Mobility, Access Heterogeneity and Security for Next Generation Public Safety Communications

Giuliana Iapichino, Christian Bonnet
Mobile Communications Department
Eurecom
Sophia Antipolis, France
name.surname@eurecom.fr

Oscar del Rio Herrero
RF Payload System Division
European Space Agency
Noordwijk, Netherlands
Oscar.del.Rio.Herrero@esa.int

Cedric Baudoin, Isabelle Buret
Research Department
Thales Alenia Space
Toulouse, France
name.surname@thalesaleniaspace.com

Abstract—**Next Generation Public Safety Communication (PSC) is a crucial topic for research community worldwide. There is a strong need of research towards Public Safety user requirements, such as mobility and security support in a system architecture able to interconnect heterogeneous access technologies belonging to different agencies and jurisdiction. In this work, a combination of Proxy Mobile IPv6 (PMIPv6) and Host Identity Protocol (HIP) is proposed, in order to benefit from a complete macro and micro-mobility management protocol with the added values of intra and inter-technologies handover and multi-homing features for a heterogeneous and secure network with minimum impact on Public Safety mobile user terminals. This new approach is applied to our proposed ad-hoc satellite and wireless mesh architecture for emergency mobile communications and a complete description of the PMIPv6-HIP mobility management phases is provided.**

Keywords: Mobility, Security, Heterogeneity, Public Safety Communications, Proxy Mobile IPv6, Host Identity Protocol.

I. INTRODUCTION

The awareness of the need for effective emergency telecommunication network has raised, especially after recent major disasters. The lesson learned from them and from the interviews to team leaders at first response organizations points out that the use of public communication systems is not sufficient. There are important factors, not considered in public communication systems, which responders faced during rescue operations: mobility, access heterogeneity and security [1]. Mobility and access heterogeneity refer to the ability for Public Safety users to roam between different networks, potentially operated by different agencies and jurisdictions, and the procedures involved in self-organization as device discovery, connection establishment, address allocation, routing and topology management. On the other hand, a common secure system is needed at the disaster site in order to protect sensitive data coming from multiple federal, state and local agencies with different charters and possibly also from military forces, assuring encryption and information privacy.

Mobility management can be divided into micro-mobility and macro-mobility management, depending on Mobile Node (MN)'s movements within a domain or across domains. In the first case, several Mobile IP (MIP)-based solutions have been proposed, most of them host-based mobility management protocols, e.g. Hierarchical Mobile IPv6 (HMIPv6). They require host stack changes, signaling overhead and high deployment cost. To overcome these shortcomings, a network-based mobility management protocol called PMIPv6 [2] has been proposed by IETF. PMIPv6 enables IP mobility for a host without requiring its participation in any mobility related signaling. As regards macro-mobility management, MIPv6 and HIP [3] represent the most important solutions, which use completely different strategies. MIPv6 assigns a new address, called Care-of-Address (CoA), to the MN each time it enters a new domain. A binding between the Home Address (HoA) and the CoA is used by the MN for updating its Home Agent (HA) about its new location. On the other side, HIP introduces a new network architecture in which the IP address is used only as a locator for the MN, while the role of identifier is represented by the Host Identity (HI). Applications are linked to a 128-bit long hashed encoding of HI called Host Identity Tag (HIT), not anymore to the locator, thus any change of the IP address does not imply any connection break. IPSec Encapsulated Security Payload (ESP) and Security Association (SA) pair is created between endpoints using Diffie-Hellman authenticated key exchange. The proposed combination of PMIPv6 and HIP provides a secure macro and micro-mobility solution for heterogeneous PSC networks, representing an efficient mechanism for intra and inter-technology handover between Public Safety users at the disaster field and secure end-to-end communications inside and outside the disaster area.

The rest of this work is organized as follows. In section II an overview of our proposed hybrid satellite and terrestrial system architecture is provided. Section III describes the new proposed PMIPv6 and HIP combination, illustrating all the important phases of mobility management. In Section IV a performance analysis of our new proposal and previous micro-mobility solutions for HIP is provided. Finally, Section V concludes the paper.

II. AD-HOC SATELLITE AND WIRELESS MESH SYSTEM ARCHITECTURE FOR EMERGENCY COMMUNICATIONS

Satellite networks are the best and more reliable platform for ubiquitous communications in emergency scenarios for providing a backhaul connection to headquarters [4], as they are not affected by disasters. Wireless Mesh Networks (WMNs) are multi-hop wireless networks, able to dynamically

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

self-organize and self-configure and to operate in a heterogeneous environment with a variety of technologies. These features make them excellent candidates for PSC networks [5]. In [6] we have proposed a system architecture which links the two technologies through vehicles having double functionalities, called Vehicle Communication Gateways (VCGs). They provide on one side vehicle-to-infrastructure (V2I) communications maintaining Internet connectivity with the disaster site through satellite links: S-UMTS vehicles operating in S/L band and DVB-RCS vehicles operating in Ku/Ka band. On the other side, VCGs are able to establish vehicle-to-vehicle (V2V) communications based on ad-hoc networking, giving connectivity to mobile terminals through the mobile ad-hoc mesh network.

The result is the hybrid satellite and terrestrial system architecture illustrated in Fig. 1, which have a high level of robustness and fault tolerance together with high reliability and quick deployment. In order to manage the mobility of rescue teams inside the disaster area and to provide interoperability among equipments belonging to different Public Safety agencies, PMIPv6 has been suggested in [7] as micro-mobility management protocol. Once a Mobile Node (MN) enters the mobile ad-hoc mesh network at the disaster site and performs access authentication, the network ensures that the MN believes it is always on its home network and can obtain its home address on any access network. The ad-hoc mesh network assigns a unique home network prefix to each MN whenever they move within it. Thus, for MNs the entire network appears as their home network. In the presented architecture VCGs assume the role of Local Mobility Anchors (LMAs) in PMIPv6 protocol, being the topological anchor points for the MNs' home network prefix. LMA in PMIPv6 is responsible for maintaining the MN's reachability state and includes a Binding Cache Entry (BCE) for each currently registered MN with MN-Identifier and the MN's home network prefix. Mobile routers perform as Mobile Access Gateways (MAGs) in PMIPv6, managing the mobility on behalf of MNs. MAG in PMIPv6 is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA. Moreover, MAG establishes a tunnel with LMA for enabling the MN to use an address from its home network prefix and emulates the MN's home network on the access network for each MN.

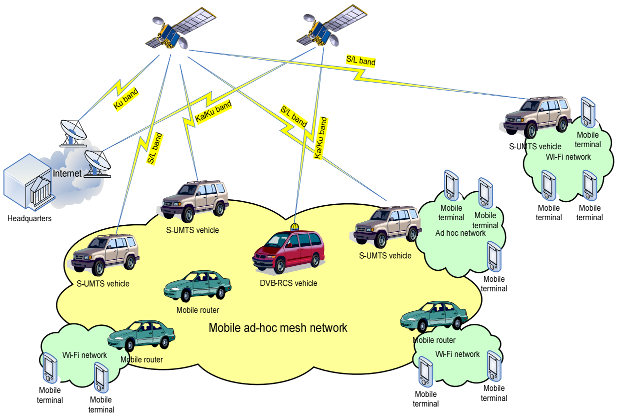

Figure 1. Hybrid satellite and terrestrial system architecture

III. PROPOSED COMBINATION OF PMIPV6 AND HIP

Comparing the most promising macro-mobility solutions, HIP and MIPv6, in a heterogeneous IPv6 network environment, it has been proved that HIP performs better than MIPv6 in terms of handover latency [8], providing also security and multi-homing features. Several micro-mobility solutions have been proposed for MIPv6. On the contrary, only few micro-mobility proposals have been presented for HIP, which still represent partial solution to the problem and still need improvements to develop all HIP's potentialities.

In [9], 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 Correspondent Node (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 [10], So and Wang propose a new HIP architecture composed of micro-HIP (mHIP) agents: mHIP gateways and mHIP routers. mHIP agents under the same network domain share a common HIT to represent the whole mHIP domain and can sign messages on behalf of the group. This scheme permits to distribute the load of the LRVS in Novaczki's scheme among mHIP agents and provides a framework in which any number of security scheme can be adopted. As in the LRVS of Novaczki's scheme, a modified SPINAT device has to be implemented in the mHIP agents to allow the overlay routing based on Security Parameters Index (SPI). In the same way, 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 support of HIP, as changing domain for the MN will imply changing HIT, thus breaking previous sessions.

Our proposal tries to overcome these issues and to provide a complete macro and micro-mobility scheme. Before starting to analyze hereafter 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.

A. Initialization

The first part of the initialization phase is quite similar to PMIPv6 initialization [2]. When a MN enters a Proxy Mobile IPv6 domain and attaches to an access link, the MAG on that access link, after identifying the MN and acquiring its identity, will determine if the MN is authorized for the network-based mobility management service. In the first step, a MN attached to the PMIPv6 domain network is detected by the MAG. The MAG sends access request message to Authentication, Authorization and Accounting (AAA) server to obtain the MN identifier (HIT_MN) and profile, together with the MMK.

For updating the LMA about the current location of the MN, the MAG sends a Proxy Binding Update message to the LMA with HIT_MN, the interface_ID and the Access Technology Type (ATT). Upon receiving and checking the validity of this Proxy Binding Update message, the LMA sends a Proxy Binding Acknowledgement message including the MN's home network prefix. It also creates the BCE in which registers the HIT_MN, the prefix, the new MN’s IP address, the MAG’s IP address and sets up its endpoint of the bi-directional tunnel to the MAG. The MAG on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the LMA and also sets up the forwarding for the mobile node's traffic. At this point, the MAG has all the required information for emulating the MN’s home link. It sends Router Advertisement messages to the MN on the access link advertising the MN's home network prefix as the hosted on-link prefix. The MN, on receiving these Router Advertisement messages on the access link, attempts to configure its interface using either stateful or stateless address configuration modes, based on the modes that are permitted on that access link as indicated in Router Advertisement messages. At the end of a successful address configuration procedure, the MN has one address from its home network prefix. The MN has to send an UPDATE message to its RVS with the new IP address. Once this message arrives to the MAG, it will start the Passive Service Discovery procedure after forwarding the packet. It will send a Service Announcement packet for mobility management to the MN. The message contains the HIT_domain and the MMK. The MN, which is interested in the offered service, can complete the registration process by sending I2 to the MAG. A R2 packet from the MAG will conclude the registration. An UPDATE message for the CN with the new LOCATOR and ESP_INFO containing the SPI values is also required in the case there is an active connection between the MN and the CN. The HIP UPDATE packet is signed but not encrypted so that the SPI values can be used by LMA to update the binding cache. Fig. 2 shows in detail the signaling flow for initialization.

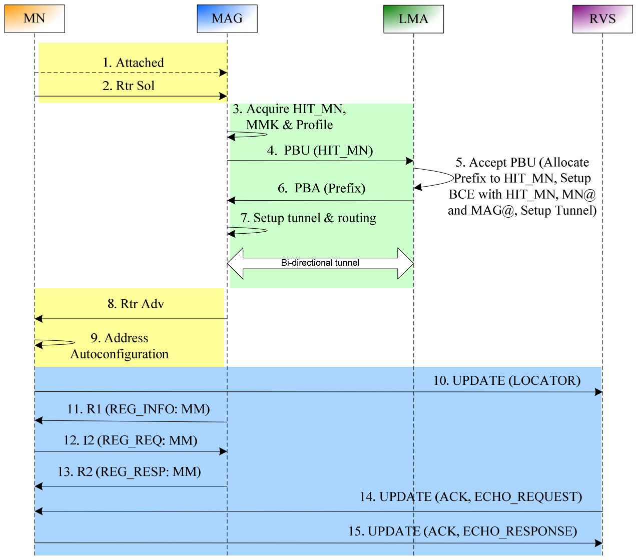
MN
MAG
LMA
RVS
1. Attached
2. Rtr Sol
3. Acquire HIT_MN, MMK & Profile
4. PBU (HIT_MN)
5. Accept PBU (Allocate Prefix to HIT_MN, Setup BCE with HIT_MN, MN@ and MAG@, Setup Tunnel)
6. PBA (Prefix)
7. Setup tunnel & routing
Bi-directional tunnel
8. Rtr Adv
9. Address Autoconfiguration
10. UPDATE (LOCATOR)
11. R1 (REG_INFO: MM)
12. I2 (REG_REQ: MM)
13. R2 (REG_RESP: MM)
14. UPDATE (ACK, ECHO_REQUEST)
15. UPDATE (ACK, ECHO_RESPONSE)

Figure 2. Initialization

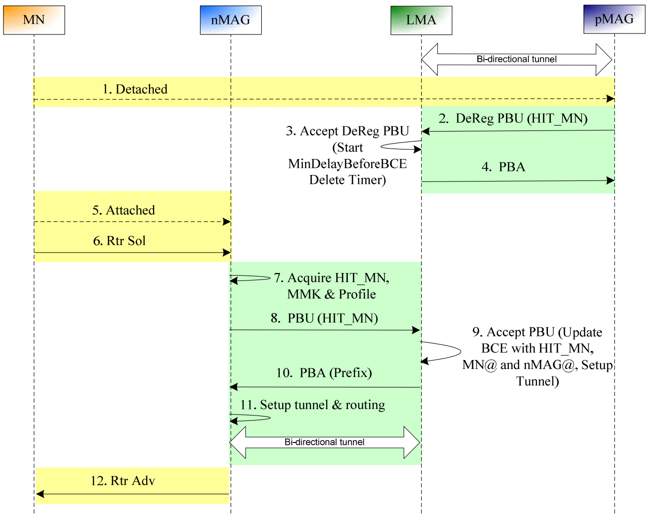
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN)
9. Accept PBU (Update BCE with HIT_MN, MN@ and nMAG@, Setup Tunnel)
10. PBA (Prefix)
11. Setup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

Figure 3. Intra-technology handover

B. *Communication setup*

HIP Base Exchange (BE) [3] is required before every HIP-based communication is established. When the CN wants to start communication with the MN, the CN will get the MN’s RVS server from the DNS server. The CN starts the HIP BE with the MN via RVS. RVS forwards the HIP I1 packet directly to the MN. In this work it is not necessary to have a LRVS as the MN’s IP address is always directing the BE through the LMA. I1 is routed by LMA to the correct MAG using the information in the BCE as in the PMIPv6 architecture. The rest of the BE will operate via a similar process. Inspecting the HIP BE, the LMA will record in the Binding Cache the mapping between the SPI, CN’s IP address, MN’s IP address and the serving MAG.

C. *Intra-technology handover*

The intra-technology handover is based on PMIPv6 procedure and it is illustrated in Fig. 3. After obtaining the initial address configuration in the PMIPv6 domain, if the mobile MN changes its point of attachment, the MAG on the previous link (pMAG) will detect the MN’s detachment from the link. It will signal the LMA and will remove the binding and routing state for that MN. The LMA, upon receiving this request, will identify the corresponding mobility session for which the request was received, and accepts the request after which it waits for a certain amount of time to allow the MAG on the new link (nMAG) to update the binding. However, if it does not receive any Proxy Binding Update message within the given amount of time, it will delete the binding cache entry.

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

D. Inter-technology handover

The inter-technology handover is based on the mobility features of HIP [11] in combination with micro-mobility features provided by PMIPv6. The MN switches on its second interface and obtains the same prefix from the network (see initialization phase). The MN realizes it is still in the same domain, so it does not need to update the RVS, the network will manage the mobility issues.

Once the MN decides to start an inter-technology handover procedure with its CN, the MN will send to the CN an UPDATE message with the LOCATOR parameter containing the second interface's IP address. In the UPDATE message it is also present the ESP_INFO parameter containing the values of the old and new SPIs for the security association. In this case, the OLD SPI and NEW SPI parameters both are set to the value of the preexisting incoming SPI; this ESP_INFO does not trigger a rekeying event. The MN waits for this UPDATE to be acknowledged, and retransmits if necessary, as specified in the base specification. The UPDATE packet with the new IP address is intercepted by the serving MAG which will start the handover procedure. The packet is processed by the MAG and it is not forwarded to the CN.

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

On the other side, a Proxy Binding Update message with Handoff Indicator option set to the value of 2 (handoff between two different interfaces of the MN) is sent by the serving MAG to LMA. It contains also the HIT_MN and the SPI. In the case of inter-technology handover, the LMA updates the information on the serving MAG in the BCE based on HIT_MN and SPI, not MN's IP address. A Proxy Binding Acknowledge is sent by LMA to nMAG with the information of the previous interface's IP address in order to setup the routing table at nMAG. No UPDATE message is sent to the CN, the complete process take place only in PMIPv6 domain. The complete process is illustrated in Fig. 4.

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

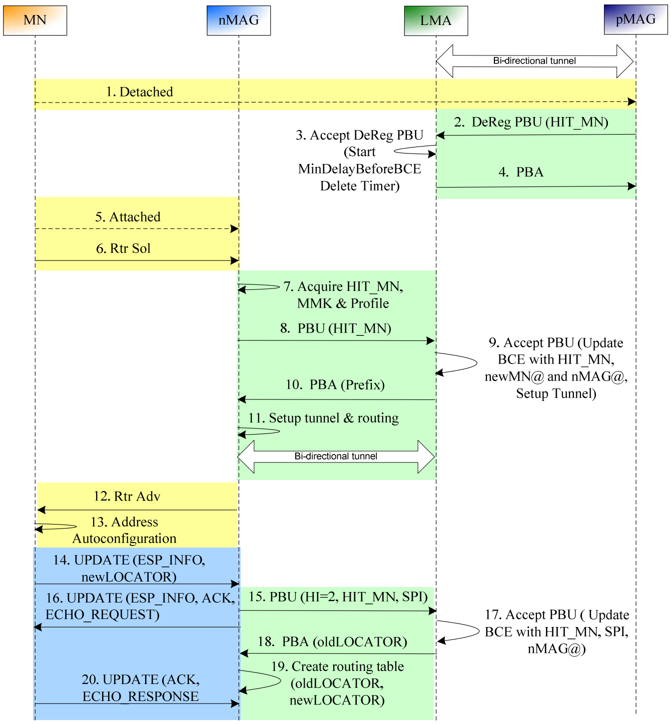
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN)
9. Accept PBU (Update BCE with HIT_MN, newMN@ and nMAG@, Setup Tunnel)
10. PBA (Prefix)
11. 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 (oldLOCATOR)
19. Create routing table (oldLOCATOR, newLOCATOR)
20. UPDATE (ACK, ECHO_RESPONSE

Figure 4. Inter-technology handover

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

IV. Performance Analysis

In this section we make a qualitative comparison between our proposal, Novaczki's scheme and So's solution in order to show the advantages of the proposed approach. Our analysis only focuses on the delay in the network transmission. We use Round Trip Time (RTT) as the measure for the propagation delay. One RTT is defined as the time required for the source transfer to and from the destination. We use $RTT_{A,B}$ to represent the RTT between node A and node B. In order to have a more clear idea of the three architectures, we can consider the LRVS of Novaczki's scheme and mHIP gateway of So's scheme collocated with the LMA of our proposal and mHIP router collocated with the MAG. We analyze the initialization, the intra-technology and the inter-technology handover phases for the three schemes.

Initialization mechanism

According to basic HIP mobility functionalities, the first registration of MN in the RVS is required for the three schemes. It is the regular four-message Base Exchange with the registration extensions. Moreover, in Novaczki's scheme and in So's scheme the registration at LRVS and mHIP gateway respectively is needed for each interface of the MN, while in our solution only one registration is done (for the first interface) with the network, in particular with the first MAG. It is important to remind that in our scheme the entire network is seen as a unique entity, which is in charge of mobility management.

Intra-technology handover mechanism

In Novaczki's scheme, each time the MN moves behind a different router it has to re-configure its IP address and to update the LRVS with the new locator. In So's scheme, the UPDATE message for signaling the new IP address to mHIP gateway is processed by the nearest mHIP agent, so the RTT is smaller (in the case mHIP agent is a mHIP router) or equal (in the case mHIP agent is the mHIP gateway) to RTT in Novaczki's scheme. In our scheme, as the same IP address is configured by the MN, there is no need for UPDATE messages. This phase represents the most relevant improvement that our proposal is providing to HIP micro-mobility.

Inter-technology handover mechanism

For Novaczki's and So's schemes, this case is the same as the intra-technology phase. In our proposal, as the new interface will obtain a new IP address from the network, different from the previous interface, the MN needs to update the CN with the new locator. The MAG intercepts the message and handles it instead of the CN. In our proposal, the RTT is smaller or, in the worst case, equal to the RTT of the other two schemes.

TABLE I. PERFORMANCE SUMMARY FOR THE THREE SCHEMES

	Initialization - first registration	**Intra-technology handover**	**Inter-technology handover**
Novaczki's scheme	$2RTT_{MN,RVS}$ + $2RTT_{MN,LRVS}$	$1,5RTT_{MN,LRVS}$ = $1,5RTT_{MN,LMA}$	$1,5RTT_{MN,LRVS}$ = $1,5RTT_{MN,LMA}$
So's scheme	$2RTT_{MN,RVS}$ + $2RTT_{MN,mHIPgw}$	$1,5RTT_{MN,MAG} \leq 1,5RTT_{MN,mHIPagent} \leq 1,5RTT_{MN,LMA}$	$1,5RTT_{MN,MAG} \leq 1,5RTT_{MN,mHIPagent} \leq 1,5RTT_{MN,LMA}$
PMIPv6-HIP scheme	$2RTT_{MN,RVS}$ + $1,5RTT_{MN,MAG}$	No messages	$1,5RTT_{MN,MAG}$

Table I represents a summary of the three micro-mobility schemes in the three phases, in which it is shown the advantages in terms of reduced signaling of our proposed PMIPv6 and HIP combination. Moreover, there is no need for SPINAT devices in our architecture, reducing the complexity in the network.

V. CONCLUSION AND FUTURE WORK

In this work, we have proposed a new approach based on PMIPv6 and HIP combination for providing mobility, security and heterogeneous networking to our satellite and wireless mesh network for Public Safety Communications. The combination of PMIPv6 and HIP protocols helps rescue teams to easily move and keep their connections on while moving under different mobile routers and switching from one access technology to another. Each MN in the ad hoc mesh network has an identifier, used for establishing security connections with peers. Diffie-Hellman scheme for secret key exchange together with IPSec is used for creating the SA between MNs, as in HIP scheme. Once the SA is established, modifications to the IP address of the MN due to the mobility do not break the connection, as the SA is linked to the identifiers. In order to avoid unnecessary signaling for updating the peer about the new locator as in HIP standard, we apply a micro-mobility solution based on PMIPv6.

Each MN obtains an IP address from the network that is routable outside the ad hoc mesh network and remains unchanged even when the MN moves behind different mesh routers inside the domain. Thanks to micro-mobility management, the network is able to route correctly the traffic to the right MN proving seamless handover features. As the IP address does not change, no update messages are needed. In the case the MN is equipped with multiple interfaces and wants to switch from one access technology to another, e.g.. in order to use a more reliable connection, it can notify the network with its intention and the traffic will be routed directly to the new interface. For communications between rescue teams located at the disaster area and decision makers at the headquarters, this mechanism is really useful as it helps to save resources and satellite bandwidth. Moreover, it reduces the delay and allows rescue teams to benefit of an Always Best Connected vision, proving robustness and reliability to the system. The mechanism is also independent from the access technology, so interoperability of communication devices within and across different agencies and jurisdictions is possible.

Next step will be the implementation of the presented mechanism in Eurecom's testbed in order to prove its advantages and to better evaluate its added value to Next Generation Public Safety Communication networks.

REFERENCES

[1] R. Dilmaghani, R. Rao, "On Designing Communication Networks for Emergency Situations", International Symposium on Technology and Society (ISTAS '06), June 2006.

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

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

[4] ETSI TR 102 641 v1.1.1, "Satellite Earth Stations and Systems (SES); Overview of present satellite emergency communications resources", August 2008.

[5] M. Portmann and A.A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Internet Computing, vol. 12, no. 1, 2008, pp. 18-25.

[6] 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.

[7] 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 Space Communications (SPSC 2008), October 2008.

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

[9] 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.

[10] 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.

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