Scalable Proxy Mobile IPv6
For Heterogeneous Wireless Networks

Huu-Nghia Nguyen
Mobile Communications Department
Eurecom Institute
2229 Route des Crêtes, Sophia Antipolis, France
+33 (0)4 93 00 82 38
Huu-Nghia.Nguyen@eurecom.fr

Christian Bonnet
Mobile Communications Department
Eurecom Institute
2229 Route des Crêtes, Sophia Antipolis, France
+33 (0)4 93 00 81 08
Christian.Bonnet@eurecom.fr

ABSTRACT

This work uses a cluster-based approach to provide scalability for Proxy Mobile IPv6 in large heterogeneous wireless network. We also propose an enhanced network-based IP-layer movement detection mechanism which allows the network to detect the attachment and the movement of each Mobile Node independently from the access technologies, without any special software support from Mobile Nodes. We implement these extensions on top of Mobile IPv6 for Linux (MIPL) v2.0. An evaluation of Proxy Mobile IPv6 in a cluster based Wireless Mesh Network is provided as a use case: we construct a virtual IPv6 Wireless Mesh Network using User-mode Linux (UML) ad Ns-2 Emulation and provide some early qualitative results to prove the correctness and the advantages of the proposals.

Categories and Subject Descriptors

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

General Terms

Design, Experimentation, Standardization.

Keywords

Proxy Mobile IPv6, Network Based Mobility Management, Mobility, Heterogeneous Access, MIPL, UML.

1. INTRODUCTION

Proxy Mobile IPv6 (PMIPv6) is currently standardized by IETF for network-based localized mobility management in IP networks, especially as a solution for inter-access system handover between 3GPP and non-3GPP [1][2][3]. PMIPv6 basically requires changes only to edge routers; the serving network is regarded as an *edge domain* within which the MN acquires and keeps the same IP address while moving. As PMIPv6 requires no modification to the IPv6 stack of the MN, it is very promising to support mobility service to a wide range of users. However, as all the intelligence is delegated to the network, the high availability becomes questionable and requires a solution for scalability in large scale access networks.

We therefore consider here a cluster-based architecture in which the access network is divided into clusters. Each cluster contains a Cluster Head (CH) that has complete knowledge about group membership and link state information in the cluster. Access Routers (ARs), control heterogeneous radio access technologies. The CH and ARs are situated at the edge of the network. The backhaul link between CH and ARs can be wireline or wireless. The cluster formation process is out of scope of the paper.

We extend Proxy Mobile IPv6 to support mobility of MN having standard IPv6 stack in such a cluster-based heterogeneous wireless network. To support a heterogeneous environment composing of different access technologies, we introduce an enhanced network-based IP-layer movement detection mechanism. It allows the network to detect the attachment and the movement of each MN independently from the access technologies and requires no special support from the MN. Upon any attachment or detachment of a Mobile Node (MN), the AR informs the CH on behalf of the MN to maintain the reachability of the MN while it is moving. Here, MNs are expected to maintain their IPv6 addresses allocated from their home link while moving within the PMIPv6 domain.

The paper is organized as follows: Section 2 describes related work including Proxy Mobile IPv6 and existing movement detection mechanisms. Section 3 concentrates on our framework with a brief description of cluster-based architecture an extended Proxy Mobile IPv6 and an enhanced network-based IP-layer movement detection. Section 4 describes Eurecom's implemented software architecture of Proxy Mobile IPv6 and the virtual IPv6 wireless testbed using User-mode Linux and Ns-2 Emulation. It also provides some qualitative results. Finally, section 5 concludes the paper and provides perspectives for future work.

2. RELATED WORK

2.1 Proxy Mobile IPv6 (PMIPv6)

PMIPv6 is designed to provide network-based mobility management to MNs having standard IPv6 stack. The new principal functional entities of PMIPv6 are the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA). The main role of the MAG is to detect the MN's movements and initiate mobility-related signaling with the LMA on behalf of the MN. The serving network assigns a unique home network prefix to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain. From the perspective of the MN, the entire PMIPv6 domain appears as its home network. The MN can configure an address using any address configuration mechanism that is allowed in the PMIPv6 domain. Here we assume a Stateless Address Configuration [4].

Figure 1 shows a typical PMIPv6 handover process of an IPv6 MN. Once a MN enters the PMIPv6 domain and attaches to a MAG, the MAG must identify the MN and acquire the Mobile

Node Identifier (MNID). If the MAG determines that the MN is authorized for the network-based mobility management service, it must start the Location Registration procedure on behalf of the MN to maintain the reachability of the MN. The MAG sends Proxy Binding Update (PBU) message to the LMA and waits for the Proxy Binding Acknowledgement (PBA) message from the LMA. At the end of this Location Registration procedure, the MAG and the LMA establish a bidirectional tunnel and update the routing entry to forward the MN traffic through the bidirectional tunnel. The soft state of a MN at the LMA ad MAGs is maintained in a Binding Cache entry which can be accessed using the MNID as search key. Such information associates a MN with its serving MAG, and allows the relationship between the MAG and the LMA to be maintained.

At any point, the MAG detects that the MN has moved away from its access link, or if it decides to terminate the mobility session, it should start the Location Deregistration procedure by sending a Proxy Binding Update message to the LMA with the lifetime value set to zero.

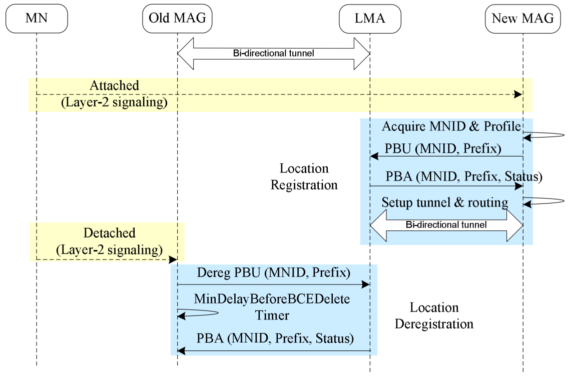

Figure 1. Proxy Mobile IPv6 Sequence Diagram

The basic PMIPv6 protocol doesn't consider the route optimization for communication between MNs in the same PMIPv6 domain. Besides, a centralized LMA is a single point of failure in a large scale network. If the LMA crashes for some reason, the mobility service in the whole network is disrupted.

2.2 Movement Detection Mechanisms

An important aspect of any mobility protocol is the movement detection. Different movement detection mechanisms have been proposed for Mobile IP. However these are host-based and require special supports from the MN. For Proxy Mobile IPv6, the MAG must be responsible for the movement detection; this requires a network-based movement detection mechanism. The hints for movement detection can be the Link-Layer Event Notifications, Traffic Monitoring Events or DNAv6 [5]. Table 1 compares advantages and the drawbacks of different approaches:

Table 1. Comparison of Movement Detection Approaches

Hints	Advantages	Drawbacks
Traffic Monitoring Events	Independent from access technologies.	Processing overhead at MAGs.
Link-Layer Events	Accurate and Rapid.	Dependent on access technologies.
DNAv6	Independent from access technologies.	Dependent on MN

A traffic monitoring based mechanism only works fine when there is uplink traffic from the MN to the network. The mechanism can be independent from the access technology but causes processing overhead at MAGs because MAGs must inspect every packet on the link. A link-layer event notification mechanism can be accurate and rapid. However in a heterogeneous environment, it depends on particular access technologies, requires a lot of modifications either on the network side or on the terminal side and therefore the deployment becomes difficult. DNAv6 also provides an IP-layer movement detection independent from access technology. DNAV6 uses the fact that the MN will send ICMPv6 message, e.g. Neighbor Solicitation (NS), and/or Router Solicitation (RS), when it move to a new link, which depends on how the MN it self detects the attachment and detachment.

An enhanced network-based IP-layer movement detection is a must to complement existing mechanisms.

3. FRAMEWORK

This framework extends PMIPv6 to provide scalability in large scale heterogeneous wireless network in a cluster-based manner. In this architecture, the MAG typically runs on the AR and the LMA runs on the CH. Therefore AR and CH can be interpreted as MAG and LMA and vice versa.

3.1 Cluster-based Architecture

The cluster-based architecture consists of clusters (see Figure 2). Each cluster should have one and only one CH which has the LMA functionality and complete knowledge about group membership and link state information in the cluster. A relay router connects two adjacent clusters. ARs control heterogeneous radio access technologies and provide access to MNs. The backhaul between the CH and the ARs in the infrastructure can be wireline or wireless. The MN, which attaches to the AR, can be connected through the infrastructure to all other routers. The MN therefore can communicate with other mobile Correspondent Nodes (CNs) through ARs as well as with CNs on the Internet through CHs.

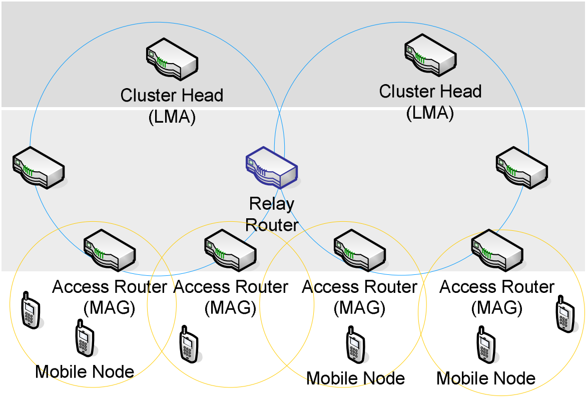

Figure 2. Scalability with Cluster-based Architecture

This type of architecture is also applied in Wireless Mesh Networks. In the case of wireless backhaul, we have a cluster based Wireless Mesh Network which can minimize the updating overhead during topology change due to mobility of mesh nodes.

If route optimization is considered, the traffic from one source MN to another destination MN should be able to pass through the relay router without passing through CHs. Detail on route optimization is out of scope of this paper.

3.2 Extended Proxy Mobile IPv6

The standard Proxy Mobile IPv6 provides a natural solution for communication between the MN and the CN outside the PMIPv6 domain. It also works fine for intra-cluster communication between two MNs in the same cluster and intra-mobility. However for inter-cluster communication, when the MN and the CN belong to different clusters in the same PMIPv6 domain, one fundamental issue is that of locating the serving MAG or the serving LMA of the CN. As for inter-cluster mobility, when the MN moves from one cluster to a new cluster, it is necessary to activate the Location Deregistration procedure in the old cluster to maintain up-to-date routing information.

When establishing the communication between a MN and a CN belonging to different clusters, the serving MAG of the MN needs to know the serving MAG or the serving LMA of the CN. This issue is expressed as the problem of mapping a CN address into its serving MAG address or serving LMA address. This issue also arises in the case of route optimization in which the traffic could be forwarded directly from a source MAG to a destination MAG without passing through LMAs.

We propose a new couple of messages: Proxy Binding Request (PBReq) and Proxy Binding Response (PBRes) and a new mobility header option, named Serving MAG Address option (see Figure 3).

Payload Proto	Header Len	MH Type = 8	Reserved
Checksum		Sequence #	
Mobility options			

Payload Proto	Header Len	MH Type = 9	Reserved
Checksum		Sequence#	
Mobility options			

Type = 0x0B	Option Len = 18	Reserved
MAG Address		

Figure 3. New messages and options

The Proxy Binding Request message structure is similar to that of Binding Refresh Request of Mobile IPv6 [6] except that the MH Type takes a value of 8 instead of 0. The value should be registered at IANA. This message is sent by the LMA to an All-LMA multicast group, an All-MAG multicast group, or to a centralized LMA to find which MAG is serving a mobile CN. The Proxy Binding Response message has similar structure as that of Proxy Binding Update except that the MH Type takes a value of 9. It responses to a PBReq and contains Serving MAG Address option which is a mandatory.

The establishment for inter cluster communication is described as in Figure 4. Any NS message for Address Resolution (ARP) will be inspected by the edge entities which are either MAG or LMA. As the CN address is stored in the target field, these entities can lookup the target in its binding cache to check if it is the serving entity of the CN.

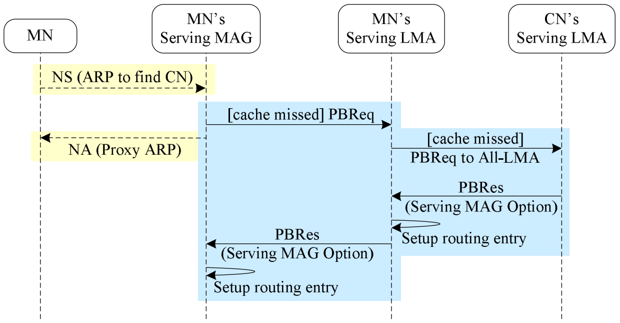

Figure 4. Inter-cluster communication establishment

If the serving MAG of the MN doesn't have any information about the target which belongs to the same PMIPv6 domain, i.e. cache missed, the MAG assumes that the CN is away from its home link and will send a PBReq message to the serving LMA of the MN. The MAG will also perform Proxy ARP for the CN. If the LMA doesn't have any information about the target, it must send a PBReq to All-LMA multicast address. The serving LMA of the CN will be able to answer with a PBRes carrying a Serving MAG Address Option. Later, the serving LMA of the MN can then setup a routing entry pointing to a pre-established tunnel to the serving LMA of the CN. If route optimization is considered, a path between the serving MAG of the MN and the serving LMA of the CN can be established. As for intra-cluster communication, the Serving MAG Address Option can help to set up a direct path from the serving MAG of the MN and the serving MAG of the CN for the route optimization. Once the path is set up, the traffic between the MN and the CN can be delivered.

When the MN moves from one cluster to a new cluster, the old LMA may not be aware about the changes, the new LMA can send a PBRes message to All-LMA multicast address. This message helps the old LMA to activate the Location Deregistration procedure if necessary, and helps other LMAs to maintain up-to-date routing information to keep on-going session. Especially, this mechanism becomes more useful when route optimization is considered.

3.3 Enhanced Network-based IP-layer Movement Detection

We propose here an algorithm for network-based IP-layer movement detection in heterogeneous wireless environment.

3.3.1. Precondition. In standard PMIPv6, the MN maintains an IP address that is unchanged within the PMIPv6 domain and is used for communications. This address is a global routable IP address and is referred in this paper as PMIPv6 address.

In our proposal, each AR broadcast Router Advertisements (RAs) containing two prefixes: (i) a global prefix P which is assigned to each MN (per-MN prefix) or is shared by all MNs (multi-link subnet with shared prefix) and (ii) a site-scope prefix P*. The global PMIPv6 address is configured from the global prefix P while the temporary site-scope IP address is configured from the site-scope prefix P*.

Whenever the MN moves to a new link, it configures a new temporary address and deletes the previous temporary address when its preferred lifetime is expired. The NS message in Duplicate Address Detection (DAD) process for this new temporary address is used as a hint for the network attachment detection. The following assumptions are taken into account.

Assumption 1: the MAG could extract the MNID, e.g. the MAC address or public key, from any ICMPv6 messages sent by the MN, e.g. Neighbor Solicitation (NS), Router Solicitation (RS), and Neighbor Advertisement (NA). Besides, there exists a bidirectional conversion between the MNID and the PMIPv6 address. Given a PMIPv6 address, we can infer the MNID and vice versa.

Assumption 2: If multiple addresses are active for the same interface, depending on the destination address, the source address of the communication is selected according to the Source Address Selection algorithm [7].

The first assumption allows the MAGs to detect the hints for network attachment of a MN when the MAG receives an ICMPv6 message. The second assumption ensures that the MN always prefer the PMIPv6 address for communications even when multiple addresses co-exist and therefore global prefix P and temporary site-scope prefix P* could be broadcasted by the AR on the same link.

3.3.2. Algorithm description. With the above precondition, each MN will have two IPv6 addresses: one is PMIPv6 address, which is a global IPv6 address and is unchanged within the PMIPv6 domain; another is the temporary address, which is a site-scope IPv6 address and is reconfigured whenever the MN moves from the old AR to a new AR. Here is the event-driven pseudo code:

```
on receiving a NS(target) for DAD
begin
  Extract target
  Compute MNID = get_MNID(NS)
  Compute PMIPv6 address = get_Address(MNID)
  if there is no PMIP binding entry for the MNID
  begin
    if get_Prefix(target) = P*
    begin
      Send NS (with target= PMIPv6 address) for ARP
      Create a "temporary" PMIP binding entry with a lifetime T*
    end
    else if get_Prefix(target) = P
      output Attachment Event (MNID)
  end
end
on receiving a NA(target) which replies the NS for ARP
begin
  Extract target
  Compute MNID=get_MNID(NA)
  if there exists a "temporary" PMIP binding entry for the MNID
    if get_Address(MNID) = target
      output Attachment Event (MNID)
end
on Attachment Event (MNID)
begin
  Start Location Registration Procedure (MNID)
  if there exists a "temporary" PMIP binding entry for the MNID
    Set the PMIP binding entry to "permanent"
  else if there is no PMIP binding entry for the MNID
    Create a "permanent" PMIP binding entry
end
on T* expired
begin
  Delete the associated "temporary" PMIP binding entry
end
```

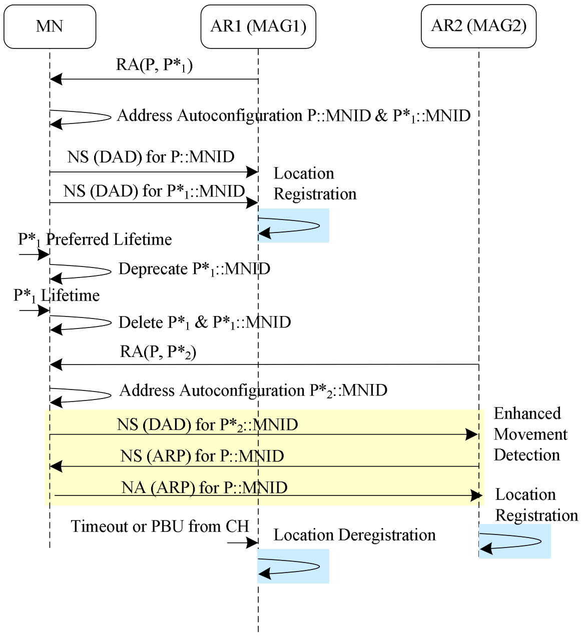

Figure 5. Example of Enhanced Network-based IP-Layer Movement Detection

Thanks to the temporary site-scope prefix P* in Router Advertisement messages, sent periodically by the AR, the MN configures temporary site-scope address and activate DAD procedure by sending an NS message. This message will be used as a hint for the new AR to verify if the MN is really attached to it. The new AR activates the Neighbor Unreachability Detection (NUD) procedure by sending NS for address resolution with the target set to PMIPv6 Address. It also creates a temporary binding cache entry for the MN with a short life time and waits for the NA. If the MN has really moved inside the coverage of the new AR and associate with the new AR at the link layer, it must be able to answer this NS with an NA as a default behavior of Neighbor Discovery for IP Version 6 (NDPv6) [8]. The NA message, with the PMIPv6 address as the target, confirms the attachment of the MN and activates the Location Registration procedure.

Figure 5 shows a sequence diagram of a typical handover scenario, with enhanced network-based IP-layer movement detection, in which the MN first comes to the PMIPv6 domain (using a shared prefix) and attaches to the AR1. Later, the MN moves away from AR1 and attaches to the AR2.

4. IMPLEMENTATION AND EVALUATION

We implemented the scalable Proxy Mobile IPv6 under Linux kernel 2.6.20, and setup a virtual IPv6 Wireless Mesh Network using User-mode Linux [9][10] and Ns-2 Emulation [11].

4.1 Proxy Mobile IPv6 Implementation

We implemented Proxy Mobile IPv6 on top of Mobile IPv6 for Linux (MIPL) v2.0 [12]. All the basic bricks of MIPL are reused in an efficient way as shown in Figure 6. In MIPL v2.0, Mobile IPv6 is implemented using multi threads: One thread for handling the ICMPv6 messages, one thread for handling Mobility Header messages, one thread for handling tasks and time events, etc.

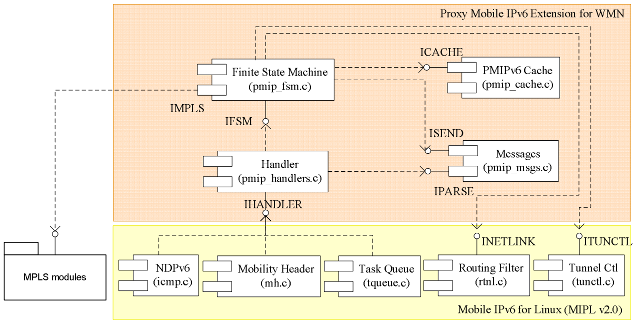

Figure 6. Proxy Mobile IPv6 Software Architecture

To support Proxy Mobile IPv6, we extend these elements and implement handlers for all necessary messages and events. All ICMPv6 messages or Mobility Header messages are parsed as the input to the finite state machine, which is the heart of the system. This finite state machine makes appropriate decisions and controls all other elements to provide a correct predefined protocol behavior. As Proxy Mobile IPv6 implementation is built on top of MIPL version 2.0, it could be later integrated in MIPL easily and grows inline with the standards as well as MIPL source code.

4.2 Virtual IPv6 Wireless Mesh Network

We consider here the application of PMIPv6 in a cluster based Wireless Mesh Network as a use case of our extensions. Wireless mesh networks (WMNs) are multi-hop wireless networks with self-healing and self-configuring capabilities. These features, plus the ability to provide wireless broadband connectivity, make WMNs a promising solution for ubiquitous Internet access and a wide range of applications [13]. In order to keep the results closest to the real experiment, we used a virtualization based testbed, using a combination of User-mode Linux (UML) and Ns-2 Emulation, which would allow migrating to the real testbed with just insignificant efforts.

UML is a Linux kernel which is compiled to run as a virtual machine on a Linux host. The virtual machine, called the guest to distinguish with the real host machine, can be assigned a guest root file system and other virtual physical resources different from the host machine. A UML virtual machine requires a guest kernel and a guest root file system. The guest root file system of an UML is stored in a file on the real host machine.

The Ns-2 emulation feature is used to emulate the wireless environment. It can grab packets from a virtual machine with real IPv6 stack, pass them through a simulated wireless network, and then inject them back into the destination virtual machine.

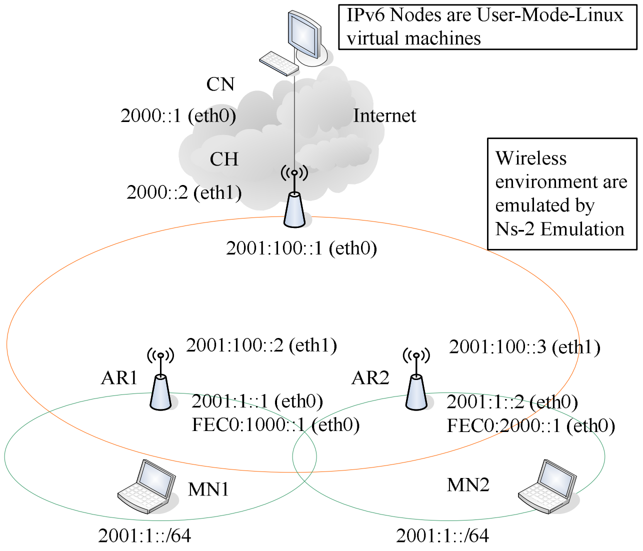

Figure 7. Virtual Wireless Mesh Testbed

Figure 7 shows the virtual Wireless Mesh testbed. The topology is generated by Virtual Network User-mode Linux (VNUML) [14]. A Linux kernel 2.6.20 is compiled under User-mode architecture to serve as a guest kernel for virtual machines. Scenarios are defined and automated with Tcl language which is a part of Ns-2 Emulation. The virtual testbed in this early phase composes of one cluster with one CH, two routers AR1 and AR2. A CN, positioned in the Internet, is connected directly with the CH. MN1 and MN2 don't have any specific software for mobility management. Initially, MN1 is attached to AR1 and MN2 is attached to AR2. As any type of access technology is allowed, we consider here IEEE 802.11 for simplification. MNs' addresses are configured through IPv6 Stateless Address Auto Configuration. We use a shared-prefix model with a shared prefix of 2001:1::/64. Two site-scope prefixes FEC0:1000::/64 and FEC0:2000::/64 are used for enhanced network-based movement detection procedure. AR1 and AR2 are configured with Router Advertisement daemons (RADVD) which broadcast RAs on their eth0 interface. RAs contain two prefixes and are sent periodically every 1s. Iperf is used to generate tcp/udp traffic while ping6 is used to generate ICMP traffic.

4.3 Qualitative Results

Different test scenarios are defined and are carried out to verify the correctness of the framework. In this early phase, only intra-cluster scenarios are validated (see Table 2).

Table 2. Test Scenarios

Scenarios	Descriptions	Results
Attachment Detection	MN1 and MN2 come inside AR1 coverage	Successful registration of MN1/MN2 in both AR1& CH
Detachment Detection	MN1 or MN2 turns down the interface (or moves away from AR1).	The cache entry is deleted in both AR1 and CH.
Intra-link Communication	MN1, MN2 are attached to AR2. Traffic between MN1 and MN2	MN1 can communicate with MN2
Intra-cluster Communication	MN1 is attached to AR1. MN2 is attached to AR2. Traffic between MN1 and MN2	The traffic is encapsulated through AR1-CH and AR2-CH tunnels.
Mobility and Movement Detection	MN1 moves from AR1 to AR2. The PMIPv6 address of MN1, which is configured with the PMIPv6 prefix, is kept unchanged. MN1 configures new temporary address, and deletes the old temporary address.	AR2 detects the attachment and starts the registration procedure. AR1 detects the detachment and starts the deregistration procedure. Session continuity is assured. On-going sessions can continue

5. CONCLUSION AND PERSPECTIVES

We extended PMIPv6 to provide scalability to PMIPv6 in large heterogeneous wireless network in a cluster-based manner. The framework can support mobility in large scale network to MNs having standard IPv6 stack without any support from MNs. A new enhanced network-based IP-layer mechanism was proposed. This movement detection mechanism allows detecting the attachment and the movement of each MN independently from the access technologies and requires no special support from the MN. We implemented and deployed the PMIPv6 protocol in a virtual IPv6 Wireless Mesh Network testbed and provide some qualitative results to prove the correctness and the advantages of the framework. The proposed framework is suitable for different applications. One of current applications is to deploy rapidly a mobile and wireless communication environment in form of a Wireless Mesh Network in Integrating Communications for enhanced environmental risk management and citizens safety (CHORIST) project [15] which proposes solutions to increase rapidity and effectiveness of interventions following natural hazards and industrial accidents, in order to enhance citizens' safety and communications between rescue actors. We provide a realistic and practical framework for future advanced mobile networking researches. Our future work will concentrate on inter-cluster communication, on route optimization as well as on QoS support. We also foresee the use of MPLS instead of IP-in-IP. Performance evaluation with quantitative results will also be realized.

6. ACKNOWLEDGEMENTS

Eurecom Institute's research is partially supported by its industrial members: BMW, Bouygues Télécom, Cisco Systems, France Télécom, Hitachi Europe, SFR, Sharp, STMicroelectronics, Swisscom, Thales. Authors are also thankful to Hussain Ahmed, Paul Marie Joseph Venmani Daniel Philip, Lamia Romdhani (Eurecom Institute) and Hirokazu Naoe (SHARP) for help and valuable advices.

7. REFERENCES

[1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6,” Internet draft (work in progress), May 2008.

[2] J. Kempf, “Goals for network-based localized mobility management (netlmm),” RFC 4831, April 2007.

[3] J. Kempf, “Problem statement for network-based localized mobility management,” RFC 4830, April 2007.

[4] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,” RFC2462, December 1998.

[5] J. Kempf, S. Narayanan,E. Nordmark, B. Pentland and JH. Choi, “Detecting Network Attachment in IPv6 Networks (DNAv6),” Internet draft (work in progress), February 2008.

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

[7] R. Draves, “Default Address Selection for Internet Protocol version 6 (IPv6),” RFC 3484, February 2003.

[8] T. Norten, E. Nordmark and W. Simpson, “Neighbor Discovery for IP Version 6,” RFC2461, December 1998.

[9] User Mode Linux Home Page, http://user-mode-linux.sourceforge.net

[10] Nguyen, Huu Nghia;Bonnet, Christian, “Practical and unified process for developing the future Mobile Internet with Simultaneous Access (MISA),” Research Report RR-08-211, February 2008.

[11] Daniel Mahrenholz and Svilen Ivanov, "Real-Time Network Emulation with ns-2," *Proceedings of The 8-th IEEE International Symposium on Distributed Simulation and Real Time Applications, Budapest Hungary*, October 21-23, 2004.

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

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

[14] Virtual Network User Mode Linux Home page http://www.dit.upm.es/vnumlwiki/index.php/Main_Page.

[15] Chorist Project Home Page, http://www.chorist.eu.