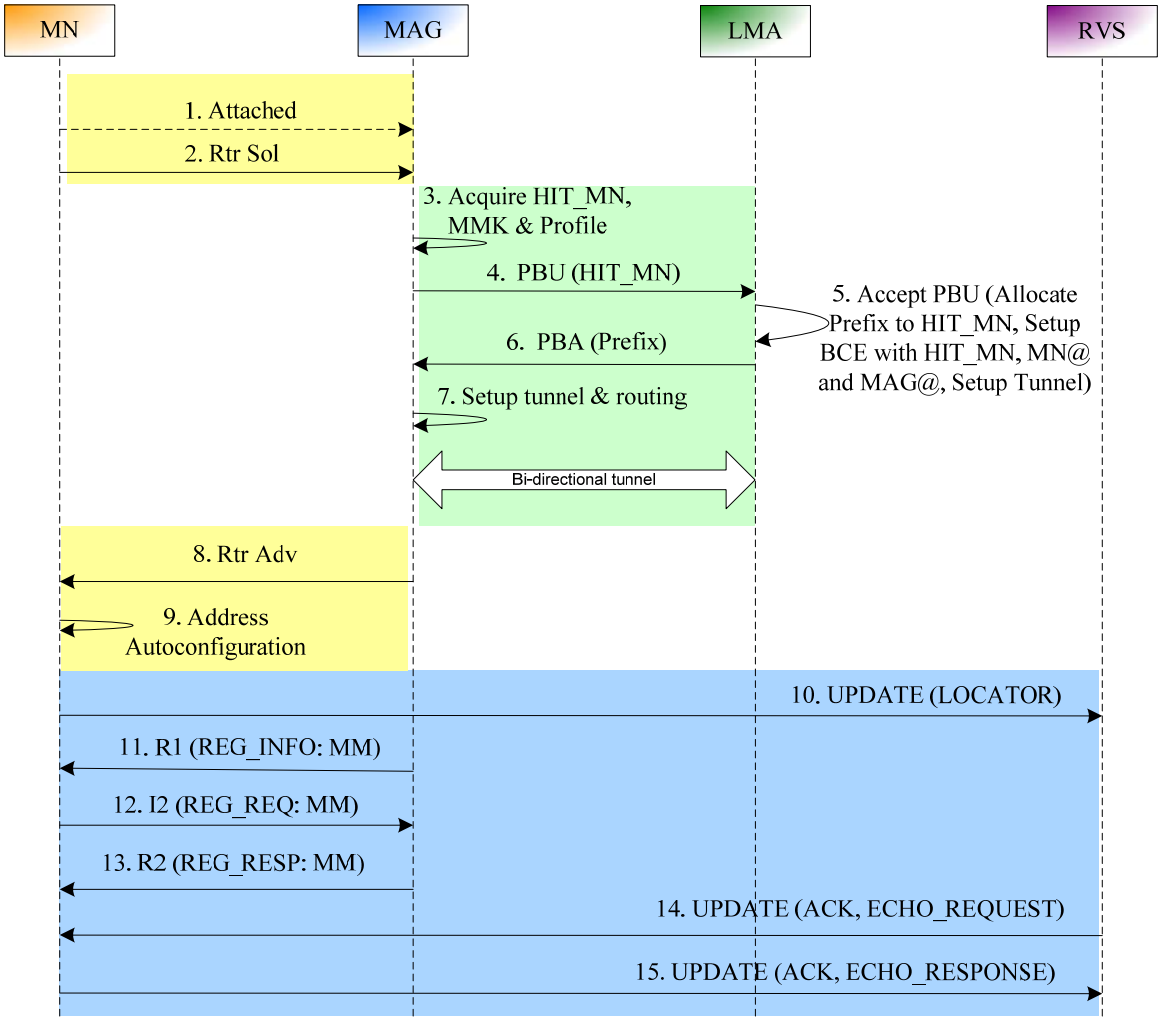

Figure 14. Inizialization

4.2 Communication setup

HIP Base Exchange is required before every HIP-based communication is established. When the CN wants to start communication with the MN, the CN will get the MN's RVS server from the DNS server. The CN starts the HIP BE with the MN via RVS. RVS forwards the HIP I1 packet directly to the MN. In this work it is not necessary to have a LRVS as the MN's IP address is always directing the BE through the LMA. I1 is routed by LMA to the correct MAG using the

information in the BCE as in the PMIPv6 architecture. The rest of the BE will operate via a similar process.
Inspecting the HIP BE, the LMA will record in the Binding Cache the mapping between the Security Parameters Index (SPI), CN's IP address, MN's IP address and the serving MAG. Table 2 shows an example of Binding Cache in LMA for a MN with multiple interfaces and an active connection with the CN.

HIT_MN	Prefix	IP@$_1$	MAG@$_1$	SPI$_1$	CN@
		IP@$_2$	MAG@$_2$		
		IP@$_3$	MAG@$_3$		

Table 2. Binding Cache in LMA

4.3 Intra-technology handover

The intra-technology handover is based on PMIPv6 procedure and it is described in Figure **15**.

After obtaining the initial address configuration in the Proxy Mobile IPv6 domain, if the mobile MN changes its point of attachment, the MAG on the previous link (pMAG) will detect the MN's detachment from the link. It will signal the LMA and will remove the binding and routing state for that MN. The LMA, upon receiving this request, will identify the corresponding mobility session for which the request was received, and accepts the request after which it waits for a certain amount of time to allow the MAG on the new link (nMAG) to update the binding. However, if it does not receive any Proxy Binding Update message within the given amount of time, it will delete the binding cache entry.

With the new attachment, the registration steps will start as in the initialization process.
The nMAG, upon detecting the MN on its access link, will signal the LMA to update the binding state as specified in the initialization phase. The update with the nMAG in the BCE is done by LMA based on the HIT_MN and MN's IP address. The LMA will send a PBA message with the prefix. After completion of the signaling, the nMAG will send the Router Advertisements containing the MN's home network prefix and this will ensure the MN will not detect any change with respect to the layer-3 attachment of its interface. The MN will not send any UPDATE messages to the RVS and CN as its IP address has not changed.

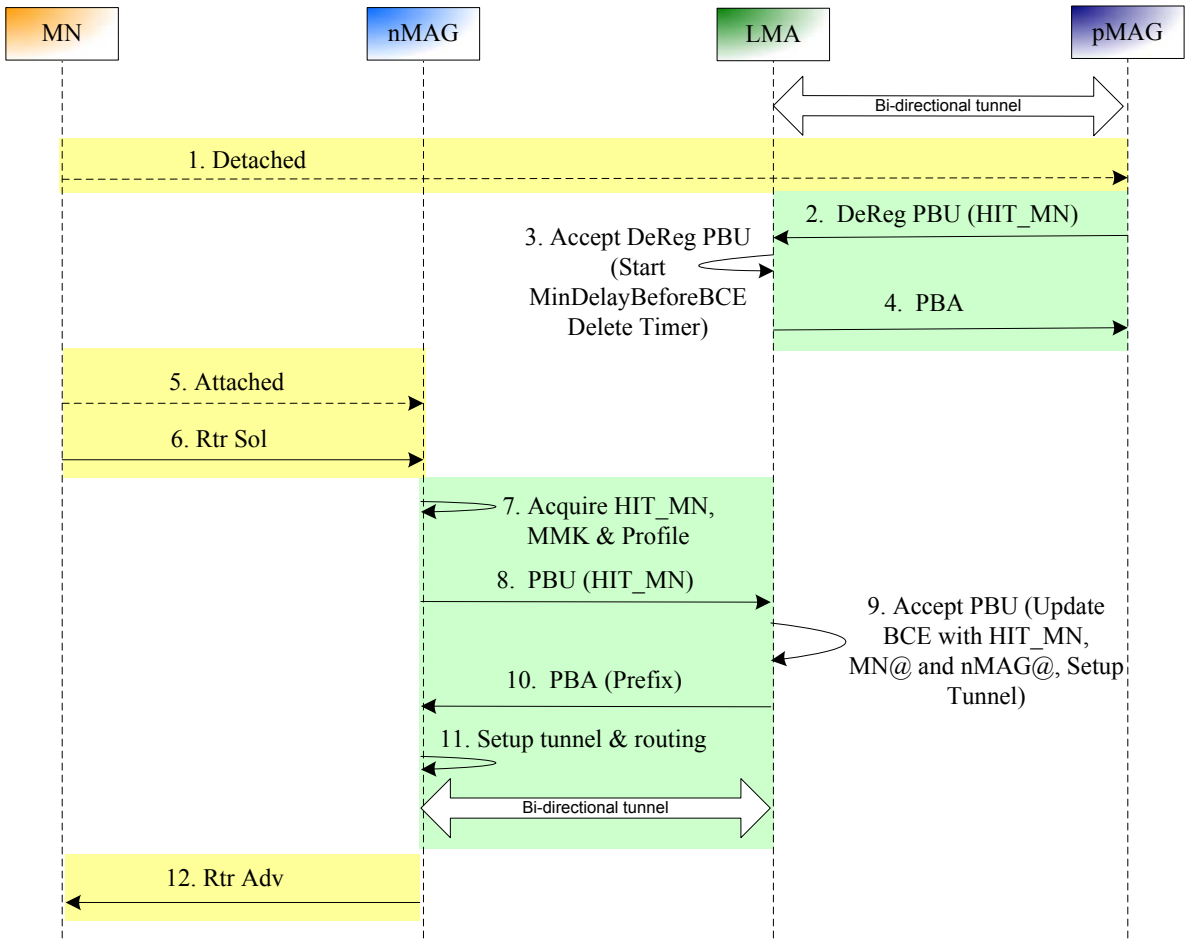

Figure 15. Intra-technology handover

4.4 Inter-technology handover

The inter-technology handover is based on the mobility features of HIP [13] in combination with micro-mobility features provided by PMIPv6.

The MN switches on its second interface and obtains the same prefix from the network (see initialization phase). The MN realizes it is still in the same domain, so it does not need to update the RVS, the network will manage the mobility issues.

Once the MN decides to start an inter-technology handover procedure with its CN, the MN will send to the CN an UPDATE message with the LOCATOR parameter containing the second interface's IP address. In the UPDATE message it is also present the ESP_INFO parameter containing the values of the old and new SPIs for the security association. In this case, the OLD

SPI and NEW SPI parameters both are set to the value of the preexisting incoming SPI; this ESP_INFO does not trigger a rekeying event.
The MN waits for this UPDATE to be acknowledged, and retransmits if necessary, as specified in the base specification. The UPDATE packet with the new IP address is intercepted by the serving MAG which will start the handover procedure. The packet is processed by the MAG and it is not forwarded to the CN.

On one side, the serving MAG is handling this UPDATE packet instead of the CN in the PMIPv6 domain and performs address verification by placing a nonce in the ECHO_REQUEST parameter of the UPDATE message sent back to the MN. It also includes an ESP_INFO parameter with the OLD SPI and NEW SPI parameters both set to the value of the preexisting incoming SPI, and sends this UPDATE (with piggybacked acknowledgment) to the MN at its new interface address. The MN recognizes the HIT_group and the signature_group in the message and accepts the reply. The MN completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO_RESPONSE. Once the serving MAG receives this ECHO_RESPONSE, it considers the new address to be verified and can put the address into full use.

On the other side, a Proxy Binding Update message with Handoff Indicator (HI) option set and the HI with value of 2 (handoff between two different interfaces of the mobile node) is sent by the serving MAG to LMA. It contains also the HIT_MN and the SPI. In the case of inter-technology handover, the LMA updates the information on the serving MAG in the Binding Cache Entry (BCE) based on HIT_MN and SPI, not MN's IP address. A Proxy Binding Acknowledge is sent by LMA to nMAG with the information of the previous interface's IP address in order to setup the routing table at nMAG. No UPDATE message is sent to the CN, the complete process take place only in PMIPv6 domain.

Table 3 shows an example of update in the BCE after an inter-technology handover.

HIT_MN	Prefix	IP@$_1$	MAG@$_3$	SPI$_1$	CN@
		IP@$_2$	MAG@$_2$		
		IP@$_3$	MAG@$_3$		

Table 3. Binding Cache in LMA after inter-technology handover

In the case the MN is multi-homed, it can have multiple SAs with different CNs. All the active connections with the corresponding SPIs are registered in the BCE of LMA.

Figure 16 illustrates the signaling flow.

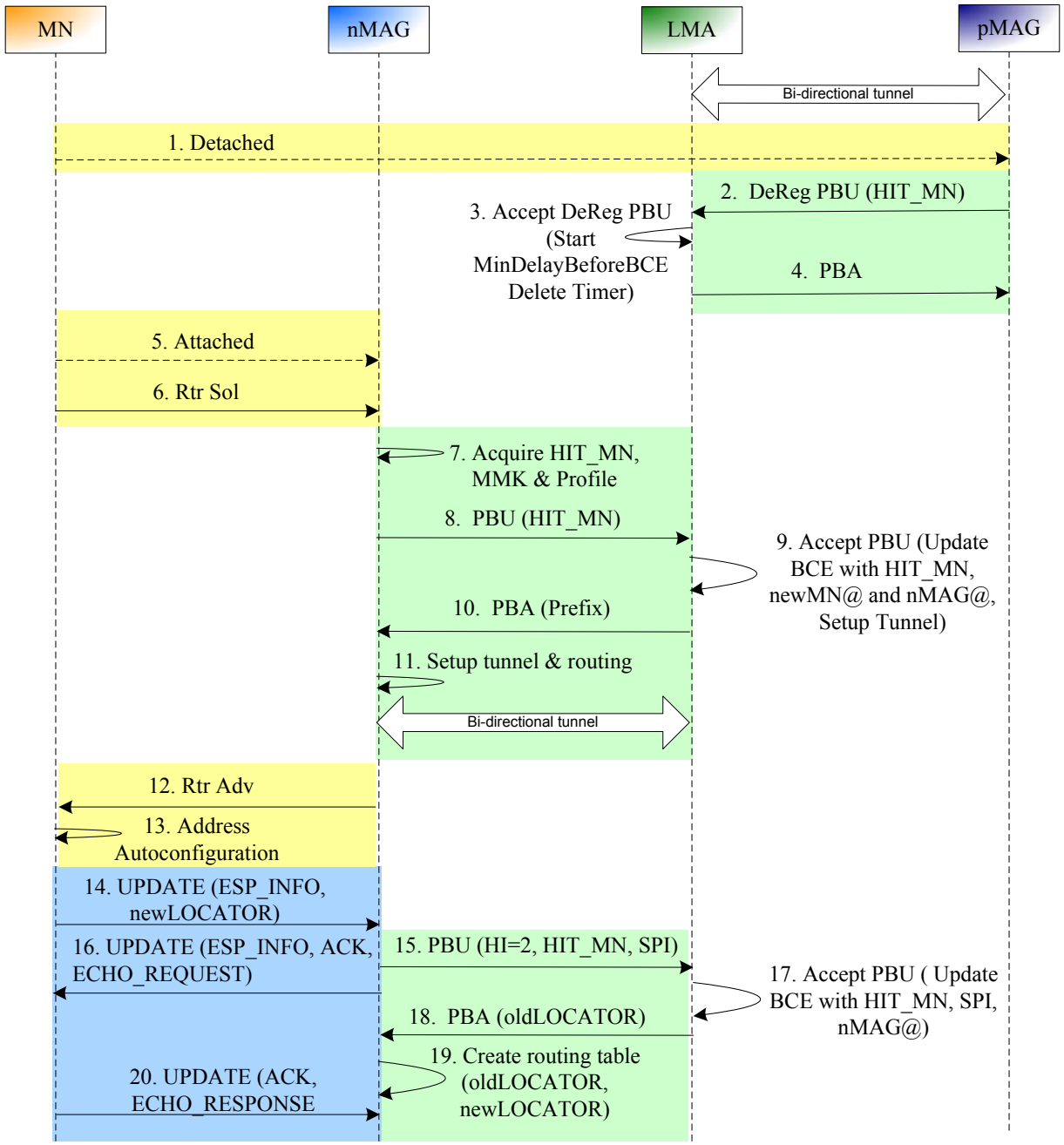

Figure 16. Inter-technology handover

The incoming packets from the CN are tunnelled by LMA to the serving MAG depending on the source and destination address information in the IP header. The serving MAG, thanks to the routing table, can send the packet to the MN that can route internally to the correct interface. For outgoing packets the CN can receive the traffic coming from a different interface of the MN as the SA contains the HIT_MN, not the MN's IP address.

CONCLUSIONS

Smooth, seamless and secure handover for mobile nodes in heterogeneous wireless IP networks is the target of future mobility management, especially for emergency management. Complete mobile management solutions involve not only the physical and data link layers, but also the network layer and above. Mobility management can be classified into two categories, macro-mobility management and micro-mobility management. The former handles the movement of a node between any two IP addresses and the latter focuses on the handover between different access points under the same domain.
Mobile IP is a widely discussed macro-mobility management protocol in the network layer, but Proxy MIPv6 is the new and most effective solution for micro-mobility management. HIP is a newly proposed protocol and has been shown to outperform Mobile IP in handover efficiency. Most of the proposed micro-mobility management solutions are Mobile IP-based. There are some HIP-based micro-mobility management solutions in recent publications, but so far they do not cover all aspects of micro-mobility management.

In this work, we have presented a complete HIP/PMIPv6-based mobility management solution, which combines micro-mobility features of PMIPv6 together with security, inter-technology handover and multi-homing properties of HIP. This solution can really improve mobility issues in the advanced satellite and wireless mesh system architecture [17] proposed for public safety communication. Mobile nodes at the disaster area can keep their connections on while moving under different mobile routers and switching from one access technology to another. The wireless mesh network is responsible of seamlessly managing the micro-mobility at the crisis site. Security is also provided thanks to HIP features, thus only authorized rescue agents can have access to the public safety communication system. Security associations are also maintained for communications between the disaster area and the headquarters, using IPSec protocol.

.

BIBLIOGRAPHY

[1] **I. F. Akyildiz, J. Xie, and S. Mohanty, "A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems'', IEEE Wireless Commun., vol. 11, no. 4, August 2004, pp. 16-28.**

[2] **G. Iapichino and C. Bonnet, "IPv6 mobility and ad hoc network mobility overview report", Research Report RR-08-217, March 2008.**

[3] **C. Perkins, "Mobile IP, Design Principles and Practices", Addison-Wesley, 1998.**

[4] **C. Perkins, "IP Mobility Support for IPv4", IETF RFC 3344, Aug. 2002.**

[5] **D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2004.**

[6] **H. Soliman, C. Castelluccia, K. El Malki and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management", IETF RFC 4140, August 2005.**

[7] **S. Gundavelli et al., "Proxy Mobile IPv6", IETF RFC 5213, August 2008.**

[8] **R. Koodli, "Fast Handovers for Mobile IPv6", IETF RFC 4068, July 2005.**

[9] **H. Faithi and R. Prasad, "Mobility Management for VoIP in 3G Systems: Evaluation of Low-Latency Handoff Schemes", IEEE Wireless Commun., vol. 12, no. 2, April 2005, pp. 96-104.**

[10] **K. Kong, W. Lee, Y. Han, and M. Shin, "Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol", Proc. IEEE ICC 2008, May 2008, pp. 5838-5843.**

[11] **R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol", IETF RFC 5201, April 2008.**

[12] **E. Rescorla, "Diffie-Hellman Key Agreement Method", IETF RFC 2631, June 1999.**

[13] **P. Nikander, T. Henderson, C. Vogt, and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", IETF RFC 5206, April 2008.**

[14] **P. Jokela et al., "Handover Performance with HIP and MIPv6", IEEE 1st International Symposium on Wireless Communication Systems, September 2004, pp. 324-28.**

[15] **S. Novaczki, L. Bokor, and S. Imre, "Micromobility Support in HIP: survey and extension of Host Identity Protocol", Proc. IEEE MELECON 2006, May 2006, pp. 651-54.**

[16] **J. Y. H. So, and J. Wang, "Micro-HIP: a HIP-based micro-mobility solution", Proc. IEEE ICC Workshop 2008, May 2008, pp. 430-35.**

[17] **G. Iapichino, C. Bonnet, O. del Rio Herrero, C. Baudoin, and I. Buret, "Advanced Hybrid Satellite and Terrestrial System Architecture for Emergency Mobile Communications", Proc. 26th AIAA International Communications Satellite Systems Conference, June 2008.**

ACRONYMS

AAA	Authentication, Authorization, Accounting
AR	Access Router
BCE	Binding Cache Entry
BE	Base Exchange
CN	Correspondent Node
CoA	Care-of-Address
DH	Diffie-Hellman
DoS	Denial-of-Service
ESP	Encapsulating Security Payload
FBU	Fast Binding Update
FMIPv6	Fast Mobile IPv6
HA	Home Agent
HI	Host Identity
HIP	Host Identity Protocol
HIT	Host Identity Tag
HMIPv6	Hierarchical Mobile IPv6
HoA	Home Address
LCoA	Local Care-of-Address
LMA	Local Mobility Anchor
LRVS	Local Rendezvous Server
MAG	Mobile Access Gateway
MAP	Mesh Access Point
MIPv6	Mobile IPv6
MMK	Mobility Management Key
MN	Mobile Node
MRP	Mobile Routing Point
NAR	New Access Router
NCoA	New Care-of-Address
PAR	Previous Access Router
PBA	Proxy Binding Acknowledge
PBU	Proxy Binding Update
PMIPv6	Proxy Mobile IPv6
RCoA	Regional Care-of Address
SA	Security Association
SPI	Security Parameter Index
UNA	Unsolicited Neighbor Advertisement