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

Research Report RR-09-237

# Ad hoc network connection continuity for security applications report

November 10th, 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 Host Identity Protocol (HIP) and the Proxy Mobile IPv6 (PMIPv6) in order to have a secure global and localized mobility management scheme for service and connection continuity applicable to any kind of access technology used by rescue teams. Our contribution is two-folds. First, it represents an efficient micro-mobility solution for HIP that does not introduce any IP stack complexity to standard HIP Mobile Nodes (MNs). Second, it gives support to multiple interfaced MNs in PMIPv6, resolving the problems of inter-technology handover and multihoming thanks to the identifier/locator split of HIP used as a virtual interface.

Moreover, this document presents a novel mobility architecture for future Internet and Next Generation Public Safety Networks, derived from HIP and PMIPv6, which assures the principle of ad hoc network connection continuity. The proposed architecture not only preserves the best of both protocols, such as the idea of separating a host's identity from its present topological location in the Internet and the mechanism of network-based mobility management without host involvements, but it combines them in an efficient way. In our architecture the host identifier is used as a virtual interface for multihomed terminals and the group identifier to identify nodes in an ad-hoc network, while the locator is configured such as it provides location privacy and avoids the use of local NATs. The result is a mobility architecture which addresses the requirements of future Internet and operators, as well as Next Generation Public Safety Networks, like addressing, name resolution, security, location privacy, mobility, multihoming, ad-hoc networking, routing and traffic engineering. Reduced network and terminals' complexity as well as signaling overhead are pointed out.

## *1.2 Structure of the Document*

The document starts, in section 2, first describing HIP and the related work on its micro-mobility, and then PMIPv6 with the related work on IP session continuity across different technologies.

Section 3 presents our proposed combination of HIP and PMIPv6, combining the micro-mobility scheme of PMIPv6 and the macro-mobility and multi-homing aspects of HIP. The initialization phase together with intra and inter-technology handover phases are provided.

Section 4 presents a detailed description of our proposed mobility architecture for future Internet and Next Generation Public Safety Networks.

Section 5 describes and compares, with our architecture, related work and relevant proposals done by IETF Working Groups (WGs) and researches with the aim to solve similar problems. Finally, conclusions are provided.

# 2 RELATED WORK

In the early days of Internet, hosts were big and clumsy and remained in fixed locations. This led to the current Internet architecture in which the IP address is used for describing the topological location of the host, and at the same time, to identify the host. This feature is not efficient in handling mobility, so different schemes have been proposed to enhance current network model's support to mobility.

Mobile IPv6 (MIPv6) [1] is the most popular scheme. It assigns a new IP address, called Care-of-Address (CoA), to the Mobile Node (MN) each time it changes its point of attachment to the Internet. A binding between the Home Address (HoA) and the CoA is used by the MN for updating its Home Agent (HA) about its new IP address to maintain its reachability. MIPv6 is just by-passing the main problem. A new network architecture that could separate the identifier and the locator role of the traditional IP addresses is needed for Next Generation Public Safety Networks.

Host Identity Protocol (HIP) [2] is resolving this problem by introducing a Host Identifier (HI) for each MN and a new layer between the network and the transport layer. In HIP, the transport layer connections are bound to the Host Identity Tag (HIT), a 128-bit hash of the HI, not anymore to the IP address. HIP represents a new secure Global Mobility Management (GMM) protocol that overcomes MIPv6, providing security and inherent multihoming features to heterogeneous mobile networks with multihomed hosts [3], and having light impact on mobile terminals [4]. Anyway, an efficient micro-mobility solution for HIP is still missing. Current solutions take inspiration from micro-mobility schemes for MIPv6 [5] [6]. Having in mind such a different Internet architecture, they do not represent an optimized solution for HIP.

As specified in [7], the fact that future wireless IP nodes may support a GMM protocol that is not MIPv6, such as HIP, has suggested a new network-based paradigm for Localized Mobility Management (LMM), called Proxy Mobile IPv6 (PMIPv6) [8], which does not require any additional effort to implement, deploy, or in some cases, even specify in a non-Mobile IPv6 mobile environment. PMIPv6 is based on the concept that the network provides always the same Home Network Prefix (HNP) to the MN independently of its point of attachment to the PMIPv6 domain. Experimental protocols developed in the past for LMM, namely Fast-Handovers for Mobile IPv6 (FMIPv6) [9] and Hierarchical Mobile IPv6 (HMIPv6) [10], are host-based solutions that require host involvement at the IP layer similar to, or in addition to, that required by MIPv6 for GMM.

PMIPv6 can be applied to any GMM protocol and reduces host stack software complexity, expanding the range of MNs that could be accommodated. So far, PMIPv6 has been applied only to MIPv6 [11], even if its main added value is to provide micro-mobility to unmodified MNs, i.e. non MIPv6 devices. Moreover, at the moment, PMIPv6 is also lacking of specific functionalities for IP session continuity across different network interfaces for multihomed MNs.

In this section, we shortly overview HIP and existing micro-mobility solutions for it, inspired from host-based MIPv6 localized mobility management protocols, and PMIPv6 with on-going research for inter-technology handover and multiple interfaces support.

## *2.1 HIP and its current micro-mobility solutions*

HIP defines a four way handshake mechanism (I1, R1, I2, R2) called HIP Base Exchange (BE) to establish a HIP end-to-end connection between MNs. During BE, MNs create a session key through the Diffie-Hellman scheme, used then in the IPSec Encapsulating Security Payload (ESP) Security Association (SA). With HIP the SAs are bound to HITs, not to IP addresses as the current IPSec defines. Therefore the change of IP address is transparent to applications and SAs remain valid. When a host changes its address during a connection, it can send a HIP UPDATE packet to any HIP enabled correspondent peer. This packet contains the current ESP sequence number and Security Parameter Index (SPI) to provide denial-of-service and replay protection, and is authenticated with a HIP signature [12]. Mobility is handled via secure DNS updates just as in end-to-end mobility, but, to avoid frequent DNS updates, HIP introduces a new entity called Rendezvous Server (RVS). The DNS stores the HIT of the MN together with a stable locator, thus the RVS' IP address, and the RVS is in charge of keeping updated information about MN's current locator. The RVS replaces the role of HA in MIPv6.

In [5], Novaczki et al. propose a micro-mobility scheme for HIP similar to HMIPv6. They introduce a new entity, the Local Rendezvous Server (LRVS), which acts as the Mobile Anchor Point (MAP) for HMIPv6. The MN needs to register itself in the RVS and in the LRVS. When the MN moves inside the domain, it needs to notify the LRVS of its new address and not anymore the CN. The LRVS is in charge of redirecting all HIP-based communication streams into its new address. As a drawback, this scheme is affected by the high number of messages needed to update the LRVS for each MN's movement and by the fact that the LRVS has to be a Security Parameter Index multiplexed Network Address Translator (SPINAT) device to allow the overlay routing based on SPI.

In [6], 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 type of security scheme can be adopted. As in the LRVS of Novaczki's scheme, a modified SPINAT device has to be implemented in the mHIP agents. In the same way, the MN registers itself in the RVS and in the mHIP gateway, with the difference that the MN registers itself in the RVS with the HIT of the mHIP gateway. This behavior breaks the macro-mobility support of HIP, as changing domain for the MN will imply changing HIT, thus breaking previous sessions.

## *2.2 PMIPv6 and inter-technology handover with multihoming*

In PMIPv6 the mobility entities, i.e. Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG), in the network are responsible for tracking the movements of the MN and initiating the required mobility signaling on its behalf. The LMA is the HA for the MN in PMIPv6 domain, maintaining the MN's binding state and being the topological anchor point for the MN's HNP. The MAG is the entity responsible for detecting MN's movements to and from the access link and initiating mobility signaling with the MN's LMA. This mechanism provides the MN with an IPv6 address that is routable outside the PMIPv6 domain and managed by the LMA inside the domain. The configured IPv6 address remains unchanged for every intra-technology handover.

Ensuring session continuity to a MN equipped with multiple radio interfaces during inter-technology handoff is an open issue for PMIPv6. The precondition for a MN to move IP sessions from one interface to another is that it is able to configure the same IP address on both interfaces, using the same interface identifier and the same HNP in order to create the same IP address. The fact that there are link layers which do not allow for MAC address negotiation and where the MAC address assigned to the device is authenticated by the certificate and thus cannot be changed, i.e. IEEE 802.16, leads to consider specific functionalities for this issue.

In [13]-[14] the proposed solution is based on Virtual Interface (VI) configuration, that hides the multiple physical interfaces involved in the handover. The address configured by the MN is assigned to the VI, which is the only one visible to the applications. This method is efficient when only one interface is active at a time, as the MN maps the VI to the active physical interface. When a handover happens, the MN maps the VI to the new active physical interface. This solution represents the most reasonable one, but it does not cover the case in which the MN is multihomed and uses several interfaces at the same time, as the basic rules of IP networking impose that the same IP address cannot be assigned to more than one interface. Moreover, as highlighted in [15], the MN has to be enhanced with PMIPv6 specific capabilities to be able to notify its willingness of moving IP sessions across interfaces and it has to be aware about the PMIPv6 service availability. Extension to Router Advertisement (RA) and Router Solicitation (RS) messages, e.g. new flags, have been proposed in [16], but they are not sufficient and still an explicit notification from the MN about which IP session coming from which interface should be moved to the new interface is missing.

# 3 PROPOSED COMBINATION OF HIP AND PMIPV6

Our scheme represents a novel micro-mobility management solution for HIP and, at the same time, an enhancement for PMIPv6 to support MNs roaming between different network interfaces and multihoming. The architecture is illustrated in Fig. 1.

Before starting to analyze each mobility management phase, some assumptions need to be done for the proposed scheme. As in So's scheme, we suppose that all the entities in the PMIPv6 domain (LMA and MAGs), besides their own HIT, share 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 Mobility Management Key (MMK). The MN can verify the signature of the group.

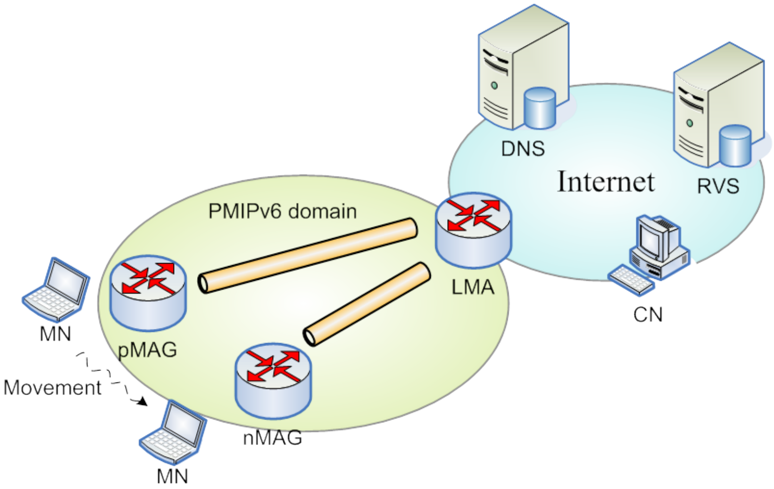

**Figure 1. Proposed Global and Localized Mobility Management Architecture**

## *3.1 Initialization*

We suppose the MN is already registered in the RVS and it enters a PMIPv6 domain. The complete process is illustrated in Fig. 2 and described hereafter.

The first part of the initialization phase is based on PMIPv6 prefix allocation [8]. As soon as a MN attaches to a PMIPv6 domain, it will be detected by the serving MAG on the access link. In particular, the link local address in the RS message sent by the MN is used by the MAG to obtain the interface identifier (interface_ID), i.e. the MAC address. A request is sent by the MAG to the Authentication, Authorization and Accounting (AAA) server or to the Local Policy Device with the interface_ID of the MN, in order to receive the authorization to provide the network-based mobility management service to the MN together with the MN identifier (HIT_MN) and profile, and the MMK.

The PMIPv6 procedure starts. The MAG sends a Proxy Binding Update (PBU) message to the LMA containing the HIT_MN, the interface_ID and the Access Technology Type (ATT). The LMA replies with a Proxy Binding Acknowledgement (PBA) message including the MN's HNP, unique for that specific HIT_MN. A Binding Cache Entry (BCE) is created by the LMA in which it registers the HIT_MN, the HNP, the interface_ID, the ATT, the new MN's IP address created using HNP and interface_ID and the MAG's IP address. LMA and MAG set up their endpoints for creating a bi-directional tunnel between them.

The MAG sends RA messages to the MN on the access link advertising the MN's HNP as the hosted on-link prefix. The MN can configure an IP address for its interface that will never change as long it remains inside the PMIPv6 domain.

Once the environment for micro-mobility management is created, the macro-mobility management procedure will start as in HIP. The new IP address needs to be registered by the MN in the RVS. It is done following the RVS update procedure as defined in [17]. An UPDATE message containing the new LOCATOR is created by the MN and sent to the RVS. Once this message reaches the MAG, it will play the role of service provider for the micro-mobility service offered by PMIPv6 as in [15]. In order to establish a trusted relationship between the MN and the MAG, we use HIP service provision and discovery mechanism as specified in [18]. A SERVICE_OFFER_UNSIGNED (SOU) parameter is added by the MAG to the UPDATE ACK message sent by the RVS. This parameter is not covered by signature in the HIP control packet, so it can be added by HIP-aware middleboxes. The SOU contains three parts: SERVICE_PROPERTIES (SP) for describing the type of service, SERVICE_ID (SID) to identify a specific service and SERVICE_DESCRIPTION (SD) for providing specific service-related information, in our case the MMK and HIT_domain. The MN, that accepts the micro-mobility service, replies with a SERVICE_ACK parameter in the next UPDATE message to RVS. At this point the MMK and HIT_domain will be used by the MN to authenticate the service provider. In alternative to this solution, the PMIPv6 mobility management service can be notified by the MAG in the RA by setting a specific flag, as suggested in [15].

In the case there are on-going sessions with Correspondent Nodes (CNs), the MN needs to send an UPDATE message to each CN with the new LOCATOR and ESP_INFO parameter containing the SPI value assigned to that specific session. As the HIP UPDATE packets are signed but not encrypted, they can be used by LMA for activating the status of the MN's interface adding the SPI value and CN's IP address to the interface_ID in the BCE. This aspect is explained in details in the next paragraph.

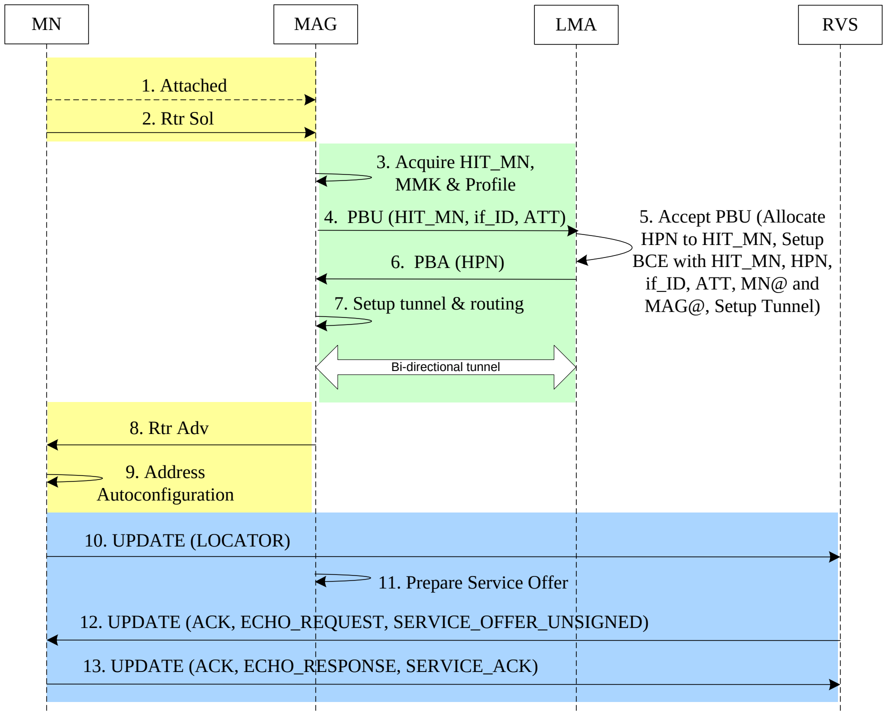
MN
MAG
LMA
RVS
1. Attached
2. Rtr Sol
3. Acquire HIT_MN, MMK & Profile
4. PBU (HIT_MN, if_ID, ATT)
5. Accept PBU (Allocate HPN to HIT_MN, Setup BCE with HIT_MN, HPN, if_ID, ATT, MN@ and MAG@, Setup Tunnel)
6. PBA (HPN)
7. Setup tunnel & routing
Bi-directional tunnel
8. Rtr Adv
9. Address Autoconfiguration
10. UPDATE (LOCATOR)
11. Prepare Service Offer
12. UPDATE (ACK, ECHO_REQUEST, SERVICE_OFFER_UNSIGNED)
13. UPDATE (ACK, ECHO_RESPONSE, SERVICE_ACK)

**Figure 2. Inizialization**

## 3.2 *Communication setup*

HIP Base Exchange [2] is required before every HIP-based communication is established. A CN that wants to reach a MN needs to contact the DNS server to get, first, the RVS' IP address for that MN. Then the CN can start the HIP BE with the MN via RVS. The first packet, a HIP I1 message, is forwarded by the RVS directly to the recorded locator of the MN. The peculiarity of PMIPv6 is that the IP addresses generated through the PMIPv6 prefixes are routable outside the PMIPv6 network and always point to the LMA. This feature allows us to avoid using a LRVS in the local network as in [5] and [6]. As soon as I1 reaches the LMA, it is tunneled to the serving MAG and then delivered to the MN. The rest of the BE operates in the standard way, the MN and the CN exchange R1, I2 and R2 packets directly without passing through the RVS.

As HIP BE packets, but also HIP UPDATE packets as seen before, are not encrypted, they can be used by the LMA for updating the BCE. Thus, only HIP control packets are inspected, not data packets. An interface of a MN registered in a "preliminary" (P) status (no active connections) can become "active" (A) as in [19] adding the SPI and CN's IP address information carried in HIP BE or UPDATE packets. Table I represents an example of BCE at LMA for a MN with two interfaces. When BE or UPDATE processes have finished, there is not anymore HIP overhead in data packets. LMA is not a SPINAT device in our architecture, so routing at LMA for tunneling packets to the correct MAG is done based on the IP addresses of MN and CN.

TABLE I. EXAMPLE OF BINDING CACHE ENTRY PER MN AT LMA

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| HIT_MN | HPN | If_ID$_1$ | ATT$_1$ | @$_1$ | MAG$_1$ | A | CN$_1$ | SPI$_1$ |
|  |  | If_ID$_2$ | ATT$_2$ | @$_2$ | MAG$_2$ | Preliminary |  |  |

**Table 1. Example of Binding Cache Entry per MN at LMA**

## 3.3 *Intra-technology handover*

The intra-technology handover phase represents the most important contribution of PMIPv6 to micro-mobility management for HIP. As the MN's locator does not change, the process is completely transparent to HIP. This phase is based on PMIPv6 procedure [8] and it is illustrated in Fig. 3. When the MN changes its point of attachment, the MAG on the previous link (pMAG) detects the MN's detachment from the link. It sends to the LMA a Deregistration PBU with the HIT_MN, interface_ID and ATT. The LMA, upon receiving this request, identifies the corresponding MN and interface for which the request was received. The LMA accepts the request and then 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 a given amount of time, the LMA deletes the interface from the MN entry in the BCE.

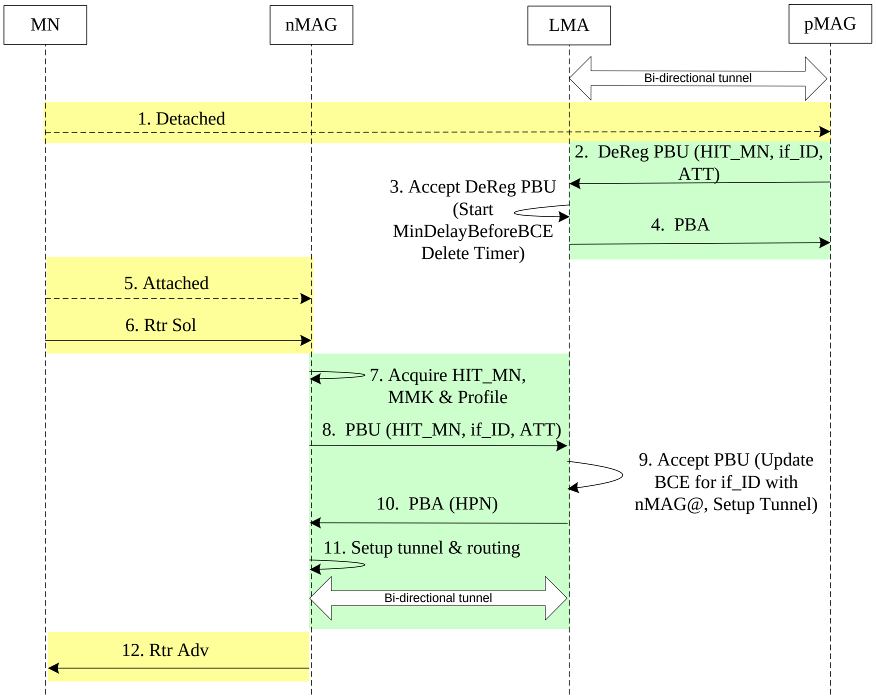
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE for if_ID with nMAG@, Setup Tunnel)
10. PBA (HPN)
11. Setup tunnel & routing
Bi-directional tunnel
12. Rtr Adv

**Figure 3. Intra-technology handover**

With the new attachment, the PMIPv6 prefix allocation procedure starts, as in the initialization process, and terminates with the RA message sent by the nMAG to the MN containing the HNP. The LMA updates the BCE for that interface with the nMAG's IP address. The MN does not detect any change with respect to the layer-3 attachment of its interface, the IP address has not changed. There is no need for UPDATE messages to RVS and CN.

## *3.4 Inter-technology handover*

The multihoming support in PMIPv6 [8] is simply simultaneous connection/attachment support for a multiple interfaced MN. However, there are many scenarios in which the simultaneous "usage" of multiple interfaces for a MN and the possibility of moving a single IP flow from a certain access technology to another one require some enhancement/modification to the current PMIPv6 base protocol. [20] explores the merits and the tradeoffs of the basic principle of two PMIPv6 multihoming models such as the same unique prefix across all the interfaces and per interface unique prefix. Our proposal is based on unique HNP for all interfaces of a MN and on the mobility features of HIP [12] in combination with micro-mobility features provided by PMIPv6. Advantages of this choice are described hereafter.

To illustrate this phase we suppose the MN has an ongoing IP session with a CN and wants to move it to its second interface without disconnecting the first one. When the MN switches on its second interface to configure the IP address, it obtains the same HNP from the network, as the HNP is assigned to MN's identifier, reducing operation complexity at LMA. In this way the MN realizes it is still in the same domain and no UPDATE messages are sent to the RVS, due to the fact that anyway all the IP addresses configured in the PMIPv6 are pointing to the LMA. In order to explicitly notify its willingness to move a particular IP session, the MN has to send to the CN an UPDATE message with the new 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 SA. 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 UPDATE packet with the new IP address is intercepted and processed by the nMAG and it is not forwarded to the CN as illustrated in Fig. 4.

On one side, the nMAG is handling the UPDATE packet on behalf of the CN, performing address verification by placing a nonce in the ECHO_REQUEST parameter of the UPDATE message sent back to the MN. The MN recognizes the HIT_domain and the MMK in the message and accepts the reply. It completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO_RESPONSE.

On the other side, thanks to the information carried in the UPDATE message, the nMAG knows that it is an inter-technology handover and can send to the LMA a PBU message containing Handoff Indicator option set to the value of 2 (handoff between two different interfaces of the MN), the HIT_MN and the SPI. Based on these parameters the LMA updates the corresponding BCE substituting the pMAG's IP address with the nMAG's one. A PBA is sent by LMA to nMAG.

As highlighted in [20], when applying the same HNP for all interfaces of a MN, there are three different methods for routing using the cache at LMA. We have chosen the address based cache method, thus LMA tunnels the incoming packets from the CN to the correct MAG depending on the IP source and destination addresses in the IP header. With this approach the willingness of the MN of using the new locator and thus the new access technology is respected even if the CN has not been updated and keeps using the previous locator. When packets reach the MAG, they are routed based on the HNP. Moreover, the MN can be configured to accept packets to be received by any interface as long as the destination address matches the HNP regardless of the actual address configured for that interface. For outgoing packets, the CN can still receive them even if they are coming from a different interface of the MN due to the fact that the SA takes into account the MN's identifier and not its locator.

The HIP identifier/locator split principle is based on the same basic idea of the virtual interface (IP session continuity is assured by the fact that applications are linked to the identifier or to the VI, not to the current IP address), but our proposal represents a more complete solution as it can be applied to multihomed MNs using multiple active interfaces.

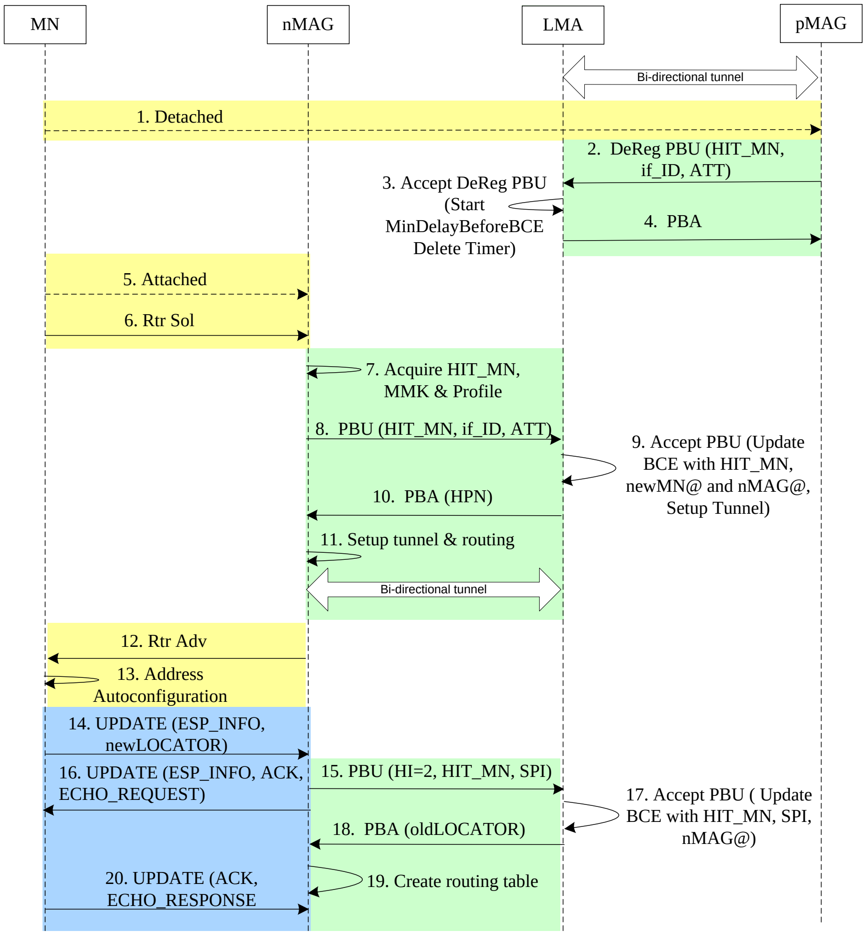
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE with HIT_MN, newMN@ and nMAG@, Setup Tunnel)
10. PBA (HPN)
11. Setup tunnel & routing
Bi-directional tunnel
12. Rtr Adv
13. Address Autoconfiguration
14. UPDATE (ESP_INFO, newLOCATOR)
16. UPDATE (ESP_INFO, ACK, ECHO_REQUEST)
15. PBU (HI=2, HIT_MN, SPI)
17. Accept PBU ( Update BCE with HIT_MN, SPI, nMAG@)
18. PBA (oldLOCATOR)
20. UPDATE (ACK, ECHO_RESPONSE
19. Create routing table

**Figure 4. Inter-technology handover**

The multihoming features of our proposed scheme can be summarized as follows. A comparison with the MobiSplit architecture [21], which separates mobility management and multihoming at global and local levels using MIPv6 and NetLMM, can help to better explain multihoming in our scheme.  At global level, HIP-PMIPv6 scheme is similar to MobiSplit approach, but instead of using multiple CoAs, one per domain, associated to the same HoA and registered in the HA, in our scheme multiple locators, one per PMIPv6 domain, are associated to the identifier and registered in the RVS. At local level, as in MobiSplit, the external entities to the PMIPv6 domain (RVS, CNs) do not distinguish the situation in which the MN is using one or more interfaces. The MN registers only one locator per PMIPv6 domain. The difference with MobiSplit consists on the fact that the MN is not forced to configure the same locator on each of its active terminal interfaces. As the SAs are linked to the MN’s identifier, CNs can receive and process packets having a different source address.

# 4 HIP AND PMIPV6 BASED MOBILITY ARCHITECTURE

The proposed combination of HIP and PMIPv6 [22] has lead to the design of a mobility architecture for future Internet and for Next Generation Networks, based mainly on the two principle ideas behind these protocols. This design is directly applicable to Next Generation Public Safety Networks.

The first idea is the concept of *host identity layer* located in the middle of network and transport layers. This layer provides unique cryptographic identifiers for hosts, called *host identifiers*, which are independent of the host's current location and network address.

The second idea is to create a *locator*, which defines the topological location of a host in a way that it is routable in the Internet, but has a specific scheme for routing in the local domain to which the host is attached.

From these two basic ideas we have defined a unique architecture where each host has:

- an identifier which uniquely identify the host and which is created as the public key of a public/private key pair, bringing built-in security support;
- one or several locators, depending on the fact of having multiple interfaces and being multihomed; locators are used for routing, but they have different topological semantics depending on the network considered, allowing inherent location privacy.

The result is an architecture which has the advantages of HIP and PMIPv6 protocols, such as on one side security, global mobility, multihoming and on the other side local mobility and location privacy, together with an efficient and dynamic mobility and multihoming scheme at local and global level.

The architecture is designed keeping in mind the requirements of Internet and operators in the future. Access network operators should not depend on functions of an external operator to provide their own connectivity and mobility service, while home operators should focus on customer support and rely on multiple access operators to provide their users with efficient local mobility management. For this reason we split the design in two parts:

- the core network in which home operators with their providers are located;
- the edge network where Local Mobility Domains (LMDs) are located. A LMD is associated with an Access Network Provider (ANP) and one or more Wireless Access Networks (WANs), having same or different access technologies.

The core network has multiple connections with the edge network, which are managed by four basic components:

- the Domain Name Server (DNS), which has the functionality of resolving Fully-Qualified Domain Names (FQDNs) with the corresponding host identifiers and locators;
- the Rendezvous Server (RVS) [17], which is the entity registering the locators associated with a host identifier;
- the Local Mobility Anchor (LMA), which represents the access point to the LMD and the topological anchor point for hosts in the LMD;

- the Mobility Access Gateway (MAG), which is the access router for the WAN that manages the mobility-related signaling for the MNs attached to its access link.

The overall architecture is illustrated in Fig. 5.

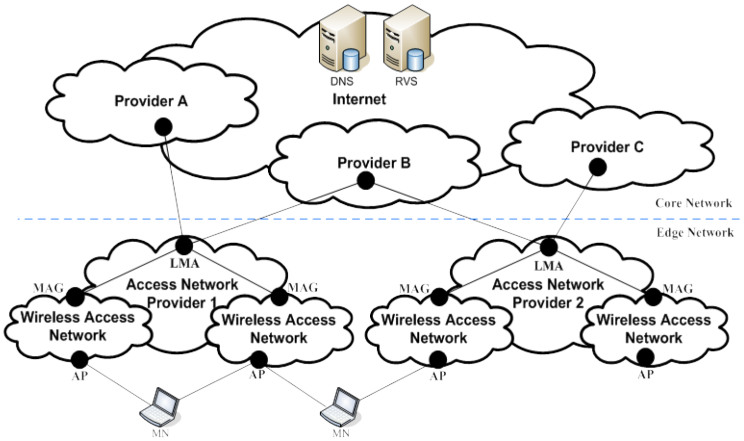

**Figure 5. Mobility architecture**

## *4.1 Addressing Scheme*

The IPv6 address (i.e. the locator) configured by MN in the mobility architecture is obtained through the PMIPv6 mechanism. When a MN attaches to a PMIPv6 domain (a LMD in this architecture), the MAG on that access link performs an access authentication procedure with a policy server sending the MN's identifier. The MAG receives the MN's profile, which contains the Home Network Prefix (HNP), the LMA address and other related configuration parameters. Then, the MAG sends to the LMA a Proxy Binding Update (PBU) message on behalf of the MN including the MN's identifier, its HNP and the used interface's MAC address. Upon accepting the message, the LMA replies with a Proxy Binding Acknowledgement (PBA) message, and it creates a Binding Cache Entry (BCE) with MN's identifier, its HNP, the locator (created from the HNP and the MAC address) and the MAG's address. Then, the MAG and the LMA create an IP-in-IP bidirectional tunnel for routing MN's traffic. As last step, the MAG sends a unicasted Router Advertisement (RA) message to the MN advertising the HNP 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 HNP that it can use while moving in the PMIPv6 domain.

## *4.2 Name Resolution*

The name resolution procedure begins with a FQDN, which nodes resolve via the DNS. The DNS returns the identifier of the MN and the locator of its RVS. With these two information, communication between peers can start. The first Base Exchange (BE) message (I1) sent by the Correspondent Node (CN) passes through the RVS which redirects it to the MN's locator. Once the MN receives the packet, it can reply to the CN directly providing its locator. The rest of BE (R1, I2, R2) for establishing the Security Associations (SAs) can occur through direct communication between peers.

## *4.3 Security*

The cryptographic nature of the host identifiers is the security cornerstone of HIP architecture as well as of our architecture. Each end-point generates exactly one public key pair. The public key of the key pair functions as the host identifier. The end-point keeps the corresponding private key secret and does not disclose it to anybody. The use of the public key as the name makes it possible to directly check that a party is actually entitled to use the name. A simple public key authentication protocol, such as the Diffie-Hellman scheme included in the HIP BE, is sufficient for that. This is accomplished with a four-way handshake, consisting of messages I1, R1, I2 and R2. After these exchange messages, both communicating hosts know that at the other end-point there indeed is an entity that possesses the private key that corresponds to its host identifier. Additionally, the exchange creates a pair of IPSec Encapsulated Security Payload (ESP) SAs, one in each direction. The hosts use the ESP SAs to protect the integrity of the packets flowing between them.

## *4.4 Location Privacy*

Standard HIP architecture does not provide location privacy as the locator information contained in the BE messages are not encrypted and can be disclosed by third parties. Moreover, there are scenarios in which even the correspondent peer should not be aware of the exact location of its peer. In the proposed mobility architecture, even if the locator is disclosed by peers or on-lookers, it is configured in a way that it always points to the LMA of the LMD where the MN is located, but does not reveal the exact position of the MN. Only the LMA is able to locate the MN and to route packets to it. In particular, the BCE at LMA contains entries for each MN attached to the LMD with the corresponding serving MAG.

## *4.5 Mobility*

The global and local mobility scheme of our architecture is a combination of HIP and PMIPv6 schemes.

As regards global mobility, when a MN moves from a LMD to another one, it obtains through the PMIPv6 mechanism a new HNP (HNP2), which it is used to create a new locator (Locator 2). As in standard HIP, the MN needs to update the RVS with its new locator as in Fig. 6.

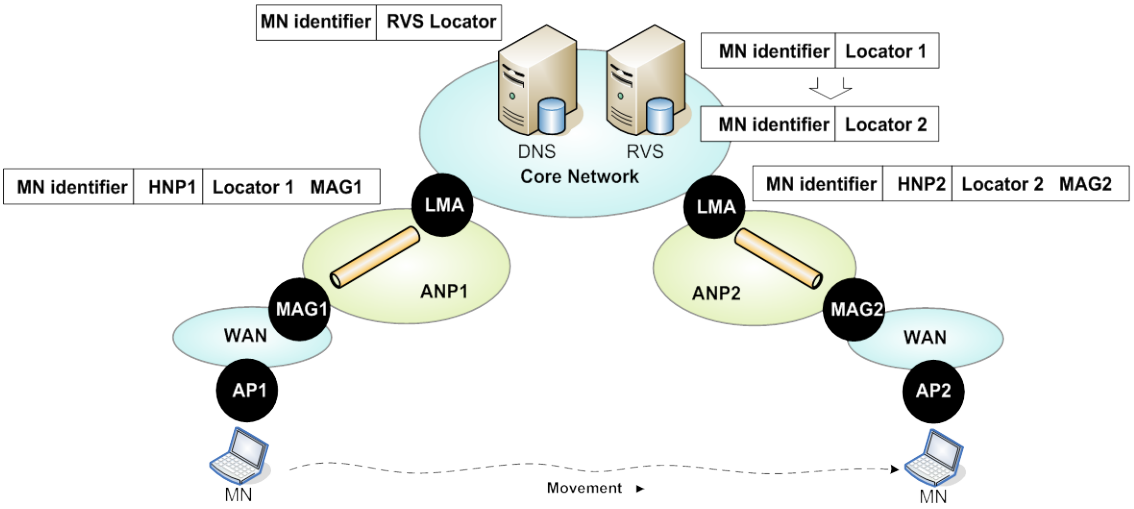
MN identifier | RVS Locator
MN identifier | Locator 1
MN identifier | Locator 2
DNS
RVS
Core Network
MN identifier | HNP1 | Locator 1 MAG1
MN identifier | HNP2 | Locator 2 MAG2
LMA
LMA
ANP1
ANP2
MAG1
MAG2
WAN
WAN
AP1
AP2
MN
MN
Movement

**Figure 6. Global Mobility**

The case of local mobility management follows exactly the standard PMIPv6 procedure. Each LMD provides always the same HNP to the MN regardless the used interface, as the HNP is linked to the MN's identifier. The LMA updates the BCE with the correct information of locator and MAG associated with the MN's identifier and HNP as shown in Fig. 7. In this case, there is no need for the MN of updating the RVS as the registered locator in the RVS is always routable to the LMA.

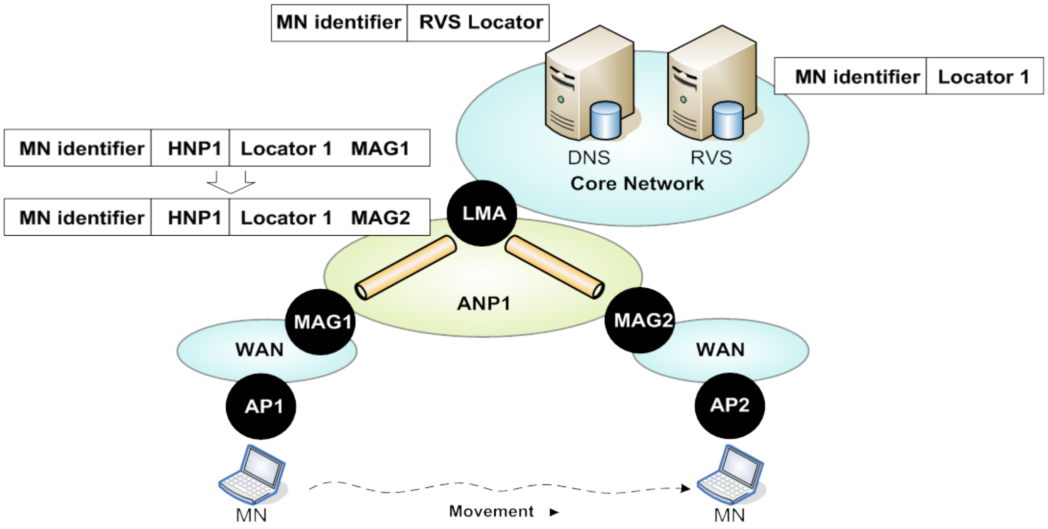

**Figure 7. Local Mobility**

## *4.6 Multihoming*

At global level, multihoming consists on the registration done by the MN, in the RVS database, of multiple locators, one per LMD, associated to the same identifier.

At local level, it is the LMA that keeps updated its BCE associating multiple locators to the same identifier and HNP. Even if the MN is multihomed at local level, external entities, such as RVS and CNs, are not aware about it.

## *4.7 Ad-hoc Networking*

We have considered as well the case in which, instead of having just a MN attached to the LMD, there is an ad-hoc network. As defined in [23], the nodes in the ad-hoc network can share a common identifier, called Group Identifier (GI), which can be used in the PBU instead of the host identifier. The BCE data structure maintained by the LMA, can be extended to store it and have a corresponding HNP for that GI. In this way the HNP is shared by all the nodes of the ad-hoc network which use it to configure their IPv6 addresses. All the traffic having as destination address an address with that particular HNP is routed by the LMA to the serving MAG for the ad-hoc network, and then by the MAG to the ad-hoc network, which will use its internal ad-hoc routing protocol for delivering the traffic to the correct MN.

## *4.8 Routing*

Routing in the core and in the edge networks is done in two different ways. While in the core network it can be based on any standard routing protocol of Internet, routing in the LMDs is completely based on information contained in the BCE of each LMA. The LMA can route packets for the MN to the correct MAG based on the destination IPv6 address (locator) or, in case there is no entry for it, on the HNP.

## *4.9 Traffic Engineering*

The LMD can silently decide to move the traffic of a MN from one WAN to another. In our architecture, this is possible thanks to locator/identifier split and to the fact that SAs are linked to identifiers and not to locators. Even if the IP address of the interface in which the MN is receiving packets is different from the destination address of the packets, the MN can accept the data traffic as far as the same HNP is used in the destination address.

# 5 ARCHITECTURES COMPARISON

The separation of identity and location is fundamental in our mobility architecture and so also in many other proposed architectures including FARA [24], the Layered Naming Architecture [25] and DOA [26], the NAT-based architectures TRIAD [27] and IPNL [28], Host Identity Indirection Infrastructure (Hi$^3$) [29], a combination of HIP and the Internet Indirection Infrastructure (i$^3$) [30][31], in TurfNet [32] and in the Split Naming/Forwarding Architecture (SNF) [33]. There are also several proposals in the IETF and IRTF that use the idea of locator/identity split as in HIP. There are host-based proposals like Site Multihoming by IPv6 Intermediation (SHIM6) [34] and router-based solutions such as LISP [35] and Six/One [36]. The proposals differ for instance in how the identifiers are defined. The Layered Naming Architecture and DOA also propose the use of topology independent endpoint identifiers from a flat namespace, while in TRIAD and IPNL domain names (FQDNs) are used as identifiers. Hi$^3$ and i$^3$ do not support internetworking across heterogeneous domains, while TurfNet uses a large number of proxy locators to forward data instead of host identities. The more incremental solutions Shim6, LISP and Six/One, do not fully separate the identifier and locator functions but use IP addresses (or parts of IP addresses) also as identifiers. Due to space limitations, this paper cannot compare all these systems to our architecture. Instead we prefer to restrict the analysis to two specific architectures, MobiSplit [21] and NodeID Architecture [37], which have several similar mechanisms and scenarios to our proposed architecture, even if significant differences exist.

The Node-ID architecture has as common design elements with our mobility architecture the fact of having independent locator domains, end-to-end security based on Node-IDs and reliance on cryptographic self-managed Node-IDs. The difference consists on the role of Node-ID routers (located in the LMAs in our architecture) , which are the contact locators for local nodes, mapping communications across borders by translating between different locator spaces and connectivity technologies, taking over the role NATs have today. The Node-ID router is similar to the Mobility Anchor Point (MAP) of Hierarchical Mobile IP v6 (HMIPv6) [10], and better to the Local RVS (LRVS) with Security Parameter Index multiplexed Network Address Translator (SPINAT) functionalities as defined in [5] [6], in which local mobility is managed with a host-based scheme. Such mechanism has the drawback of adding complexity to the network and to the terminals and of increasing signaling overhead in the wireless links, compared to the network-based local mobility management proposed in our architecture.

On the other side, MobiSplit uses network-based mobility management mechanism for LMD and is based on the idea of separating mobility management in two levels, local and global, that are managed in completely independent ways.  However, MobiSplit does not decouple identifiers from locators and uses MIPv6 as global mobility management protocol. As a consequence, in order to move sessions from one interface to another one, as sessions are linked to the locators, the MN needs to keep the same IP address while changing interface. This mechanism can bring difficulties from the point of view of the implementation because it is not the normal behavior of IP stack. Moreover, to achieve local multihoming, the same CoA needs to be configured by the MN on each terminal active interface, using for example a virtual interface. This implies that the MN cannot use its interfaces at the same time, as the basic rules of IP networking impose that the same IP address cannot be assigned to more than one interface at time. Compared to MobiSplit, our solution has built-in mechanisms for multihoming thanks to the identifier/locator split and does not implies any modification to the standard IP stack.

Table 2 summarizes briefly some characteristics of above described architectures.

| | **Node-ID** | **MobiSplit** | **HIP-PMIPv6** |
|---|---|---|---|
| **Global Mobility** | Host-based | Host-based | Host-based |
| **Local Mobility** | Host-based | Network-based | Network-based |
| **Multihoming** | Local | Global and Local | Global and Local |
| **Ad-hoc networking** | Y | N | Y |
| **Security** | Y | N | Y |
| **Network complexity** | High | Low | Low |
| **Terminal complexity** | Low | High | Low |
| **Signaling overhead** | High | Low | Low |

**Table 2. Architectures Comparison**

# CONCLUSIONS

In this work, we have first presented a secure global and localized mobility management scheme based on HIP and PMIPv6, where security, mobility and multihoming are the key aspects. We have demonstrated that our proposal represents an important improvement to PMIPv6 for inter-technology handover and multihoming, as it overcomes the current virtual interface solution in proving simultaneous usage of multiple interfaces for multihomed MNs. At the same time, we have proved that our scheme represents also a very efficient micro-mobility solution for HIP.

Moreover, we have presented a mobility architecture for future Internet and Next Generation Networks, applicable also to Next Generation Public Safety Networks, which is based on HIP and PMIPv6. The combination of these two protocols not only creates an efficient mobility and multihoming management scheme for multihomed terminals used by rescue teams and ad-hoc networks at local and global level, but puts also the basis for a new architecture that benefits of HIP built-in features such as security and efficient HI namespace. In addition, thanks to the particular locators (IPv6 addresses) created through the PMIPv6 scheme, location privacy, efficient routing and traffic engineering at local level are also supported. The mobility and multihoming scheme adopted by this architecture significantly reduces the signaling overhead in the wireless links as well as in the infrastructure without increasing the complexity on networks or on mobile terminals, important requirement for Public Safety Networks.

.

# BIBLIOGRAPHY

[1] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”, IETF RFC 3775, June 2004.

[2] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, “Host Identity Protocol”, IETF RFC 5201, April 2008.

[3] T. R. Henderson, “Host Mobility for IP Networks: A Comparison”, IEEE Network, Nov-Dec. 2003, vol. 17, issue 6, pp. 18-26.

[4] A. Khurri, E. Vorobyeva, and A. Gurtov, “Performance of Host Identity Protocol on Lightweight Hardware”, MobiArch’07, August 2007.

[5] 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.

[6] 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.

[7] J. Kempf, “Problem Statement for Network-Based Localized Mobility Management (NETLMM)”, IETF RFC 4830, April 2007.

[8] S. Gundavelli et al., “Proxy Mobile IPv6”, IETF RFC 5213, August 2008.

[9] R. Koodli, “Fast Handovers for Mobile IPv6”, IETF RFC 4068, July 2005.

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

[11] G. Giaretta, “Interactions between PMIPv6 and MIPv6: scenarios and related issues”, draft-ietf-netlmm-mip-interactions-02, IETF Internet Draft, February 2009.

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

[13] R. Wakikawa, S. Kiriyama, S. Gundavelli, “The use of Virtual Interface for Inter-technology handoffs and Multihoming in Proxy Mobile IPv6”, Mobiworld 2008, September 2008.

[14] V. Devarapalli, N. Kant, H. Lim, and C. Vogt, “Multiple Interface Support with Proxy Mobile IPv6”, draft-devarapalli-netext-multi-interface-support-00, IETF Internet Draft, March 2009.

[15] D. Damic, “Proxy Mobile IPv6 indication and discovery”, draft-damic-6man-pmip6-ind-00, IETF Internet Draft, March 2009.

[16] D. Premec, and T. Savolainen, “Inter-Technology handover in PMIPv6 domain”, draft-premec-netlmm-intertech-handover-01, IETF Internet Draft, March 2009.

[17] J. Laganier, and L.Eggert, “Host Identity Protocol (HIP) Rendezvous Extension”, IETF RFC 5204, April 2008.

[18] T. Heer, H. Wirtz, S. Varjonen, “Service Identifiers for HIP”, draft-heer-hip-service-00, IETF Internet Draft, February 2009.

[19] M. Liebsch, and L. Le, “Inter-Technology Handover for Proxy MIPv6”, draft-liebsch-netlmm-intertech-proxymip6ho, IETF Internet Draft, February 2009.

[20] **M. Jeyatharan, C. Ng, V. Devarapalli, and J. Hirano, draft-jeyatharan-netlmm-multi-interface-ps, IETF Internet Draft, October 2008.**

[21] **J. Abeille, R. Aguiar, T. Melia, I. Soto, and P. Stupar, “MobiSplit: a Scalable Approach to Emerging Mobility Networks”, ACM Mobiarch 2006, December 2006.**

[22] **G. Iapichino, C. Bonnet, “Host Identity Protocol and Proxy Mobile IPv6: a Secure Global and Localized Mobility Management Scheme for Multihomed Mobile Nodes”, to appear in IEEE GLOBECOM 2009, December 2009.**

[23] **G. Gundavelli et al., “Mobile Node Group Identifier option”, Internet Draft draft-gundavelli-netext-mn-groupid-option-01, June 2009.**

[24] **D. Clark, R. Braden, A. Falk and V. Pingali. “FARA: Reorganizing the Addressing Architecture”, ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA), August 2003, pp. 313-321.**

[25] **H. Balakrishnan, K. Lakshminarayanan, S. Ratnasamy, S. Shenker, I. Stoica, M. Walfish. “A Layered Naming Architecture for the Internet”, ACM SIGCOMM, September 2004, pp. 343-352.**

[26] **M. Walfish, J. Stribling, M.Krohn, H. Balakrishnan, R. Morris, and S. Shenker, “Middleboxes No Longer Considered Harmful”, In Proceedings of the OSDI, 2004.**

[27] **D. R. Cheriton and M. Gritter. TRIAD: A Scalable Deployable NAT-based Internet Architecture. Stanford Computer Science Technical Report, January 2000.**

[28] **P. Francis and R. Gummadi, “IPNL: a NAT-extended Internet Architecture”, ACM SIGCOMM, 2001.**

[29] **P. Nikander, J. Arkko, B. Ohlman, “Host Identity Indirection Infrastructure (Hi3)”, Second Swedish National Computer Networking Workshop (SNCNW), November 23-24, 2004.**

[30] **I. Stoica, D. Adkins, S. Zhuang, S. Shenker and S. Surana. “Internet Indirection Infrastructure”, ACM SIGCOMM, August 2002, pp. 73-88.**

[31] **D. Adkins, K. Lakshminarayanan, A. Perrig and I. Stoica. “Towards a More Functional and Secure Network Infrastructure”. Technical Report No. UCB/CSD-03-1242, EECS Department, University of California, 2003.**

[32] **S. Schmid, L. Eggert, M. Brunner, J. Quittek, “Towards Autonomous Network Domains”, 8th IEEE Global Internet Symposium, March 2005.**

[33] **A. Jonsson, M. Folke, B. Ahlgren, “The Split Naming/Forwarding Network Architecture”, First Swedish National Computer Networking Workshop (SNCNW), September 2003.**

[34] **G. Huston, “Architectural Commentary on Site Multi-homing using a Level 3 Shim”, Internet Draft draft-ietf-shim6-arch-00 (Work in Progress), July 2005.**

[35] **D. Farinacci, V.Fuller, D. Meyer, D. Lewis, “Locator/ID Separation Protocol (LISP)”, Internet-Draft, draft-farinacci-lisp-12, work in progress), March 2009.**

[36] **C. Vogt, “Six/One: A Solution for Routing and Addressing in IPv6”, Internet-draft, draft-vogt-rrg-six-one-01, November 2007.**

[37] **B. Ahlgren, J. Arkko, L. Eggert, J. Rajahalme, “A Node Identity Internetworking Architecture”, IEEE INFOCOM 2006.**

# 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 |
| GMM | Global Mobility Management |
| HA | Home Agent |
| HI | Host Identity |
| HIP | Host Identity Protocol |
| HIT | Host Identity Tag |
| HMIPv6 | Hierarchical Mobile IPv6 |
| HoA | Home Address |
| LMA | Local Mobility Anchor |
| LMM | Local Mobility Management |
| LRVS | Local Rendezvous Server |
| MAG | Mobile Access Gateway |
| 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 |
| SA | Security Association |
| SPI | Security Parameter Index |