A Mobile Ad-hoc Satellite and Wireless Mesh Networking Approach for Public Safety Communications

G. Iapichino, C. Bonnet
Mobile Communications Department
Eurecom
Sophia Antipolis, France
{Iapichin, Bonnet}@eurecom.fr

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

C. Baudoin, I. Buret
Research Department
Thales Alenia Space
Toulouse, France
Cedric.Baudoin@thalesaleniaspace.com

Abstract—**It is widely recognized that emergency management and disaster recovery systems are an issue of paramount importance in communities through the world. The definition of a Public Safety communications infrastructure is a high-priority task due to the lack of interoperability between emergency response departments, the reduced mobility during coordinated operations on a broad scale and the need for access to critical data in real-time. This work proposes an "ad-hoc networking" approach for emergency mobile communications in a satellite and wireless mesh scenario, in which ad hoc and IPv6 mobility mechanisms are combined together. First we analyze mobility management aspects and IP layer protocols and then we focus on Proxy Mobile IPv6, a network-based mobility management protocol which represents the more suitable micro-mobility solution for the proposed scenario with heterogeneous networks and unmodified mobile terminals.**

Keywords: Ad-hoc Networking, Mobility Management, Proxy Mobile IPv6, Public Safety and Disaster Relief.

I. Introduction

Public Safety and Disaster Relief (PSDR) networks have traditionally been owned and managed by individual agencies (e.g. fire, law enforcement, and emergency medical services) as stand-alone networks at the state or local government levels. While these networks are designed to support critical voice services within their respective coverage areas, they are often not interoperable with each other nor do they support data services. Major disasters all around the world have repeatedly shown the limitation of existing Public Safety Communications (PSC), not able to fulfill at the same time the critical requirements of mobility, ubiquitous access, reliability, scalability, configurability and flexibility. Users of these networks could greatly benefit from a common IP-based "mobile ad-hoc networking" [1] environment in which satellite and terrestrial technologies are combined together for the development of a comprehensive end-to-end communications solution for emergency management applications.

In this work, we propose a new mobile ad-hoc satellite and wireless mesh networking approach in which IPv6 *unmodified* mobile terminals (e.g. IPv6 off-the-shelf PDA, handhelds or PC) can access to the mobile ad-hoc mesh network deployed at the disaster site, moving from the coverage of one mobile mesh router to another transparently and seamlessly. It is possible through a flexible mechanism of mobility management implemented in the mobile ad-hoc mesh network based on Proxy Mobile IPv6 (PMIPv6) [2], which is able to provide mobility support to mobile terminals that may not have a protocol stack for mobility. Thus, the mobile ad-hoc mesh network brings interoperability among equipments used by different Public Safety agencies and, thanks to its multi-hop nature, self-healing and self-configuring capabilities, it is a promising solution for a dynamic, easy to configure and scalable infrastructure at the disaster site. On the other side, local and international connectivity, as well as ubiquitous coverage of the disaster area, are provided through Vehicle Communication Gateways (VCGs). As shown in Fig. 1, thanks to the satellite and wireless interfaces, VCGs are able to connect via satellite the disaster area with headquarters, to create an inter-vehicular mobile ad-hoc mesh network in the emergency field and to provide connectivity to isolated IPv6 cells. Two types of VCGs are envisaged from a satellite interface point of view, S-UMTS vehicles operating in L or S band and nomadic DVB-RCS vehicles operating in Ku or Ka band. Each of them assumes a different role during network deployment phases that follow the hazard detection.

The rest of this article is organized as follows. In Section II, we present the proposed hybrid satellite and terrestrial system architecture for emergency mobile communications and the challenges for mobility management in such architecture. Section III presents an overview of mobility management, describing location and handoff management together with IP layer mobility management approaches. Section IV introduces a new network-based mobility management protocol, Proxy Mobile IPv6, for providing IP micro-mobility support. In Section V we analyze the suitability of PMIPv6 for creating a mobile ad-hoc satellite and wireless mesh networking for PSC. Finally, Section VI concludes the paper.

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

978-1-4244-2573-0/08/$25.00 ©2008 IEEE

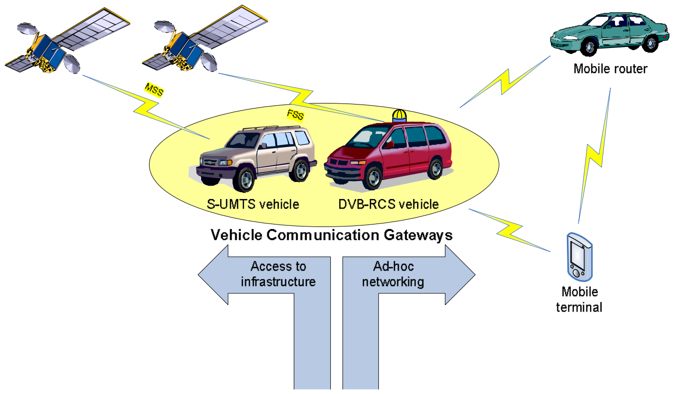

Figure 1. Vehicle Communication Gateways

II. SATELLITE AND WIRELESS MESH SYSTEM SCENARIO FOR PUBLIC SAFETY COMMUNICATIONS

A widely accepted concept in the PSDR community is to handle an emergency situation by resorting to a mobile broadband communication infrastructure that is quickly deployable at the disaster site and able to interconnect heterogeneous networks, so as to promptly support communications among the personnel of safety and emergency agencies. In [3], we have proposed a suitable IPv6-based hybrid satellite and terrestrial system architecture, shown in Fig. 2, formed by the interaction of two different types of communications:

- Vehicle-to-infrastructure (V2I) communications for providing Internet connectivity to the disaster site via satellite links;
- Vehicle-to-vehicle (V2V) communications based on ad-hoc networking, for giving connectivity to mobile terminals through the mobile ad hoc mesh network.

Since a disaster occurs, two different and consecutive phases can be identified for the network deployment of rescue teams in the disaster area. The first phase is characterized by Public Safety vehicles moving to the crisis site and reaching the most critical areas of the disaster. Although the mobile ad hoc mesh network can provide situational awareness for the nodes within its network, mobile backhaul communications capabilities are required to distribute that information to the headquarters. S-UMTS vehicles provide a mobile communications solutions through S/L band between the mobile ad hoc mesh network at the disaster field and the Internet backbone where the headquarters are situated. Thus, logistic information can be collected locally within the ad hoc mesh network, then transported via Mobile Satellite Service (MSS) and aggregated to provide a Common Operational Picture (COP) to the headquarters. S-UMTS vehicles can provide external broadband connectivity combining together and sharing the available MSS capacity.

In the second phase, once vehicles have reached critical areas, pedestrian Public Safety units start the rescue operations. Wi-Fi and ad hoc networks are created by mobile terminals and connected to the ad hoc mesh network through the closest mobile router. The mobility in the crisis field decreases in this phase. Transportable terminals, like DVB-RCS vehicles, working on-the-pause or at very low speeds, permit to benefit of high throughput, efficient bandwidth utilization and cheap capacity. The available bandwidth is very large and not much occupied and it is possible to use small antennas for terminals as Ultra-Small Aperture Terminal (USAT), able to provide multimedia data and services. In addition, S-UMTS vehicles can be used to give external connectivity to groups not reached by the mobile ad-hoc mesh network.

In both phases a key role is played by the ad hoc mesh network [4]. We propose to implement the future IEEE 802.11s standard [5], the most relevant emerging standard for mesh networking technology in the context of public safety and disaster recovery communications. Its aim is to extend the MAC protocol of 802.11 networks to support mesh functionality. Every IEEE 802.11s compliant device is required to implement the Hybrid Wireless Mesh Protocol (HWMP) [6], a path selection protocol that contains both reactive and proactive routing components. HWMP uses an adaptation of the reactive routing protocol Ad Hoc On Demand Distance Vector (AODV) [7] called Radio-Metric AODV (RM-AODV). While AODV works on layer 3 with IP addresses and uses the hop count as routing metric, RM-AODV works on layer 2 with MAC addresses and uses a radio-aware routing metric for the path selection. On the other side, the proactive component of HWMP creates proactive routing trees to mesh points connected to external networks (e.g. VCGs). HWMP well fits the proposed mobile ad hoc mesh network [3], as its reactive mechanism can be used for the discovery and maintenance of optimal routes among mesh points, while its proactive mechanism for the formation of tree structure based on VCGs to quickly establish paths to the headquarters.

The proposed hybrid system architecture needs a strong mobility management support in order to bring seamless mobility to Public Safety units. The mobility solution for this scenario has to take into account the heterogeneous environment and the challenge of providing roaming and service continuity to users coming from different agencies and providers.

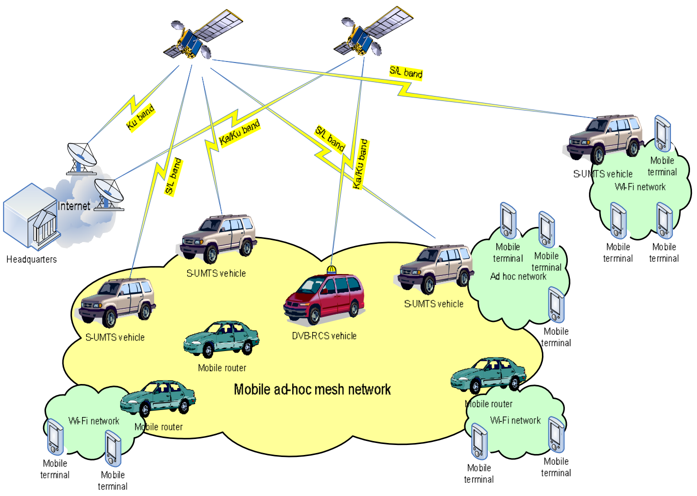

Figure 2. Hybrid satellite and terrestrial system architecture

III. Mobility Management

Mobility management [8] contains two components: location management and handoff management. Different solutions try to support mobility management in different layers of the TCP/IP protocol stack reference model. IP-based heterogeneous wireless networks can greatly benefit of a network layer solution, which provides mobility-related features at IP layer without relying on or making assumption about the underlying wireless access technologies.

A. Location Management

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

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

B. Handoff Management

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

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

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

C. IP Layer Mobility Management

In the Internet, a node is identified by an IP address that uniquely identifies its point of attachment to the Internet and packets are routed to the node based on this address. Therefore, a node must be located on the network indicated by its IP address in order to receive data. This prohibits the node from moving and remaining able to receive packets using the base IP protocol. Network layer mobility management solutions are used to manage node mobility between different domains or between different subnets inside the domain [9]. IP mobility management can be broadly classified into two schemes: *macro-mobility* and *micro-mobility*, as shown in Fig. 3.

1) Macro-mobility

Macro-mobility is the movement of mobile nodes between two subnets in two different network domains. The most known standard for IP mobility support is Mobile IP [10], which is the best and the most frequently adopted solution for supporting IP macro-mobility. Two versions of Mobile IP have been standardized on the Internet: Mobile IPv4 (MIPv4) [11] and Mobile IPv6 (MIPv6) [12].

MIPv6 involves three functional entities:

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

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

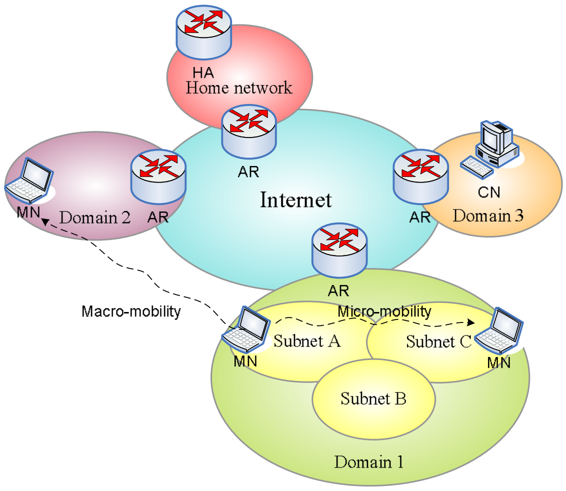

Figure 3. IP mobility schemes

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

2) Micro-mobility

Micro-mobility is the movement of MNs between two subnets within the same domain. Although MIPv6 is a mature standard for IP macro-mobility support and solve many problems such as triangle routing, security and limited IP address space, addressed in MIPv4, it still reveals some problems in the case of micro-mobility support. Hierarchical Mobile IPv6 (HMIPv6) [13] is an extension to MIPv6 to improve local mobility handling, reducing significantly the signaling and the handover delay between MN, CN and HA.

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

HMIPv6 is a *host-based* mobility management protocol, as it requires MN's participation in mobility related signalling. On the contrary, in a *network-based* mobility management approach, like in PMIPv6 [1], the serving network handles the mobility management on behalf of the MN.

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

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

IV. Proxy Mobile IPv6

The IETF has recommended a Network-based approach to Localized Mobility Management, called NETLMM, based on Proxy Mobile IPv6. PMIPv6 is an extension of MIPv6 as it reuses its signaling and many concept such as HA functionalities. As PMIPv6 is designed to provide network-based mobility management support to a MN in a topologically localized domain, its innovative point is that it exempts the MN from participating in any mobility-related signaling and proxy mobility agents 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 HoA on any access network. The serving network assigns a unique home network prefix to each MN whenever they move within the PMIPv6 domain. Thus, for MNs the entire PMIPv6 domain appears as their home network.

As shown in Fig. 4, this mechanism is possible thanks to two core functional entities in the NETLMM infrastructure:

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

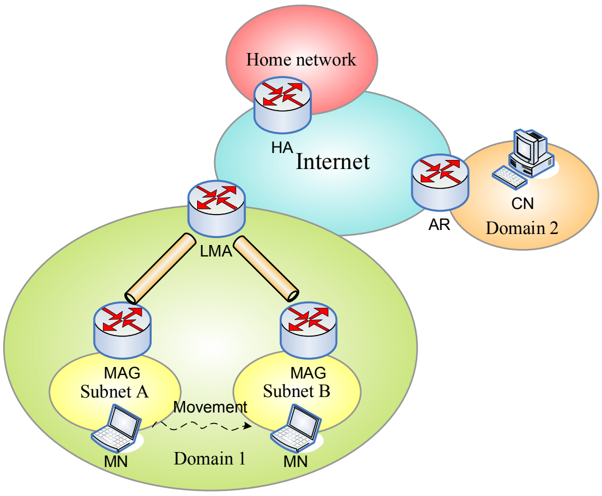

Figure 4. Overview of PMIPv6

A. *PMIPv6 Signaling*

The main steps in the PMIPv6 mobility management scheme are described hereafter and shown in Fig. 5:

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

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

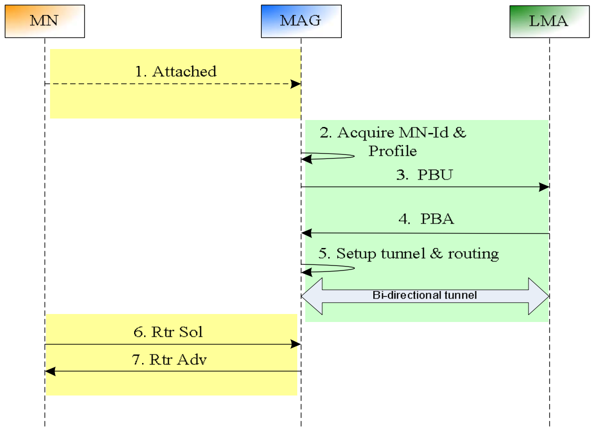

Figure 5. Message flow in PMIPv6

V. Analysis of Mobility Solutions for the Satellite and Wireless Mesh System Architecture

To demonstrate the efficiency of PMIPv6 on a quantitative point of view, we have analyzed the handover latency [14] in the hybrid satellite and terrestrial system architecture under different mobility management mechanisms. We have restricted the analysis among:

- MIPv6, as a macro-mobility approach;
- HMIPv6, as a micro-mobility approach with host-based mechanism;
- PMIPv6, as a micro-mobility approach with network-based mechanism.

Figure 6 provide a simplified model of the system architecture with the three mobility mechanisms. LMA and MAG are used for PMIPv6, while MAP for HMIPv6.

Generally, IP handover latency T_{HO}, the most critical factor for all-IP mobile networks, is expressed as

$$T_{HO} = T_{MD} + T_{DAD} + T_{AAA} + T_{REG}$$

where T_{MD} represents the movement detection delay, T_{DAD} the address configuration delay, T_{AAA} the delay due to AAA procedure and T_{REG} the location registration delay.

In order to calculate them, we need to define the following delays, as the time required for a packet to be sent between two different entities:

- $t_{MN\text{-}AP}$, the delay between MN and AP (Access Point);
- $t_{AP\text{-}AR}$, the delay between AP and AR/MAG;
- $t_{AR\text{-}LM}$, the delay between AR/MAG and MAP/LMA;
- $t_{AR\text{-}HA}$, the delay between AR/MAG and HA;
- $t_{AR\text{-}CN}$, the delay between AR/MAG and CN;
- $t_{HA\text{-}CN}$, the delay between HA and CN.

As regards the registration delay T_{REG}, in the case of MIPv6 with route optimization, it is calculated as the sum of HA registration delay, CN registration delay and the delay for Return Routability (RR). It can be expressed as follows:

$$\begin{aligned}
&T_{REG}^{MIPv6} = 2\left(t_{MN-AP} + t_{AP-AR} + t_{AR-HA}\right) \\
&+ 2\left(t_{MN-AP} + t_{AP-AR} + t_{AR-CN}\right) \\
&+ 2\left(t_{MN-AP} + t_{AP-AR} + t_{AR-HA} + t_{AH-CN}\right) \\
&= 6\left(t_{MN-AP} + t_{AP-AR}\right) + 4t_{AR-HA} + 2\left(t_{AR-CN} + t_{AH-CN}\right)
\end{aligned}$$

As HMIPv6 is designed for micro-mobility, the registration delay is reduced compared to MIPv6 because only MAP registration delay is required and satellite links are not involved in the process. T_{REG} can be expressed as follows:

$$T_{REG}^{HMIPv6} = 2\left(t_{MN-AP} + t_{AP-AR} + t_{AR-LM}\right)$$

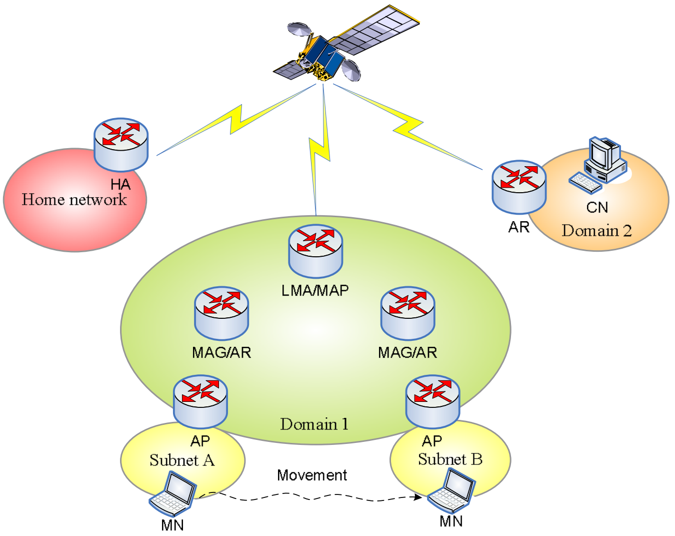

Figure 6. Simplified hybrid system architecture with mobility schemes

Finally, in the case of PMIPv6, T_{REG} is due only to the registration delay between the MAG and the LMA and the packet transmission delay from the MAG and the MN, so it can be expressed as follows

$$T_{REG}^{PMIPv6} = 2t_{AR-LM} + t_{MN-AP} + t_{AP-AR}$$

As regards T_{MD} and T_{AAA}, we can easily assess that they are all the same for the three protocols, while T_{DAD} involves only MIPv6 and HMIPv6, as PMIPv6 needs DAD procedure only when the MN enters for the first time the PMIPv6 domain. It is evident, already from the comparison of T_{REG} in the three protocols, that PMIPv6 guarantees reduced handover latency and is able to provide better performances for the mobility of pedestrian Public Safety units at the disaster site.

After an accurate analysis of mobility management mechanisms and in particular IP layer mobility schemes, it is clear that PMIPv6 is the best mobility solution for the proposed IPv6-based hybrid system architecture described in Section II. Thanks to PMIPv6 special features, the mobile ad-hoc satellite and wireless mesh networking approach supports unmodified MNs, allowing different Public Safety agencies to use off-the-shelf MNs without any software update for IP mobility support, and any type of wireless link technology, as there is no need for any wireless link specific information for basic routing management.

VCGs and mobile routers – the mesh entities composing the mobile ad-hoc mesh network – can assume LMA and MAG functionalities in order to create a PMIPv6 domain at the crisis area, to which IPv6 unmodified mobile terminals coming from different rescue teams can have access and be easily managed. In this way, seamless connectivity can be guaranteed for broadband communications inside the disaster area and with the headquarters via satellite links.

VI. Conclusion

This article has presented a mobile ad-hoc satellite and wireless mesh networking approach designed for an emergency scenario, in which the full mobility of rescue teams at the disaster site represents one of the major requirements for an emergency communication system. The combination of satellite and wireless mesh networks guarantee broadband communications in areas where no infrastructure is available, while the combination of ad hoc mobility together with IPv6 mobility mechanisms gives seamless mobility in the disaster site to Public Safety units coming from different governmental organizations.

The proposed self-healing and self-configuring wireless mesh infrastructure deployed in the emergency area is based on the new emerging standard IEEE 802.11s for PSDR communications, where ad hoc mobility scheme is provided by the hybrid routing protocol HWMP. The most important IPv6 mobility mechanisms have been presented as possible candidates for our scenario. Among them we have identified PMIPv6 as the more suitable localized mobility management protocol solution under deployment and performance perspectives. PMIPv6 can be used in IP heterogeneous wireless networks with unmodified MNs, it is able to efficiently use wireless resources and to reduce handoff latency.

References

[1] C. E. Perkins, “Ad Hoc Networking”, Addison-Wesley, 2001.

[2] S. Gundavelli et al., “Proxy Mobile IPv6”, IETF Internet draft, draft-ietf-netlmm-proxymip6-18.txt, May 2008, work in progress.

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

[4] 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.

[5] IEEE unapproved draft IEEE P802.11s/D1.09, “Draft Standard for Information Technology - Telecommunications and Information Exchange between Systems - LAN/MAN Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment: Mesh Networking”, Mar. 2008.

[6] A. Joshi et al., “HWMP specification”, IEEE 802.11-06/1778r1, November 2006.

[7] C. Perkins, E.Royer and S. Das, “Ad hoc On-demand Distance Vector (AODV) Routing”, IETF RFC 3561, July 2003.

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

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

[10] C. Perkins, “Mobile IP, Design Principles and Practices”, Addison-Wesley, 1998.

[11] C. Perkins, “IP Mobility Support for IPv4”, IETF RFC 3344, Aug. 2002.

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

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

[14] K. Kong et al., “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.