Combining Mobility and Heterogeneous Networking for Emergency Management: a PMIPv6 and HIP-based Approach

Giuliana Iapichino and
Christian Bonnet
Mobile Communications Dept.
Eurecom, France
{name.surname}@eurecom.fr

Oscar del Rio Herrero
RF Payload Systems Division
European Space Agency,
Netherlands
Oscar.del.rio.herrero@esa.int

Cedric Baudoin and
Isabelle Buret
Research Dept.
Thales Alenia Space, France
{name.surname}@thalesaleniaspace.com

ABSTRACT

Emergency Management is an important topic for research community worldwide, especially after recent major disasters. The problem of supporting mobility at the disaster site to rescue teams equipped with different heterogeneous access technologies and providing interoperability between different agencies and jurisdictions is still under investigation. In this work we propose to merge the advantages of IPv6 micro-mobility management of Proxy Mobile IPv6 (PMIPv6) with macro-mobility management, security, inter-technology handover and multi-homing features of Host Identity Protocol (HIP). This new approach applied to our proposed ad-hoc satellite and wireless mesh system architecture for emergency mobile communications can improve mobility, security, reliability and interoperability in Emergency Management domain.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design – *Wireless Communication.*

General Terms

Design, Performance, Security.

Keywords

Mobility Management, Proxy Mobile IPv6, Heterogeneity, Host Identity Protocol, Public Safety Communications.

1. INTRODUCTION

Emergency is "an urgent need for assistance or relief" as defined by ETSI EMTEL [1]. Emergencies are roughly categorized as (a) daily emergencies which are handled by regular emergency services (fire brigades, emergency medical services, etc) and (b) disaster emergencies which are "a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex long-term processes". In both cases the need for an easily deployable infrastructure at the disaster site that has mobility and heterogeneous networking support is extremely important in order to help emergency teams in their difficult tasks, having access to constant communication while moving at the crisis site.

In [2], we have defined a satellite and wireless mesh network system architecture for emergency mobile communications. In [3] we have proposed Proxy Mobile IPv6 (PMIPv6) [4] as the more suitable localized mobility management protocol for our architecture, highlighting its strengths and its applicability to the system architecture. Anyway, a global mobility solution with heterogeneous and secure networking is still missing for the proposed system architecture in order to fulfill Emergency Management requirements.

The proposed combination of PMIPv6 and Host Identity Protocol (HIP) [5] represents a secure global and localized mobility solution for the heterogeneous ad hoc mesh network deployed at the disaster site and communicating with the headquarters via satellite. This solution provides also an efficient mechanism of intra and inter-technology handover for Public Safety users equipped with heterogeneous devices at the disaster field and secure end-to-end connections for communications at the disaster area and with the headquarters.

The rest of this article is organized as follows. Section 2 presents an overview on HIP mechanism and on related works on HIP micro-mobility. Section 3 describes the PMIPv6 and HIP-based approach, illustrating the important phases for mobility management. In Section 4 handover latencies of our proposal and previous micro-mobility solutions for HIP are analyzed. Finally, Section 5 concludes the paper.

2. RELATED WORK

2.1 Host Identity Protocol and its Micro-Mobility Solutions

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 MN moves to an other location in the network, the IP address of the MN changes. As a consequence, the information used to route packets to that node is changed and, as the IP address also serves as the identifier, the identifier is also changed. This means that the same node would

IWCMC'09, June 21–24, 2009, Leipzig, Germany.
Copyright © 2009 ACM 978-1-60558-569-7/09/06...$5.00

have different identifiers depending on where it is positioned in the network. To be useful the identifier should remain the same regardless of where the MN is located.

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 possible 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 enabled node, 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 in the IP-stack. To handle this translation a new layer is added to the network architecture. In Fig. 1 the new architecture, with the new Host Identity layer, is presented. In all layers above the Host Identity layer, the HIT is used instead of the IP address to represent the host. At the Host Identity layer the HIT is translated into the IP address for correct routing in the network (or IP address to HIT when receiving packets). A node learns about the HIT of a peer in the same manner as it would have done for an IP address, e.g. via DNS.

Before two HIP nodes can communicate with each other, they perform a 4-way handshake (I1, R1, I2 and R2 messages) called the HIP Base Exchange (BE). During the BE they create a session key, using the Diffie-Hellman (DH) procedure, 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, thus, even if one of the nodes moves and gets a new IP address, the SAs stay valid.

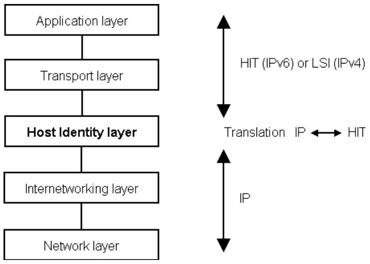


Figure 1. HIP architecture.

HIP represents a new global mobility management protocol that overcomes Mobile IPv6 (MIPv6), providing security and multihoming features to heterogeneous mobile networks with multihomed hosts. Despite MIPv6, for which several micro-mobility solutions have been proposed (e.g. Hierarchical Mobile IPv6 (HMIPv6) [6]), only few micro-mobility proposals have been presented for HIP, which still represent partial solution to the problem.

In [7], Novaczki et al. propose a micro-mobility scheme similar to HMIPv6. A new entity is introduced, the Local Rendezvous Server (LRVS), which acts as the Mobile Anchor Point (MAP) in 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.

In [8], So and Wang propose a new HIP architecture composed of micro-HIP (mHIP) agents: mHIP gateways and mHIP routers. The 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. As in the LRVS of Novaczki's scheme, a modified Security Parameter Index multiplexed Network Address Translator (SPINAT) device has to be implemented in all mHIP agents to allow the overlay routing based on SPI. As in Novaczki's scheme, the MN registers itself in the RVS and in the mHIP gateway, but with the difference that the MN registers itself in the RVS with the HIT of the mHIP gateway. This behavior breaks the macro-mobility of HIP, as changing domain for the MN will imply changing HIT, thus breaking previous sessions.

3. PMIPv6 AND HIP-BASED APPROACH

In this paper we propose a novel micro-mobility solution for HIP based on PMIPv6. PMIPv6 exempts the MN from participating in any mobility-related signaling. Proxy mobility agents, i.e. Local Mobility Anchor (LMA) and Mobile Access Gateways (MAGs), in the serving network perform mobility-related signaling 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 Home Address (HoA) on any access network. The serving network assigns a unique Home Network Prefix (HNP) to each MN whenever they move within the PMIPv6 domain. Thanks to its functionalities, PMIPv6 can reduce HIP signaling for micro-mobility.

Before starting to illustrate the integration of PMIPv6 with HIP, some assumptions need to be done. 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 and a Mobility Management Key (MMK) used by the MN to verify the signature of trusted PMIPv6's entities.

3.1 Initialization

The initialization phase is illustrated in Fig. 2. It starts acquiring the HNP as in PMIPv6. Thanks to HIP architecture, the HIT_MN is used as MN's identifier. The BCE at the LMA contains a unique HNP per HIT_MN, which is notified to all MN's interfaces, resulting in a per-MN-prefix scheme and not a per-interface-prefix approach as in PMIPv6. Thus, the binding is between the interface identifier (if_ID) and the serving MAG, not anymore between the HNP and the serving MAG.

Once the MN configures the new IP address for its interface, it has to update its RVS in order to be reachable in the Internet as in standard HIP [9]. We use this message as a hint for the serving MAG to start the micro-mobility service offered by PMIPv6 domain. A Service Offer parameter is added by the serving MAG to the reply coming from the RVS. The message contains also the HIT_domain and the MMK parameters. 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 are used by the MN to authenticate the service provider.

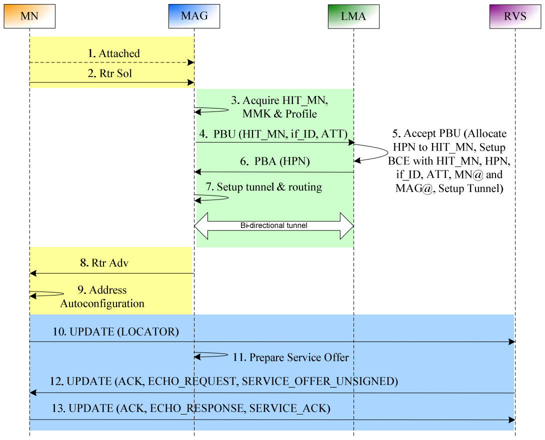

MN
MAG
LMA
RVS
1. Attached
2. Rtr Sol
3. Acquire HIT_MN, MMK & Profile
4. PBU (HIT_MN, if_ID, ATT)
5. Accept PBU (Allocate HPN to HIT_MN, Setup BCE with HIT_MN, HPN, if_ID, ATT, MN@ and MAG@, Setup Tunnel)
6. PBA (HPN)
7. Setup tunnel & routing
Bi-directional tunnel
8. Rtr Adv
9. Address Autoconfiguration
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.

3.2 Communication Setup

HIP BE is required before every HIP-based communication is established. When a Correspondent Node (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 or distributed LRVSs, as the MN's IP address configured through the PMIPv6 procedure 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 scheme. The rest of the BE will operate via a similar process. Inspecting the HIP BE, the LMA will record in the BCE the mapping between the Security Parameters Index (SPI), CN's IP address, MN's IP address and the serving MAG.

3.3 Intra and Inter-technology Handovers

The case of intra-technology handover is completely based on PMIPv6 procedure and it is described in Fig. 3. As the HNP contained in the Router Advertisement sent by any MAG in the PMIPv6 domain is always the same for a specific MN, the resulting IP address does not change. Thus the MN does not detect any change with respect to the layer-3 attachment of its interface. For this reason the MN does not send any UPDATE messages to its RVS and CNs and the complete micro-mobility process is transparent to HIP. The intra-technology handover represents the main added value of our micro-mobility solution to HIP.

The case of inter-technology handover is similar to the intra-technology handover, but it additionally requires the mobility features of HIP [10]. The complete process is illustrated in Fig. 4.

When the MN switches on its new interface, it receives always the same HNP as it is linked to the HIT_MN. This is a hint for the MN to understand it is always in the same domain, so no UPDATE messages are sent to the RVS. The advantage of using HIP is that, even if now the IP address for the new interface is different from the one of previous interface, IP session continuity is ensured as SA are linked to the identifier and not to the locator.

Anyway, when there are ongoing sessions with CNs, the MN needs to send HIP UPDATE messages to specify the IP session it wants to move to the new interface using the ESP_INFO field containing SPI.

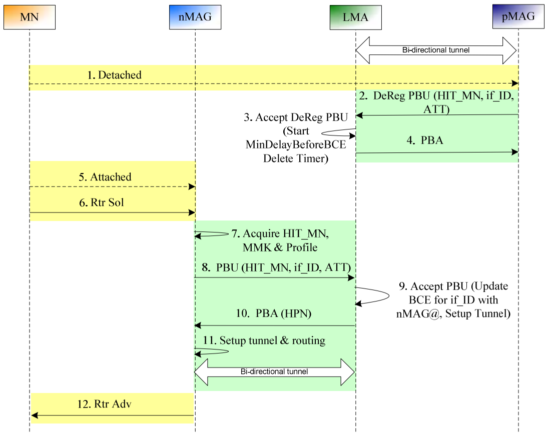

MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE for if_ID with nMAG@, Setup Tunnel)
10.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

Figure 3. Intra-technology handover.

The serving MAG is handling this UPDATE packet instead of the CN in the PMIPv6 domain. The MN recognizes the HIT_domain and the MMK in the message and accepts the reply. A Proxy Binding Update (PBU) message with Handoff Indicator (HI) option set and the HI with value of 2 (handoff between two different interfaces of the MN) is sent by the serving MAG to LMA. The LMA updates the information on the serving MAG in the BCE based on HIT_MN and SPI, not MN's IP address. A Proxy Binding Acknowledge (PBA) is sent by LMA to nMAG. 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, which creates a route for the MN based on its HNP, sends the packets to the MN that can route internally to the correct interface. For outgoing packets the CN can receive the traffic coming from any interface of the MN as the SA contains the HIT_MN, not the MN's IP address. In the case the MN is multi-homed, it can have multiple SAs with different CNs. All the active sessions with the corresponding SPIs are registered in the BCE of LMA.

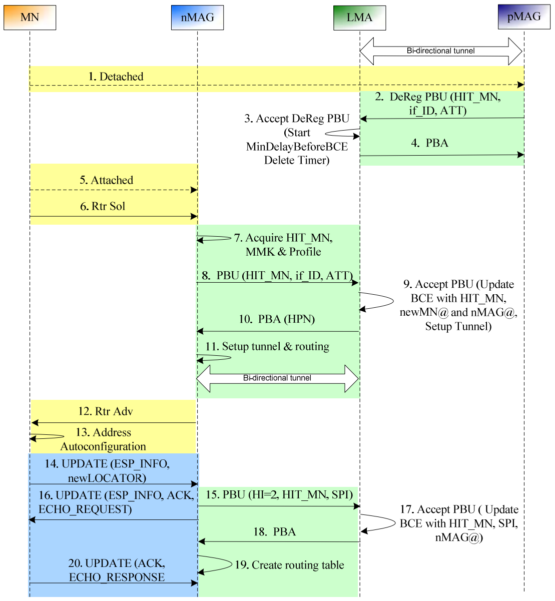

MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE with HIT_MN, newMN@ and nMAG@, Setup Tunnel)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

Figure 4. Inter-technology handover.

4. HANDOVER LATENCY ANALYSIS

The proposed PMIPv6 and HIP-based approach is a new micro HIP scheme, but also represents a macro and micro-mobility management solution that can be applied to our satellite and wireless mesh system architecture for Public Safety applications, collocating LMAs with the satellite gateways and MAGs with the mobile routers. The communication between LMAs can be done as in [11]. In this work we have simplified the architecture considering a simple domain with one LMA and two MAGs as described in Fig. 5.

In this section we analyze the handover latency of our HIP-PMIPv6 scheme for the two cases of intra and inter-technology handover between two MAGs belonging to the wireless mesh network. We compare the performances of our scheme with Novaczki's proposal. So's scheme represents an extension to Novaczki's one in a balanced binary tree structure, thus a comparison between our and So's schemes will replicate the analysis between HIP-PMIPv6 and Novaczki's proposal.

We consider the simple analytical model shown in Fig. 5, in which the LRVS of Novaczki's proposal is collocated with our LMA and the Access Routers (ARs) with MAGs. Similar to [12] [13], we use the following notations:

- The delay between MN and Radio Access Point (RAP) is t_{mr}, which is the time necessary for a packet to be sent between the MN and the RAP through a wireless link.
- The delay between RAP and AR/MAG is t_{ra}.
- The delay between AR/MAG and the LRVS/LMA is t_{am}.

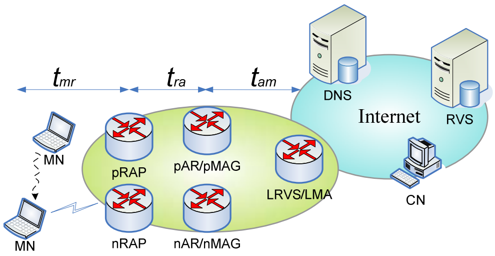


Figure 5. Simple analytical model for performance analysis.

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

$$T_{HO} = T_{L2} + T_{MD} + T_{AC} + T_{REG}$$

where T_{L2} represents the delay due to layer 2 signaling, T_{MD} the movement detection delay, T_{AC} the address configuration delay and T_{REG} the location registration delay.

In Novaczki's scheme there is no difference between the handover latency for intra and inter-technology handover. It is composed of: T_{L2} equivalent to t_{mr}; T_{MD} 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 T_{MD} is half of that, thus *(MinInt + MaxInt)/4*; T_{AC} is due to the Duplicate Address Detection (DAD) process and can be expressed as *R X D*, where *R* is *RetransTimer* and *D* is the *DuplAddrDetectTransmit*; T_{REG} includes the time of the HIP registration update delay from MN to the LRVS (i.e., $3(t_{mr}+ t_{ra}+ t_{am})$). In conclusion the handover latency for Novaczki's scheme is

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

In HIP-PMIPv6 approach the handover latency, in the case of intra-technology handover, is composed of: T_{L2} equivalent to t_{ra}; T_{MD} is null as the IP-level movement detection does not occur; 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; T_{REG} is composed of the sum of the PBU delay between the MAG and the LMA ($2t_{am}$) and the packet delivery delay from the MAG to the MN ($t_{mr} + t_{ra}$), thus

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

In the case of inter-technology handover, the handover latency of HIP-PMIPv6 is the sum of $T_{HO\text{-}INTRA}$ and an additional T_{REG}, due either to the HIP registration update delay (i.e., $3(t_{mr}+ t_{ra})$) when the delay between MN and MAG is higher than the one between MAG and LMA or to the PBU delay between MAG and LMA ($2t_{am}$) in the other case. The result is

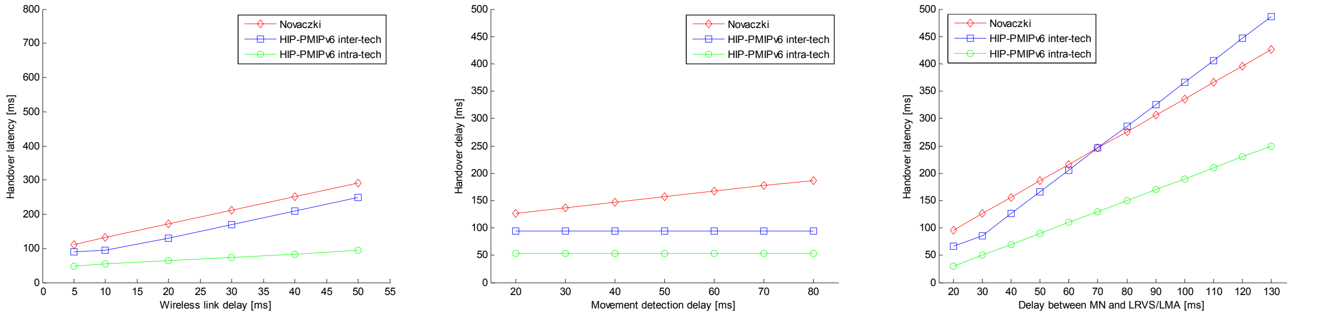
$$T_{HO-INTER}^{HIP-PMIPv6} = \begin{cases} 4t_{mr} + 5t_{ra} + 2t_{am} & for \quad 3(t_{mr} + t_{ra}) \geq 2t_{am} \\ t_{mr} + 2t_{ra} + 4t_{am} & for \quad 3(t_{mr} + t_{ra}) \leq 2t_{am} \end{cases}$$

For our analysis we use the same or similar values to the parameters shown in [13]. We assume t_{mr} to be 10 ms, considering relatively low bandwidth in a wireless link, $t_{ra} = 2$ ms, and $t_{am} = 20$ ms. We set *MinInt* = 30 ms, *MaxInt* = 70 ms, *R* = 1000 ms and *D* = 1 [13]. The numerical results are illustrated in Fig. 6.

Figure 6a shows that, in the three considered cases, handover latencies increase with the wireless link delay. The intra-technology HIP-PMIPv6 is the least affected by the distance between MN and RAP as the MN is not involved in mobility-related signaling. Comparing Novaczki's scheme with HIP-PMIPv6 inter-technology, we can see that, even if t_{mr} contributes in the same way to both schemes, Novaczki's proposal is penalized by the fact that the 3-way HIP UPDATE procedure involves the LRVS, and not the MAG as in HIP-PMIPv6 scheme for inter-technology handover, causing higher values of handover latency.

Figure 6b evaluates the impact of T_{MD} over the handover latencies of Novaczki's scheme and HIP-PMIPv6 proposal. The advantage of applying the per-MN-prefix model in our proposal is used to make the MN believe it is always in its home network, thus no IP-level movement is detected by the MN and T_{MD} has no impact in our proposal. On the contrary, the graph for Novaczki's scheme increase as T_{MD} does.

Finally Fig. 6c shows the impact of ($t_{mr}+ t_{ra}+ t_{am}$) over the handover latency, in particular the impact of t_{am} keeping t_{mr} and t_{ra} constant. The intra-technology HIP-PMIPv6 has again the best performances as it is only affected by PBU and PBA messages delay. As regards inter-technology HIP-PMIPv6 and Novaczki's scheme behaviors, we see that, when the delay between MN and LRVS/LMA reaches 70 ms, our proposal pays the price for having double PBU-PBA messages, reporting higher values of handover latency. Anyway, Fig. 6c shows the resulting handover latencies for a scenario in which the MN is single-homed, thus the handover process from one technology to the other one is done by the MN right after the new attachment. Novaczki's scheme does



(a) Impact of wireless link delay **(b) Impact of movement detection delay** **(c) Impact of delay between MN-LRVS/LMA**

Figure 6. Handover latency comparison between Novaczki's and HIP-PMIPv6 schemes.

not support multi-homed MNs. On the contrary, our proposal takes into account a scenario in which technology domains can be overlapped and multihomed MNs have the possibility, after having done the new attachment, of moving IP sessions from one interface to the other one, following the Always Best Connected concept. This is possible using the double PBU-PBA messages.

5. CONCLUSIONS

In this work we have proposed a PMIPv6 and HIP-based approach that represents a new solution for mobility and heterogeneous networking to Emergency Management domain. The result is a system architecture in which Public Safety users can use the different technologies of their multi-homed devices and be free to move IP sessions from one interface to another one without breaking the already established secure associations, being connected to the always best network available at the disaster site.

We have also proved that our approach represents a very efficient micro-mobility solution for HIP. Applying PMIPv6 features to HIP, it is possible to have an intra-technology handover process which is completely transparent to HIP MNs thanks to the fact that they do not detect any change to the previous configured IPv6 address. Thus, the necessary signaling messages for the handover are reduced and the performances in terms of handover latency demonstrate the high efficiency of this solution compared to any other previous proposal. Moreover, our scheme considers also the case of inter-technology handover and multihoming, merging together PMIPv6 with HIP mobility and multihoming features.

6. ACKNOWLEDGMENTS

This work has been supported by the European Space Agency Networking Partnering Initiative (NPI) program. It is co-funded by the European Space Agency and Thales Alenia Space.

7. REFERENCES

[1] http://www.emtel.etsi.org

[2] 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 (ICSSC 2008), June 2008.

[3] G. Iapichino, C. Bonnet, O. del Rio Herrero, C. Baudoin, and I. Buret, "A Mobile Ad-hoc Satellite and Wireless Mesh Networking Approach for Public Safety Communications", Proc. 10th IEEE International Workshop on Signal Processing for Satellite Communications (SPSC 2008), October 2008.

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

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

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

[7] 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.

[8] 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.

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

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

[11] H. N. Nguyen, C. Bonnet, G. Iapichino, " Extended proxy mobile IPv6 for scalability and route optimization in heterogeneous wireless mesh networks", to be published in International Journal of Ubiquitous Computing, June 2009.

[12] 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.

[13] K. Kong, W. Lee, Y. Han, M. Shin, and H. You, "Mobility Management for All-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6", IEEE Wireless Commun., vol. 15, no. 2, April 2008, pp. 36-45.