Host Identity Protocol and Proxy Mobile IPv6: a Secure Global and Localized Mobility Management Scheme for Multihomed Mobile Nodes

Giuliana Iapichino and Christian Bonnet
Mobile Communications Department
Eurecom
Sophia Antipolis, France
{giuliana.iapichino, christian.bonnet}@eurecom.fr

Abstract—**The evolution of Internet and its hosts does not match anymore the current Internet architecture, designed when mobility, multihoming and security were not considered, and based on IP addresses with the double role of host's identity and host's topological location. In this paper we propose a secure global and localized mobility management scheme suitable for multihomed Mobile Nodes (MNs) and based on Host Identity Protocol (HIP) and Proxy Mobile IPv6 (PMIPv6). It merges the new identifier/locator split architecture proposed by HIP, especially designed for providing security and multihoming to MNs, with the micro-mobility management scheme of PMIPv6, which has been proposed for *unmodified* MNs with future Global Mobility Management (GMM) protocols. HIP-PMIPv6 combination has double benefits. On one side, it represents an efficient micro-mobility solution for HIP. On the other side, it provides a GMM scheme for PMIPv6, which supports inter-technology handover and multihoming together with security. The HIP-PMIPv6 scheme has been implemented in a real test-bed and experimental results prove its viability.**

Keywords: Host Identity Protocol, Proxy Mobile IPv6, Mobility Management, Multihoming, Security.

I. Introduction

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 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 Networks (NGNs).

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 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 paper, we propose to combine HIP with PMIPv6 in order to have a secure global and localized mobility management scheme applicable to any kind of access technology. 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 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.

The rest of this paper is organized as follows. Section II first describes HIP and the related work on its micro-mobility, and then PMIPv6 with the related work on IP session continuity across different technologies. Section III presents our proposed combination of HIP and PMIPv6. In Section IV the real implementation of the HIP-PMIPv6 scheme is illustrated and results for intra-technology handover are presented. Finally Section V concludes the paper.

II. RELATED WORK

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.

A. 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.

B. 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.

III. 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.

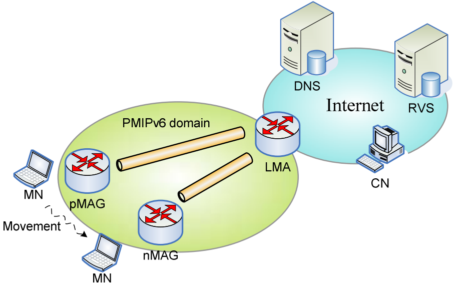

Figure 1. Proposed Global and Localized Mobility Management architecture

A. 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.

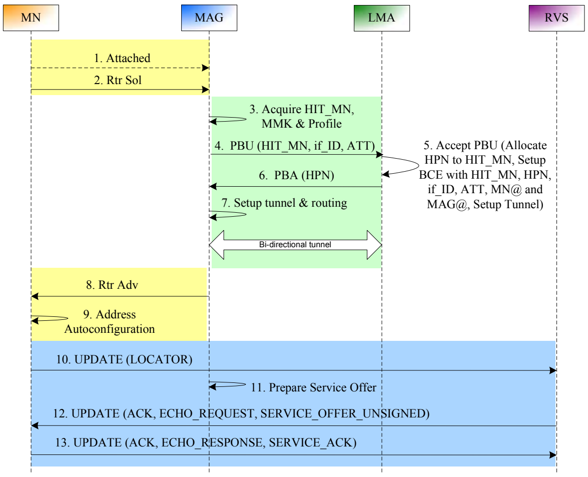
MN
MAG
LMA
RVS
1. Attached
2. Rtr Sol
3. Acquire HIT_MN, MMK & Profile
4. PBU (HIT_MN, if_ID, ATT)
5. Accept PBU (Allocate HPN to HIT_MN, Setup BCE with HIT_MN, HPN, if_ID, ATT, MN@ and MAG@, Setup Tunnel)
6. PBA (HPN)
7. Setup tunnel & routing
Bi-directional tunnel
8. Rtr Adv
9. Address Autoconfiguration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

Figure 2. Initialization

B. 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		

C. *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.

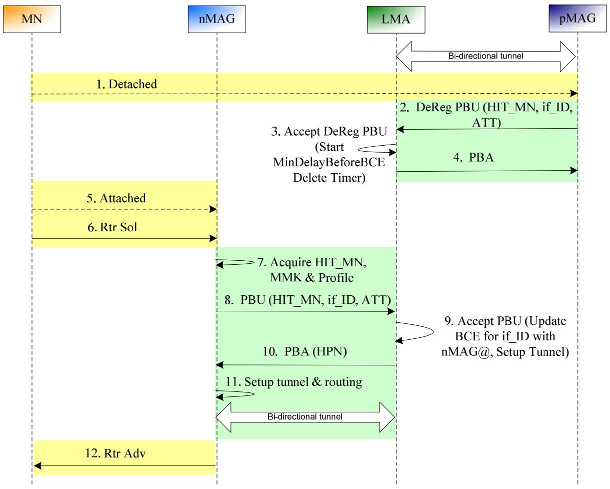
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE for if_ID with nMAG@, Setup Tunnel)
10.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

D. *Inter-technology handover and multihoming*

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.

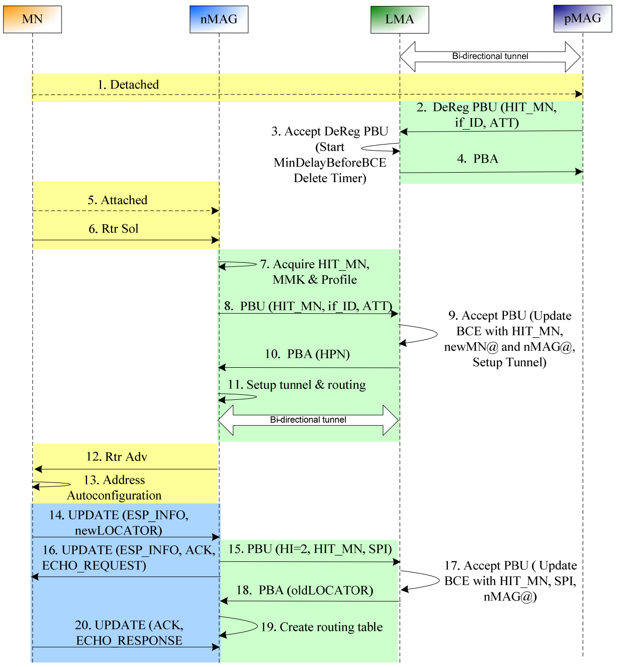
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE with HIT_MN, newMN@ and nMAG@, Setup Tunnel)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

IV. Real Implementation of HIP-PMIPv6 Scheme

The HIP-PMIPv6 scheme has been implemented in a real test-bed at our laboratory. For the HIP software we have used HIPL v.1.0.4-48 [22], an open source implementation of HIP in user-space on Linux kernel from InfraHIP project. Figure 5 illustrates the HIPL software architecture for the process of BE between client and server. More details are in [23].

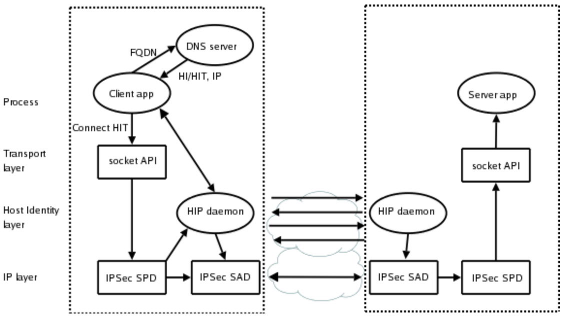

Figure 5. HIP software architecture

As regards PMIPv6 software, we have implemented it reusing the basic bricks of Mobile IPv6 for Linux (MIPL) v2.0.2 [24] for developing LMA and MAG functionalities. As shown in Fig. 6, the software architecture of PMIPv6 is built on top of MIPL v2.0.2.

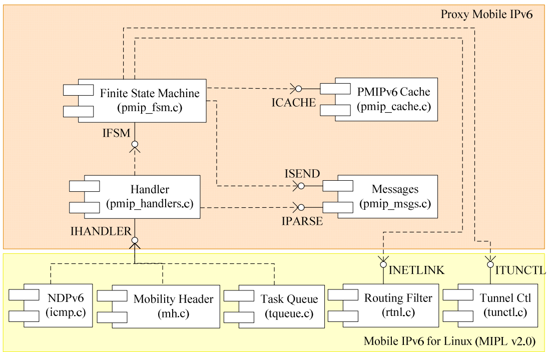

Figure 6. PMIPv6 software architecture

Our test-bed for intra-technology handover is illustrated in Fig. 7 and described hereafter. The MN, which runs HIP daemon as a client, uses its Netgear wireless card to attach to one of the two Cisco Aironet 1100 series Access Points (APs), which support IEEE 802.11a/g specifications. Each AP is directly connected to a MAG. The implementation of MAG functionalities contains additional features and modifications to MIPL to handle PBU and PBA messages and mobility options, and a modified Router Advertisement daemon (RADVD), which *unicasts* RAs with a specific HNP per MN. Each MAG is connected to the LMA. The LMA is configured as a modified HA in MIPL which stores in the BCE a unique HNP per MN and it is able to handle PBU and PBA messages.

Finally, the CN, which runs HIP daemon as a server, is connected to the LMA. All the network entities in the test-bed are running Ubuntu 7.10 with 2.6.22-15-generic Linux kernel.

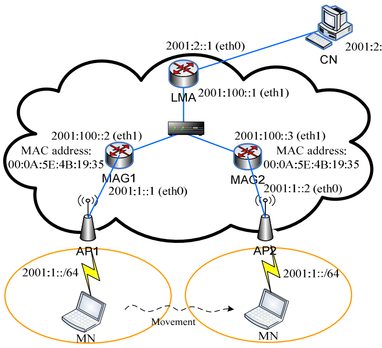

Figure 7. Test-bed configuration

In our IPv6-based scenario, the MN moves between AP1 to AP2 and also changes its subnet moving between MAG1 and MAG2. To make a realistic scenario, we have executed a test in which the MN receives a multimedia stream (video and audio) from the CN using the VideoLAN (VLC) software [25]. In order to make VLC a HIP-enabled application, we have just specified the HIT of the MN, instead of its IPv6 address, when starting the VLC at the server side. As specified by HIP, in the multimedia stream, UDP packets are encapsulated and sent using a special IPSec ESP mode called Bound End-to-End Tunnel (BEET). Video and audio data are encoded using MP4V and MPGA respectively. Video data rate is 500 Kbps using one-pass Constant Bit Rate (CBR) encoding method. Audio data rate is 128 Kbps using CBR encoding method.

In this scenario, measurements of UDP throughput are extracted from Wireshark software running in the MN during its movement from AP1 to AP2 while receiving the multimedia stream. In Fig. 8, we can see that the UDP throughput of our HIP-PMIPv6 scheme is almost stabilized at 700 Kbps when the MN stays in its subnets. When the MN performs handover, the UDP throughput becomes zero during 0.5 s due to the handover latency.

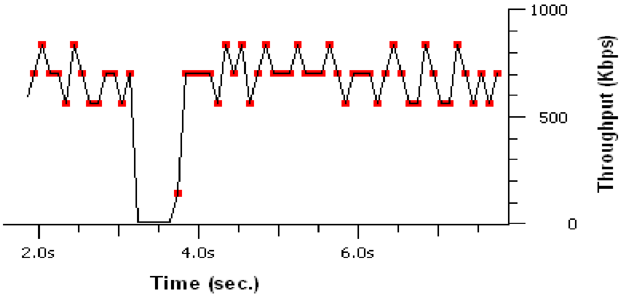

Figure 8. UDP throughput of HIP-PMIPv6 scheme

V. CONCLUSIONS

In this work, we have presented a secure global and localized mobility management scheme based on HIP and PMIPv6 and applicable to NGNs and Internet, where security, mobility and multihoming will be 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. The HIP-PMIPv6 scheme for intra-technology handover has been implemented in a real test-bed. We have tested the handover latency with a real-time application, demonstrating HIP-PMIPv6 scheme's viability.

REFERENCES

[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] HIPL, http://infrahip.hiit.fi.

[23] T. Henderson, and A. Gurtov, "HIP Experiment Report", draft-irtf-hip-experiment-05, IRTF Internet Draft, March 2009.

[24] Mobile IPv6 for Linux, http://www.mobile-ipv6.org

[25] VideoLAN software, http://www.videolan.org