Title Page

- Title of the article: Extended Proxy Mobile IPv6 for Scalability and Route Optimization in Heterogeneous Wireless Mesh Networks

- Authors' Name, Position Title, Academic Degree, Departments, Institutions, Mailing Address, and Telephone Number

1) First author: Huu-Nghia Nguyen, MSc degree, Ph.D. Student, Mobile Communications Department, Eurecom, Huu-Nghia.Nguyen@eurecom.fr, +33493008238

2) Second author: Christian Bonnet, MSc degree, Professor and Head of Mobile Communications Department, Mobile Communications Department, Eurecom, Christian.Bonnet@eurecom.fr, +33493008108

3) Third author: Giuliana Iapichino, MSc degree, Ph.D. Student, Mobile Communications Department, Eurecom, Giuliana.Iapichino@eurecom.fr, +33493008252

Extended Proxy Mobile IPv6 for Scalability and Route Optimization in Heterogeneous Wireless Mesh Networks

Huu-Nghia Nguyen, Christian Bonnet, Giuliana Iapichino
Mobile Communications Department
Eurecom
{name.surname}@eurecom.fr

Abstract

This work proposes extensions to Proxy Mobile IPv6 (PMIPv6) for providing scalability and route optimization features to heterogeneous Wireless Mesh Networks (WMNs). WMNs are multi-hop wireless networks with self-healing and self-configuring capabilities. PMIPv6 is designed to provide network-based mobility management to Mobile Nodes (MNs) having standard IPv6 stack. Applying PMIPv6 and its proposed extensions to WMNs can make them a promising solution for ubiquitous Internet access and a wide range of applications, as Public Safety and emergency communications.

A cluster-based approach is proposed for federating the mesh routers into different PMIPv6 domains, each of them managed by a cluster-head. All mesh routers can act as access routers for "unmodified" MNs. No assumptions are made on MNs' access technology. Taking into account such cluster-based architecture, inter-clusters communication and mobility aspects with route optimization have been tested in our virtual IPv6 WMN. We have developed a virtualization-based testbed, using a combination of User-mode Linux (UML) and Ns-2 Emulation, with the scope of being as close as possible to real experimentation results and to easily migrate to the real testbed in the near future. A preliminary measurement on the signaling cost in terms of delay is also provided.

The obtained results show that PMIPv6, together with scalability and route optimization features, can improve the mobility issues of WMNs and this work can represent a good solution for crisis management and emergency scenarios.

1. Introduction

WMNs are able to dynamically self-organize and self-configure [1]. The nodes in a WMN automatically detect neighbor nodes and establish and maintain network connectivity in an ad hoc fashion. The self-configuring nature of WMNs allows easy and rapid network deployment. WMNs also have the ability to dynamically adapt to changing environments and to essentially self-heal in case of node or link failures. If one mesh link becomes unavailable, traffic is automatically redirected via an alternative path. Unlike in existing point-to-point radio systems, mesh networks are inherently redundant with no single point of failure. Moreover, WMNs are able to operate in a heterogeneous environment with a variety of technologies. The result is that WMNs have a high level of robustness and fault tolerance. These features, together with the high reliability and the quick deployment, make WMNs a promising solution for ubiquitous Internet access and a wide range of applications.

A WMN generally consists of a set of mesh nodes that interconnect with each other via wireless medium to form a wireless backbone. Some or all of the mesh nodes also serve as access points for mobile users under their coverage. One or more mesh nodes can have wired/wireless connections to the Internet and function as gateways. Compared to traditional wireless LANs, the main feature of wireless mesh networks is their multi-hop wireless backbone.

We extend PMIPv6 to support the seamless mobility in heterogeneous Wireless Mesh Networks. Our design addresses two main issues: scalability and route optimization. Besides, it inherits the feature of PMIPv6 which can support mobility to MNs having unmodified IPv6 stack and allow reducing the flooding signaling traffic during the registration process and during the dynamic route discovery process. The term “heterogeneous” can be interpreted in the sense that: (i) the radio access technology of the backhaul link can be different from the one used by the access link; (ii) access links can have different radio access technologies simultaneously and a MN can perform intra-technology (or inter-technology, if MNs are equipped with multiple interfaces) handover thanks to PMIPv6 protocol.

For the scalability, we consider a cluster-based architecture in which the WMN is divided into clusters that could minimize the updating overhead for topology change due to the mobility of mesh nodes and MNs. Each cluster, containing a Cluster Head (CH), has complete knowledge about group membership and link state information in the cluster. The CH is often elected in the cluster formation process. The other nodes within a cluster, called Access Routers (ARs) in this paper, have reduced mobility and control heterogeneous radio access technologies. A relay router connects two adjacent clusters. All nodes in the backhaul are interconnected through OLSR routing protocol.

A MN, attached to an AR, can communicate with a Correspondent Node (CN) located either in the WMN, or in the Internet through the CH. The MN can keep its on-going session while moving between ARs within the mesh. We also consider Route Optimization (RO) for MN and CN belonging to different clusters. The traffic can be routed from the AR to the relay router, reaching the other AR without passing through CHs (see Figure 1).

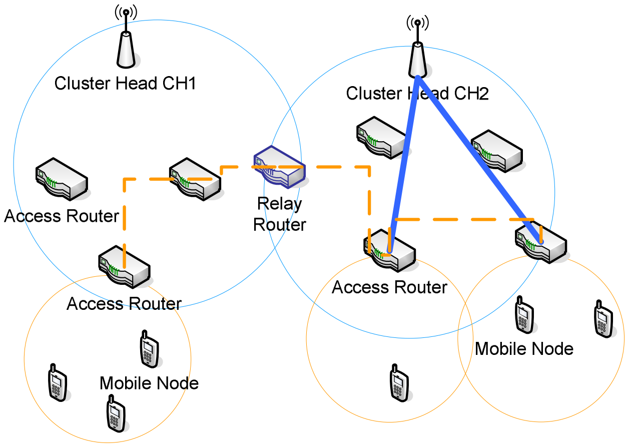


Figure 1. Scalability and route optimization support for WMNs

The paper is organized as follows. Section 2 describes the complete framework including PMIPv6 architecture, existing movement detection mechanisms and the cluster-based architecture. Section 3 describes the proposed extensions for PMIPv6. Section 4 illustrates Eurecom's implemented software architecture of Extended PMIPv6 and the virtualization-based development process using UML and Ns-2 Emulation. Section 5 provides evaluation of our extended PMIPv6 with qualitative and quantitative results. In Section 6 we describe the applicability of our proposed work to Public Safety applications. Finally, section 7 concludes the paper and provides perspectives for future work.

2. Framework

2.1. Proxy Mobile IPv6

PMIPv6 [2] is designed to provide network-based mobility management [3][4] 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 MAG is to detect MN's movements and initiate mobility-related signaling with 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 allowed in the PMIPv6 domain. Here we assume a Stateless Address Configuration [5].

Figure 2 shows a typical PMIPv6 handover process of an IPv6 MN. Once an 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 its reachability. 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 the MN at the LMA and MAGs is maintained in a Binding Cache entry which can be accessed using the MNID as search key. Such information associates the MN with its serving MAG, and allows the relationship between the MAG and the LMA to be maintained.

At any point, the detachment of the MN can be detected by the MAG due to MN's movements out of MAG's coverage, or to the MN's decision of terminating the mobility session. The Location Deregistration procedure starts and the MAG sends a Proxy Binding Update message to the LMA with the lifetime value set to zero.

The basic PMIPv6 protocol does not consider the route optimization for communication between MNs in the same PMIPv6 domain. Besides, a centralized LMA represents 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.

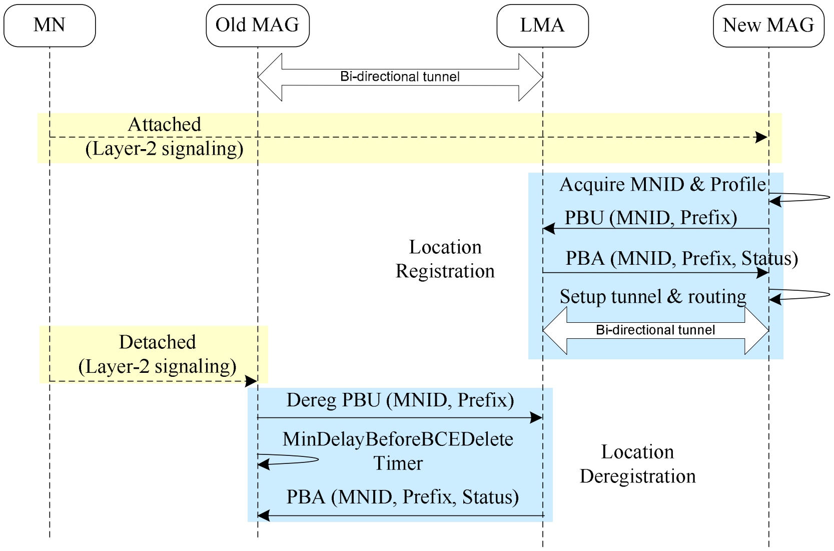


Figure 2. Proxy Mobile IPv6 sequence diagram

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, they are host-based and require special supports from the MN. For Proxy Mobile IPv6, the MAG must be responsible for the movement detection, requiring a network-based movement detection mechanism. The hints for movement detection can be the link-layer event notifications, traffic monitoring events or DNAv6 [6].

A traffic monitoring based mechanism only works properly 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 as they 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 and requires a lot of modifications either on the network side or on the terminal side; 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 moves to a new link, which depends on how the MN itself detects the attachment and detachment.

From a long term perspective, link-layer based approach is the best choice for movement detection. A possible candidate with this approach is Media Independent Handover (IEEE 802.21). We also presented in [7] an enhanced network-based IP-layer movement detection as a short-term solution for heterogeneous networks.

2.3. Cluster-based Architecture

To provide scalability in large scale heterogeneous wireless mesh networks, we consider a cluster-based architecture, as shown in Figure 3. Each cluster should have one and only one CH with LMA's functionalities. The CH has the 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. Each MN, attached to one of the AR, can be connected through the wireless backhaul to all the other routers. The MN therefore can communicate with other mobile CNs in the network through ARs as well as with CNs in the Internet through CHs.

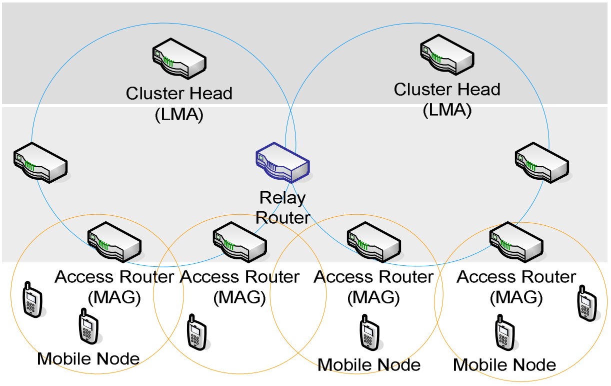


Figure 3. Scalability with cluster-based architecture

3. Extended PMIPv6

The standard Proxy Mobile IPv6 provides a natural solution for communication between an MN and a CN located outside the PMIPv6 domain. It is also efficient for intra-cluster communication and intra-cluster mobility.

In case of inter-cluster communication or in case of route optimization, we need to extend the protocol to solve the following fundamental issues: (i) detecting the communication establishment, (ii) locating the serving entities of the CN, (iii) setting route optimization between ARs and (iv) maintaining the soft state along the route.

3.1. Detecting Communication Establishment

We define the communication in this work as the exchange of traffic between two nodes. The communication is identified by the source and the destination's IP addresses.

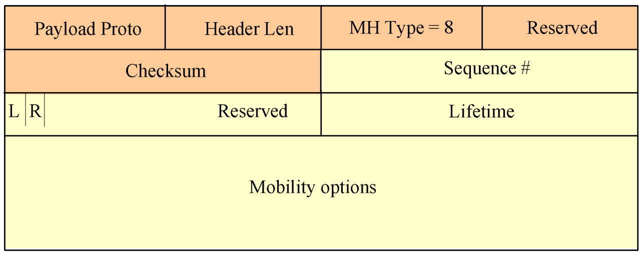
When the Per-MN prefix scheme is used, a *connection tracking* module must be installed on MAGs. Netfilter subsystem can provide such feature with the ip_conntrack module.

When the shared prefix approach is used, both nodes use the same network prefix. MNs in the domain consider each other as on-link and therefore trigger Neighbor Unreachability Detection (NUD) during their communication establishment. The MN sends a NS message to resolve the IP address of the CN to the MAC address of the CN. All NS messages for Address Resolution are inspected by the edge entities - the MAG or the LMA. As the CN address is stored in the target field, the serving entities can lookup the target in their binding cache to check if they are also the serving entities for the CN.

3.2. Locating the Serving Entities

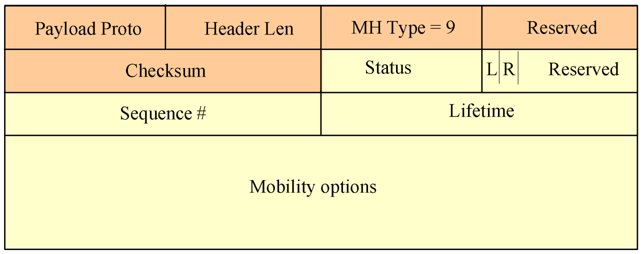
Let MAG_{MN} and LMA_{MN} denote the serving MAG and the serving LMA of the MN respectively. Also let MAG_{CN} and LMA_{CN} denote the serving MAG and the serving LMA of the CN respectively. When establishing the communication between an MN and a CN belonging to different clusters, LMA_{MN} needs to know LMA_{CN} and MAG_{CN}. The same problem arises when establishing the communication with route optimization between an MN and a CN in the same cluster or in different clusters: MAG_{MN} needs to know MAG_{CN}. This location issue is expressed as the problem of mapping a CN address into its serving MAG address or its serving LMA address.

We propose a new couple of messages: Proxy Binding Request (PBReq) and Proxy Binding Response (PBRes). Five new options are also defined: four options named generally Serving Entity Address options, and Source MN Address option.



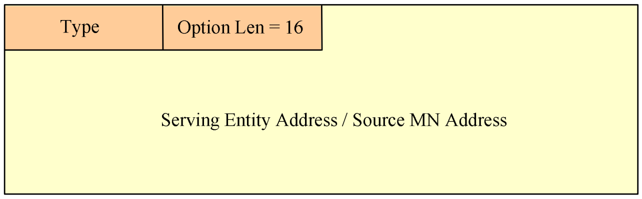
Payload Proto	Header Len	MH Type = 8	Reserved
Checksum		Sequence #	
L R Reserved		Lifetime	
Mobility options			

Figure 4. Proxy Binding Request Message



Payload Proto	Header Len	MH Type = 9	Reserved
Checksum		Status	L R Reserved
Sequence #		Lifetime	
Mobility options			

Figure 5. Proxy Binding Response Message



Type	Option Len = 16
Serving Entity Address / Source MN Address	

Figure 6. Serving Entity or Source MN Address Options

Figure 4 shows the PBReq message structure with Mobile Header (MH) Type taking the value 8 (the official value should be registered at IANA). The PBReq with the Location (L) bit is sent by $\mathrm{MAG}_{\mathrm{MN}}$ to $\mathrm{LMA}_{\mathrm{MN}}$ to find which MAG is serving the CN. The Link-layer Identifier option and the Home Network Prefix Option are mandatory and used to carry the CN address. To identify and maintain the RO cache entry, the MN address within the Source MN Address is combined with the CN address as the search key. The PBReq is also sent by the LMA to All-LMA multicast group in case of inter-cluster communication to find which MAG and which LMA are serving the CN. When the RO Indication (R) bit is set, the message is used to request the peer's serving entity to setup the optimized bidirectional tunnel.

Figure 5 shows the PBRes message with the MH Type taking the value 9. It is the reply to a PBReq and can eventually contain options carrying the $\mathrm{MAG}_{\mathrm{CN}}$ address and/or the $\mathrm{LMA}_{\mathrm{CN}}$ address.

As regards the Serving Entity Address options and the Source MN Address option (see Figure 6), we use five different values of Option Type to classify: Source MN address (0x0B), $\mathrm{MAG}_{\mathrm{MN}}$ address (0x0C), $\mathrm{LMA}_{\mathrm{MN}}$ address (0x0D), $\mathrm{MAG}_{\mathrm{CN}}$ address (0x0E) or $\mathrm{LMA}_{\mathrm{CN}}$ address (0x0F).

The inter-clusters communication establishment is illustrated in Figure 7. Once the MN triggers a NS to find the CN, $\mathrm{MAG}_{\mathrm{MN}}$ uses the target field for lookup in its binding cache, i.e. cache missed. If no information is found for that target belonging to the same PMIPv6 domain, the $\mathrm{MAG}_{\mathrm{MN}}$ assumes that the CN is away from its home link and sends a PBReq message to the $\mathrm{LMA}_{\mathrm{MN}}$. If the $\mathrm{LMA}_{\mathrm{MN}}$ does not have any information about the target, it must send a PBReq to All-LMA multicast address. The $\mathrm{LMA}_{\mathrm{CN}}$ will reply with a PBRes carrying at least the $\mathrm{MAG}_{\mathrm{CN}}$ address. Later, the $\mathrm{LMA}_{\mathrm{MN}}$ can setup a routing entry pointing for a bidirectional tunnel with the $\mathrm{LMA}_{\mathrm{CN}}$. As a result, a default path traversing LMAs is set up for the communication between MN and CN.

The $\mathrm{LMA}_{\mathrm{MN}}$ then will reply with a PBRes to the $\mathrm{MAG}_{\mathrm{MN}}$ to inform the $\mathrm{MAG}_{\mathrm{MN}}$ about the $\mathrm{MAG}_{\mathrm{CN}}$ address and eventually the RO Indication. The $\mathrm{MAG}_{\mathrm{MN}}$ will also perform Proxy ARP for the CN if the shared-prefix scheme is used.

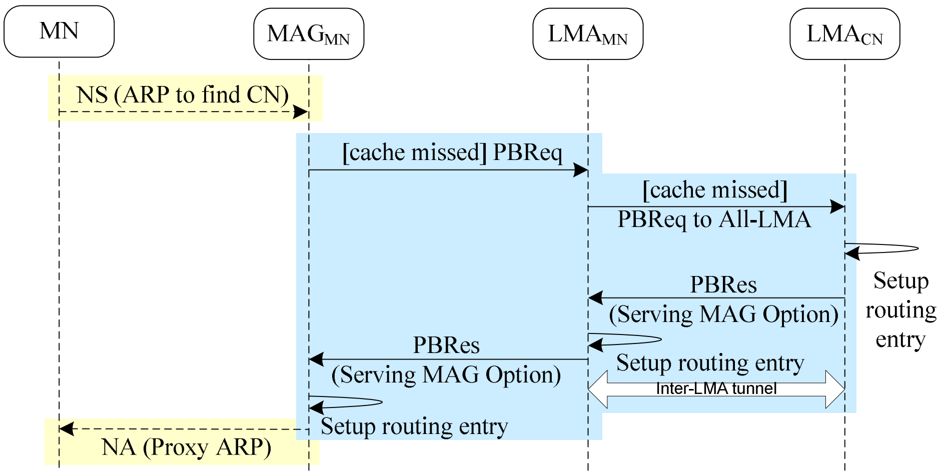


Figure 7. Inter-clusters communication establishment

3.3. Setting Route Optimization

When the LMA$_{MN}$ decides to start RO with IP tunneling, it includes the peer's Serving Entity address (MAG$_{CN}$ address or LMA$_{CN}$ address) and an explicit RO Indication flag in the PBRes. Once received this RO Indication, the MAG$_{MN}$ must send a PBReq to the peer's Serving Entity with RO Indication flag and wait for the PBRes. At the end of the procedure, the MAG$_{MN}$ and the peer's serving entity establish a bidirectional tunnel and update routing entry to forward the traffic through the optimized bidirectional tunnel. The traffic is then forwarded in an optimized way directly between MAGs, e.g. MAG$_{MN}$-MAG$_{CN}$, or through one LMA, e.g. MAG$_{MN}$-LMA$_{MN}$-MAG$_{CN}$, MAG$_{MN}$-LMA$_{CN}$-MAG$_{CN}$. Once the path is set up, the traffic between the MN and the CN can be delivered directly through the optimized bidirectional tunnel. The RO soft state of the communication is then maintained in all serving MAGs and LMAs'RO cache also during MN and CN's movements within the mesh domain. Figure 8 illustrates the complete process.

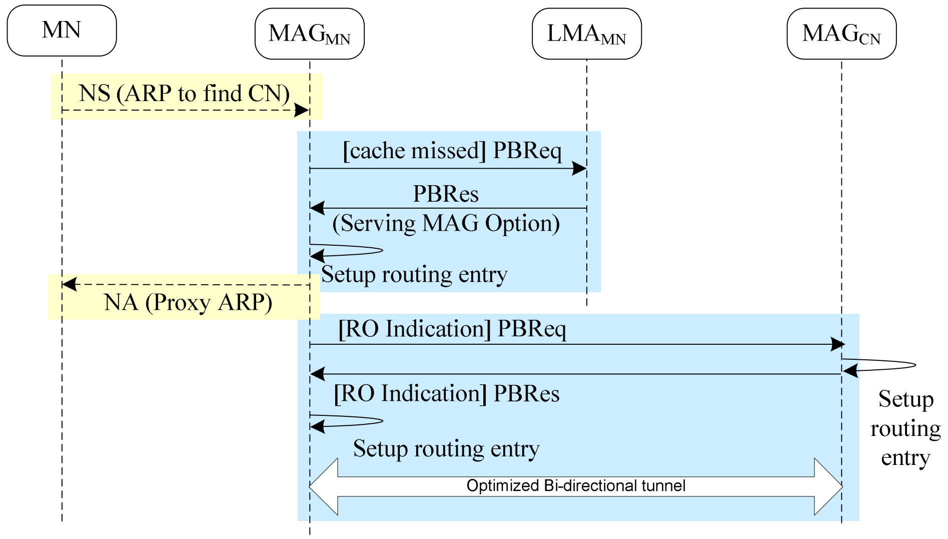


Figure 8. Route Optimization Setup

3.4. Maintaining Route Optimization Soft State

MN’s mobility between different ARs affects the RO soft state. In the case of intra-cluster mobility, any deregistration event will cause the cancellation of the RO soft state at the previous MAG$_{MN}$. The LMA$_{MN}$, whenever its binding cache entry is modified due to the mobility, must inform involved MAG$_{CN}$ about the new MAG$_{MN}$ to redirect the related traffic through the default route in the meantime the new RO is again established.

In the case of inter-clusters mobility, as the previous LMA$_{MN}$ may not be aware about the changes, the new LMA$_{MN}$ can send a PBRes message to All-LMA multicast address. This message helps the old LMA$_{MN}$ to activate the Location Deregistration procedure if necessary, and helps other LMAs to maintain up-to-date routing information for on-going sessions.

4. Implementations

4.1. Proxy Mobile IPv6 Implementation

We implemented the proposed extensions of Proxy Mobile IPv6 for wireless mesh network under Linux kernel 2.6.20 while reusing Mobile IPv6 for Linux (MIPL) v2.0 [8]. All the basic bricks of MIPL are reused in an efficient way as shown in Figure 9.

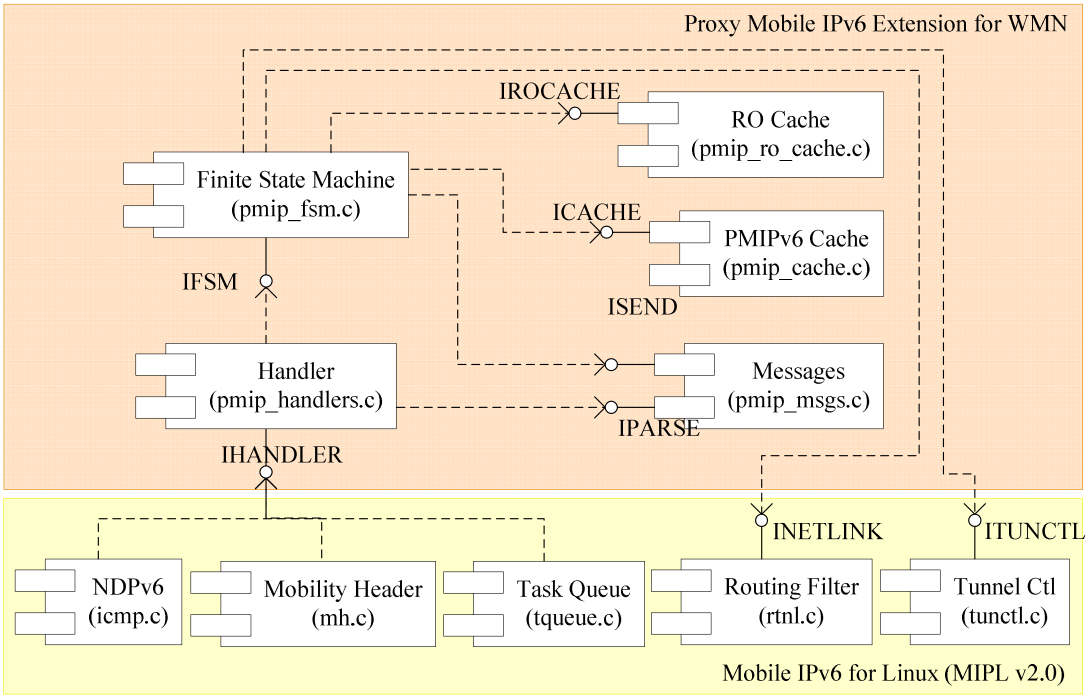


Figure 9. Extended Proxy Mobile IPv6 Software Architecture

In MIPL v2.0, Mobile IPv6 is implemented using multi threads: one for handling the ICMPv6 messages, one for handling Mobility Header messages, and another one for handling tasks and time events, etc.

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 inputs 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. The PMIPv6 binding cache stores all information about MNs' points of attachment and it is kept up-to-date with the mobility of MNs. RO soft state is stored in a separated RO cache. Each RO cache entry represents a communication between MN and CN and can be accessed using their IP addresses as the search key. As Proxy Mobile IPv6 implementation is built on top of MIPL version 2.0, it could be, in the future, easily integrated in MIPL, growing in line with the standards as well as with MIPL source code.

4.2. Virtualization-based Development Process

The development is realized in a virtualization-based process using a combination of UML [9] [10] and Ns-2 Emulation [11] and allowing the migration to the real testbed with 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 it with the real host machine, can be assigned to 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 guest root file system is a normal file that can be mounted directly to the host file system. This allows developers to work with the guest file system without the need of turning on the virtual machine. Copy-On-Write is another interesting feature when playing with UML as it allow different virtual machines to run on the same guest root file system and save the disk space by storing the differences in .cow files. Figure 10 shows the dependency between different components of UML.

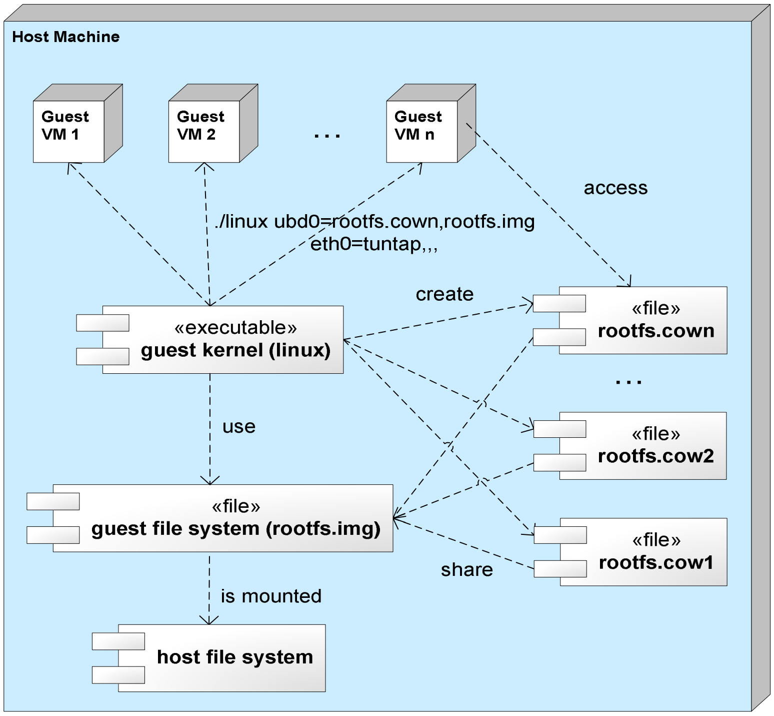


Figure 10. Virtualization with User-mode Linux

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. To emulate the wireless transmission and the mobility of the mobile node, we extend the Ns-2 Emulation, allowing the mapping of the virtual machines into Ns-2 wireless nodes.

5. Evaluation Methodology

5.1. Virtual IPv6 Wireless Mesh Network

We use a virtualization-based approach to evaluate the extended PMIPv6 for WMN in this early phase. Figure 11 shows the virtual Wireless Mesh testbed. The topology is generated by the Virtual Network User-mode Linux (VNUML) [12]. A Linux kernel 2.6.20 is compiled under User-mode architecture to serve as a guest kernel for virtual machines. Different scenarios are defined and automated with Tcl language, which it is a part of Ns-2 Emulation. The virtual testbed is composed of two clusters under the control of CH1 and CH2, and three routers AR1, AR2 and AR3. LMA functionality runs on CHs while MAG functionality runs on ARs. AR1 and AR2 are under the control of CH1. AR3 is under the control of CH2. CH1 and CH2 are interconnected.

MN1 and MN2 do not have any specific software for mobility management. Initially, MN1 and MN2 can be attached to any ARs. As any type of access technology is allowed, we consider here IEEE 802.11 for simplification. MNs’ addresses are auto-configured through IPv6 Stateless Address Auto Configuration. We assume that there is no IPv6 address conflict and therefore we can use a shared-prefix model with a shared prefix of 2001:1::/64. The three site-scope prefixes FEC0:1000::/64, FEC0:2000::/64 and FEC0:3000::/64 are used for enhanced network-based movement detection procedure [7]. Three ARs are configured with Router Advertisement daemons (RADVD) which broadcast RAs on their eth0 interface. RAs contain two prefixes and are sent periodically every 100 ms. Iperf is used to generate tcp/udp traffic while ping6 is used to generate ICMP traffic.

The logical connectivity between entities in the mesh backhaul is represented by Ns2 point-to-point links which are characterized by bandwidth and delay. This allows us to impose specific delay in the transmission of messages between entities to produce emulation results that are closest to real experimentation results.

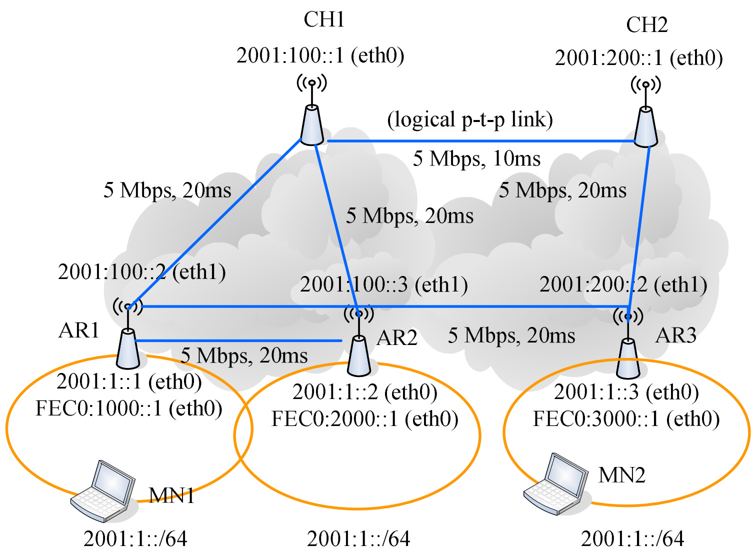


Figure 11. Virtual Wireless Mesh Testbed

Different test scenarios have been defined and carried out: We have shown in [7] the correctness of the proposed framework with qualitative results. In the following sections, we provide quantitative results with regards to the cost and the performance.

5.2. Scenario 1: Intra-cluster Communication

This scenario considers the communication of two MNs attached to two different ARs inside the same cluster: MN1 is attached to AR1 while MN2 is attached to AR2. Both AR1 and AR2 are under the control of CH1. Once registered with the Location Registration process, the two MNs can communicate with each other through the AR1-CH1-AR2 path using two IPv6 tunnels.

We use ping6 tool to test the reachability with Echo Request and Echo Reply message. Iperf tool is used to generate tcp traffic between MN1 and MN2 while scp application is used to test the file transfer at application level. Tcpdump tool are used to capture the traffic.

To measure the extra delay caused by the signaling mechanism, we use the ping6 tool and measure the RTT of the first packet in two scenarios: (i) on-demand route with signaling and (ii) pre-established route without signaling. Let r_1 and r_2 respectively be the random variable representing the RTT of the first ping packet in (i) and (ii) scenarios. In both cases, we include also the time of Neighbor Unreachability Detection (NUD) procedure between MNs and their serving MAGs. The average cost in terms of extra delay can be calculated as $mean(r_1)$-$mean(r_2)$.

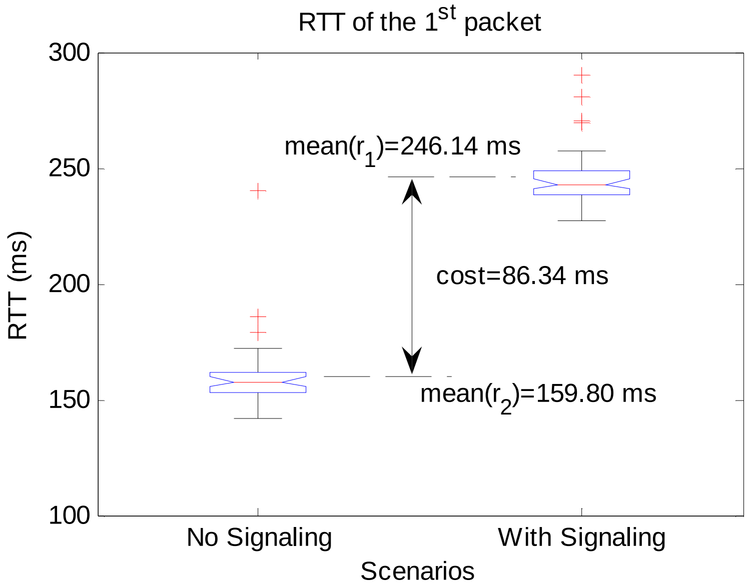


Figure 12. Signaling cost in terms of delay in intra-cluster communication

The scenario is repeated 50 times; 50 samples of r_1 and 50 samples of r_2 are captured. Figure 12 shows the distribution of r_1 and r_2 in form of box-and-whisker diagram. Box-and-whisker diagram is a convenient way of graphically depicting groups of numerical data through their five-number summaries (the lower extreme, lower quartile, median, upper quartile, and upper extreme). The cost is then calculated and depicted as the difference between the mean of r_1 and the mean of r_2 in the figure. In our virtual testbed, it takes in average 86.34 ms for establishing a new communication. This delay depends on both the processing time at edge entities and the message exchange delay between them. In comparison with the RTT of ping packets between the two MNs, which has the average value of 90.15 ms over 500 samples in this case, the extra delay for the first packet is almost the same and quite acceptable; especially as this extra delay happens only once during the communication.

5.3. Scenario 2: Inter-clusters Communication

This scenario considers the communication of two MNs attached to two different ARs belonging to different clusters: MN1 is attached to AR1 under the control of CH1, while MN2 is attached to AR3 under the control of CH2. Once registered with the Location Registration process, the two MNs can communicate with each other through the AR1-CH1-CH2-AR2 path using three IPv6 tunnels.

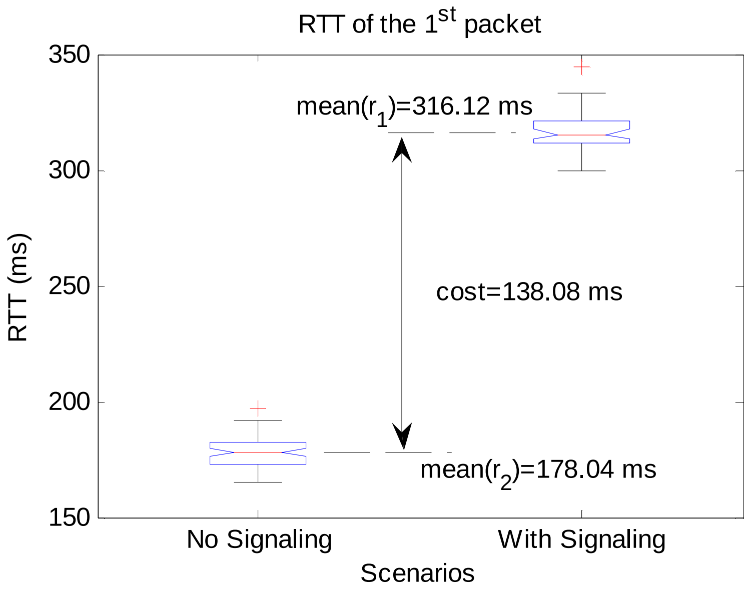
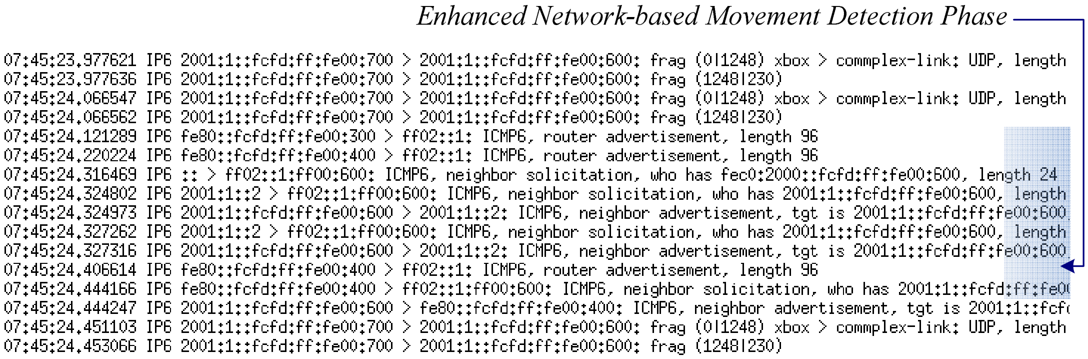


Figure 13. Signaling cost in terms of delay in inter-cluster communication

We apply the same qualitative and quantitative tests as in the section 5.2 to verify the proposed functionalities and evaluate the cost to setup the inter-clusters communication. Figure 13 shows the distribution of r_1 and r_2 in form of box-and-whisker diagram. The cost is then calculated and depicted as the difference between the mean of r_1 and the mean of r_2 in the figure. In this virtual testbed, it takes in average 138.08 ms for establishing a new inter-clusters communication. This delay is more important than the one measured for the intra-cluster scenario. This is due to the presence of the additional LMA and the additional inter-LMA link which increase the overall processing time and the message exchange delay. In comparison with the RTT of ping packets between the two MNs, which has the average value of 111.35 ms over 500 samples, the extra delay for the first packet is still quite acceptable; especially as this extra delay happens only once during the communication.

5.4. Scenario 3: Intra-cluster Mobility

This scenario considers the mobility of a MN within one cluster. Considering the scenario 2 in section 5.3, we start a UDP and a TCP session from MN2 to MN1 and let the MN1 moving from AR1 to AR2 in the middle of the session. To emulate the fact that all MAGs have the same shared MAC address as specified in the standard PMIPv6 [2], we update the ARP cache of the MN1 so that the MN1 always use the valid MAC address which corresponds to the serving AR.



```
07:45:23.977621 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (0|1248) xbox > commplex-link: UDP, length
07:45:23.977636 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (1248|230)
07:45:24.066547 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (0|1248) xbox > commplex-link: UDP, length
07:45:24.066562 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (1248|230)
07:45:24.121289 IP6 fe80::fcfd:ff:fe00:300 > ff02::1: ICMP6, router advertisement, length 96
07:45:24.220224 IP6 fe80::fcfd:ff:fe00:400 > ff02::1: ICMP6, router advertisement, length 96
07:45:24.316469 IP6 :: > ff02::1:ff00:600: ICMP6, neighbor solicitation, who has fec0:2000::fcfd:ff:fe00:600, length 24
07:45:24.324802 IP6 2001:1::2 > ff02::1:ff00:600: ICMP6, neighbor solicitation, who has 2001:1::fcfd:ff:fe00:600, length
07:45:24.324973 IP6 2001:1::fcfd:ff:fe00:600 > 2001:1::2: ICMP6, neighbor advertisement, tgt is 2001:1::fcfd:ff:fe00:600,
07:45:24.327262 IP6 2001:1::2 > ff02::1:ff00:600: ICMP6, neighbor solicitation, who has 2001:1::fcfd:ff:fe00:600, length
07:45:24.327316 IP6 2001:1::fcfd:ff:fe00:600 > 2001:1::2: ICMP6, neighbor advertisement, tgt is 2001:1::fcfd:ff:fe00:600,
07:45:24.406614 IP6 fe80::fcfd:ff:fe00:400 > ff02::1: ICMP6, router advertisement, length 96
07:45:24.444166 IP6 fe80::fcfd:ff:fe00:400 > ff02::1:ff00:600: ICMP6, neighbor solicitation, who has 2001:1::fcfd:ff:fe0
07:45:24.444247 IP6 2001:1::fcfd:ff:fe00:600 > fe80::fcfd:ff:fe00:400: ICMP6, neighbor advertisement, tgt is 2001:1::fcf
07:45:24.451103 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (0|1248) xbox > commplex-link: UDP, length
07:45:24.453066 IP6 2001:1::fcfd:ff:fe00:700 > 2001:1::fcfd:ff:fe00:600: frag (1248|230)
```

Figure 14. UDP session log during intra-cluster mobility

We use iperf tool to generate UDP traffic with a rate of 128Kbps from MN2 to MN1. During the handover process, we observe that 4 packets are lost. Once the MN1 is registered, the UDP traffic can be immediately forwarded to the MN1. Figure 14 shows a UDP session log captured by tcpdump on MN1 during its movement. Once moved to the AR2, MN1 receives the Router Advertisement (RA) from AR2, and configures a temporary address with the site-scope prefix fec0:2000::/64. MN1 starts the Duplication Address Detection process by multicasting the Neighbor Solicitation (NS) message using unspecified source address. AR2 inspects the NS message and uses it as a hint for MN1’s attachment. It verifies the attachment by sending a unicast NS to MN1. When receiving the Neighbor Advertisement as a confirmation, AR2 starts the Location Registration procedure.

Let define the handover latency as the duration between the last arriving packet before handover and the first arriving packet after a successful location registration. The estimated handover latency is 384.55 ms. The handover latency includes 260.75 ms for enhanced network-based movement detection [7]. We note that the handover latency is mostly impacted by the movement detection time in this case. A link-layer based movement detection mechanism should greatly reduce the overall handover latency in the future.

As regards TCP traffic, we believe it is interesting to analyze the Time-Sequence graph. This graph is versatile for analyzing the TCP protocol behavior and implicitly shows different metrics such as congestion, RTT, throughput, etc. We use iperf tool to generate TCP traffic, tcpdump tool to capture the traffic and tcptrace tool to analyze the TCP traffic and to generate graphs. Figure 15 shows the Time-Sequence graph generated from the captured TCP session between the two MNs when intra-cluster mobility is considered.

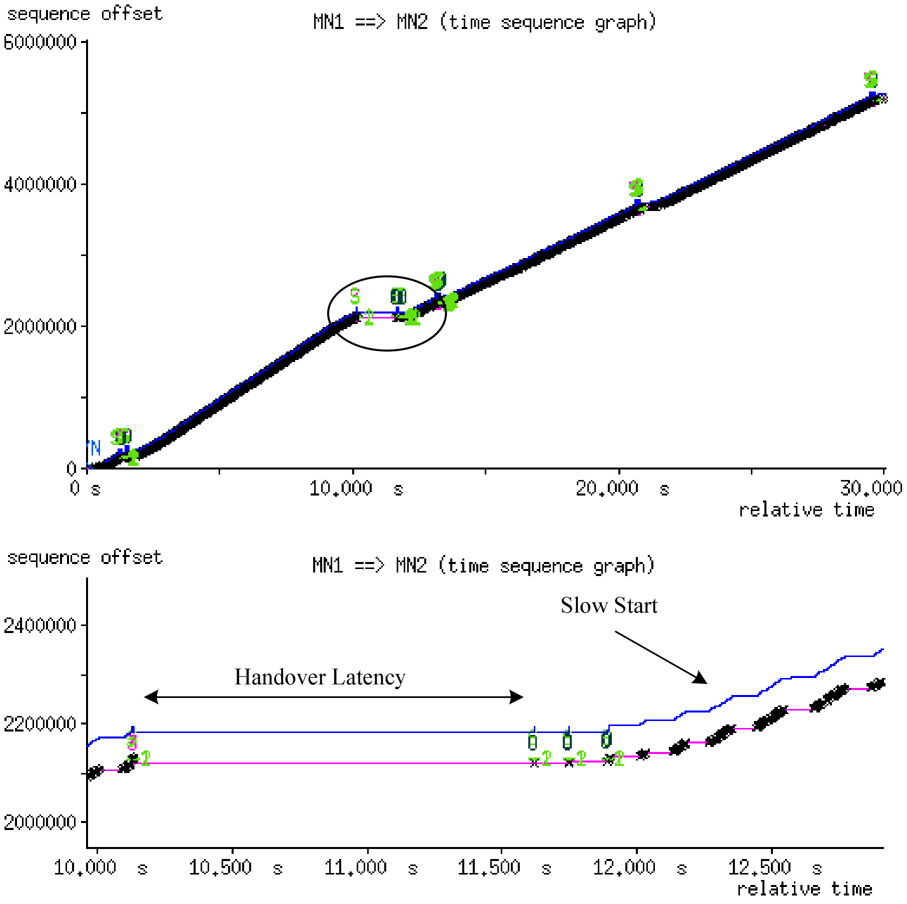


Figure 15. Time-Sequence graph of TCP session during intra-cluster mobility

The gap at 10s represents the handover process. Taking a closer look into the handover process, during which no traffic can be delivered in both direction, we can see that the estimated handover latency is about 1.5s. Once the registration process at the AR2 finishes, the TCP session can continue and the sender can start the retransmission after a certain timeout with the slow start algorithm as expected. By comparing the handover latency in UDP and TCP case, we can conclude that TCP protocol is more sensitive to the mobility of MNs as its congestion control behavior provokes extra delay in the reaction of the sender. We also observe that if the assumption about shared MAC address is not applied, the handover latency will be larger due to the invalid ARP cache of MN1.

5.5. Scenario 4: Route Optimization for Intra-cluster and Inter-cluster Communication

This scenario shows the results of RO. Let consider the intra-cluster scenario (section 5.2) and inter-cluster scenario (section 5.3) with activated RO option. We use ping6 to measure the Round Trip Time (RTT). Figure 16 shows the cumulated distribution function of the RTT of 500 Echo Request and Echo Reply samples in four cases: (i) intra-cluster communication without RO, (ii) intra-cluster communication with RO, (i) inter-cluster communication without RO and (iv) inter-cluster communication with RO.

In the case of intra-cluster communication, the mean value of RTT without RO is 90.15 ms and the traffic passes through AR1-LMA1 and LMA1-AR2 tunnels; while the mean value of RTT with RO is 49.01 ms, and the traffic passes directly through the AR1-AR2 tunnel. As illustrated in the above figure, it is obvious that the RTT with RO is much less than the RTT without RO.

In consideration of the inter-cluster communication, the mean value of RTT without RO is 111.35 ms and the traffic passes through AR1-LMA1, LMA1-LMA2 and LMA2-AR3 tunnels. The mean value of RTT with RO is 50.15 ms and the traffic passes directly through AR1-AR3 tunnel.

Thus, we can conclude that the effect of RO is reducing the RTT of traffic communication between two MNs. As a consequence, we will gain a better TCP throughput, especially in case of inter-cluster communication.

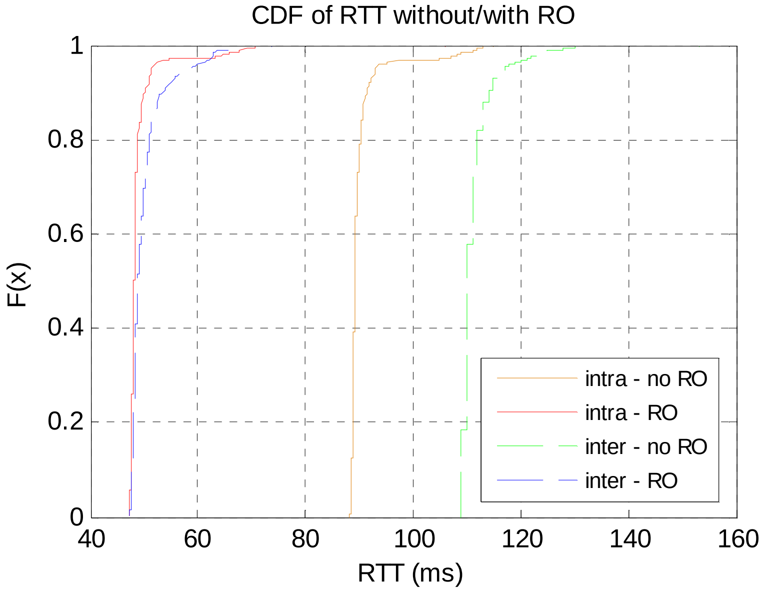


Figure 16. CDF of RTT without/with RO in intra/inter cluster communication

With regard to the impact of RO on TCP throughput, we use iperf tool to generate TCP traffic from MN2 to MN1 and analyze the throughput graph of the captured traffic with tcptrace tool. Figure 17 represents the instantaneous throughput (yellow dots), the moving average throughput (the red line) calculated as the average of 10 previous yellow dots, and the average throughput of the connection up to that point in the lifetime of the connection. It is shown that with RO, the TCP throughput increases thanks to smaller RTT between MNs.

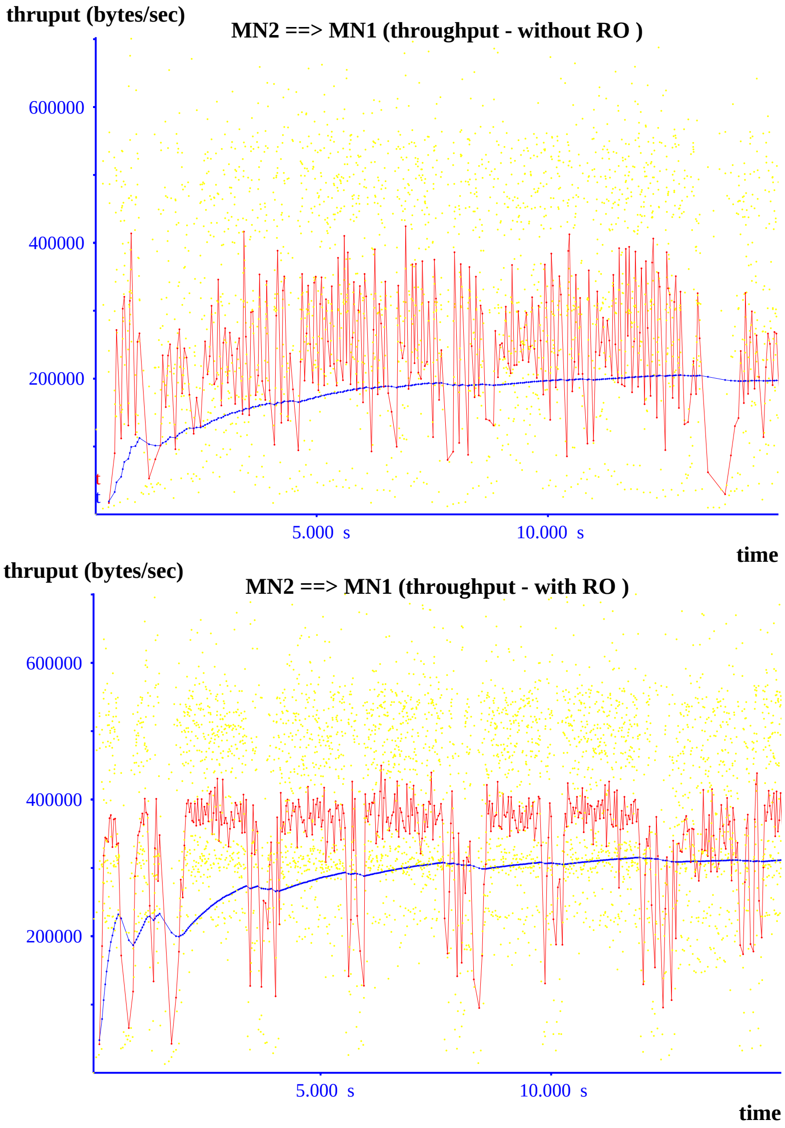


Figure 17. TCP Throughput without/with RO in intra-cluster communication

6. Application to Public Safety Communications

In this work, the combination of WMNs with PMIPv6 and its extensions intent to cover the important research area of Public Safety communications and its application to emergency mobile communications.

When a large scale disaster strikes, first responders are sent to the site immediately. Once the most pressing needs of the disaster are addressed, the next step is to establish a command and control center. To accommodate this need, a communication infrastructure is required to provide decision makers with data and information from the site to receive digital maps, data and feedback from personnel in the field in a timely manner. Also, it should be able to provide a reliable connection with enough resources for a distributed command and control center. The communication infrastructure needs to be reliable and interoperable with the existing responder organizations' devices in a distributed system. Additionally, it needs to be easily configurable and quickly deployable at low cost. The system should be designed in a modular fashion that is easily upgradeable with the technology evolvement without the need to replace the entire system. This leads to an economic deployment solution which is affordable for different public and private agencies. Furthermore, it is desirable to provision redundancy for an effective network management based on the trade-off between reliability and cost.

Mesh network infrastructure well fulfils this application domain's specific requirements [13], but to assess its complete suitability to Public Safety and disaster recovery applications, it is necessary to include mobility support and scalability requirements to WMNs.

As regards mobility, in order to help emergency personnel to concentrate on the tasks, the emergency network must be mobile, deployed easily and fast with little human maintenance. Therefore, devices must be capable of automatically organizing into a network. Procedures involved in self-organization include device discovery, connection establishment, scheduling, address allocation, routing, and topology management. Public Safety users must have access to constant communication while traveling at reasonable speeds. The mobility requirement includes the ability to roam between different networks, potentially operated by different agencies and jurisdictions. WMNs still need a mobility management mechanism for transparently and seamlessly achieve handover during mobile nodes movements.

On the other side, disasters may affect a locality or could spread or cascade to affect larger areas, thus horizontal and vertical scalability requirements are of extreme importance for Public Safety communication systems. Horizontal scalability refers to the network's ability to grow efficiently and cost-effectively in terms of geographical coverage, while vertical scalability stands for the ability to efficiently support an increasing number of users.

Suboptimal deployment and a frequently changing environment challenge network functionality. Therefore, the network must be able to report environment changes for proper management or be self-manageable to avoid service disruption. WMNs have to take into account the degradation of the throughput when increasing the number of hops in the end-to-end communication and the difficulties of managing the changing in the network topology.

The proposed extended PMIPv6 for heterogeneous wireless mesh networks resolves many important issues, like mobility and scalability with unmodified mobile nodes, which arises when designing a robust communication infrastructure with applications for emergency response situations. The architecture presented in Figure 3 can be considered as a simplified scenario for several possible practical situations. In order to provide a better understanding on how the proposed scenario can approach the most common emergency situations, we take into consideration the following practical scenarios:

- The first scenario represents the case in which a natural disaster occurs in a populated area, causing lives in danger and disruption of the complete network infrastructure. Different governmental agencies, like fire brigades, law enforcement agency and emergency medical teams, need a new rapidly deployable infrastructure suitable for emergency operations. As shown in Figure 18, the WMN with mobility and scalability features can be the common core network used for interconnecting mobile end user networks. Each local wireless network is free to use a different technology depending on the agency and unmodified mobile terminals. It relies upon the high scalable WMN architecture for communications inside the disaster area with other rescue teams. For communications outside the crisis site, one or more gateways, i.e. satellite gateways, can be connected to the WMN in order to provide connectivity with the headquarters for rescue coordination commands.
- The second scenario represents the case in which several buildings are burning in a limited area, lives are in danger inside the buildings and the fire has disrupted the network in that area. Fire brigades and medical teams need an extended coverage of the fixed and untouched network in order to communicate and follow rescue commands inside the affected area. As illustrated in Figure 19, the proposed extended PMIPv6 can be used to provide such coverage extension, deploying from the gateway attached to the fixed infrastructure a cluster head and mobile routers in order to bring connectivity to mobile rescue teams.

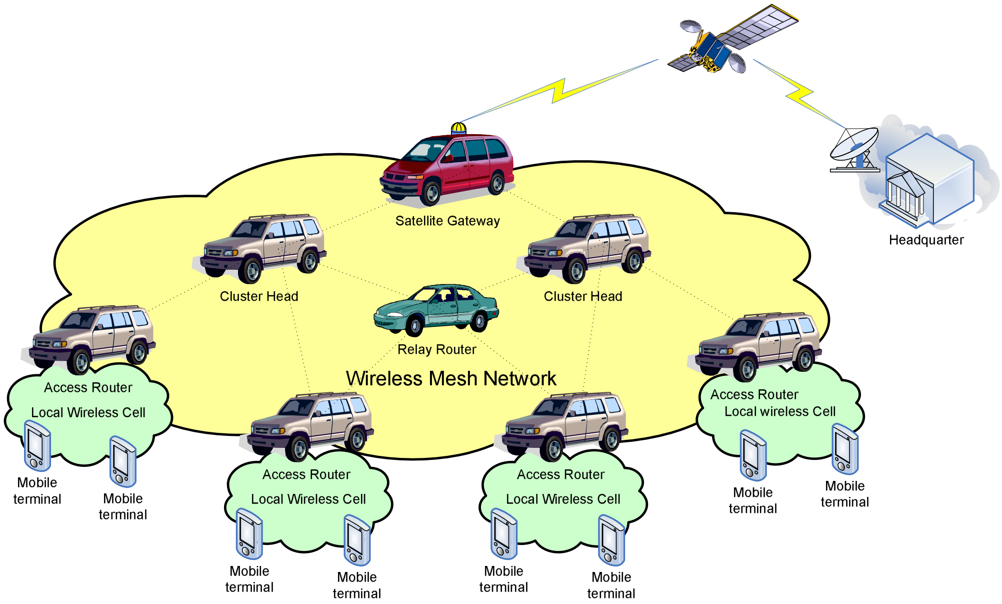


Figure 18. Extended PMIPv6 for post-disaster network deployment in Public Safety communications

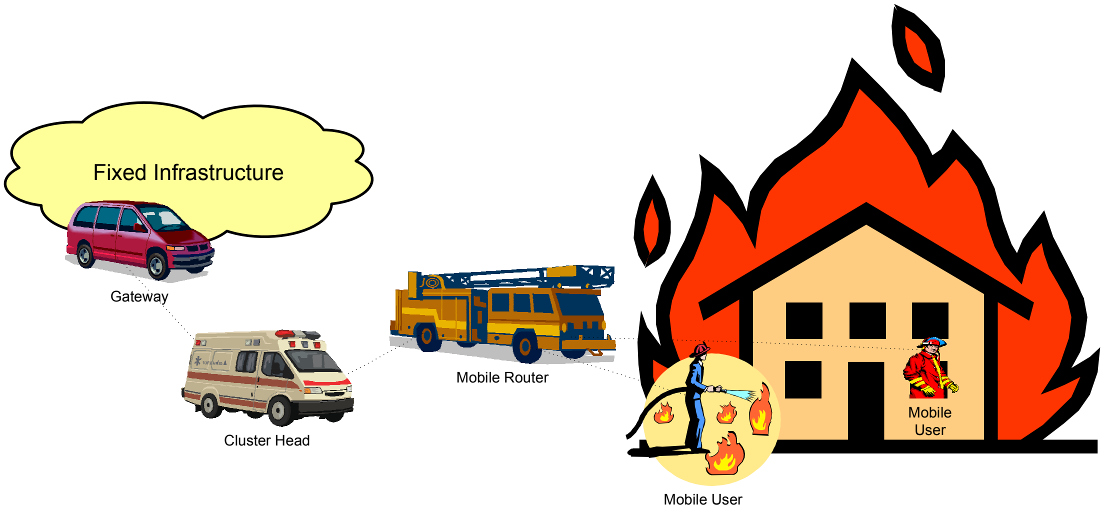


Figure 19. Extended PMIPv6 for coverage extension of fixed infrastructure in Public Safety communications

7. Conclusions

We have extended PMIPv6 to provide scalability and route optimization to large heterogeneous wireless mesh 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. In particular, WMNs can greatly benefit from a low cost location discovery and management process such as PMIPv6, due to the fact that the MN is able to keep the same IP address while moving in the WMN. Moreover, the proposed extension can be used to setup optimized routes in the WMN. The scheme is also valid for a general PMIPv6 domain.

We have implemented the extended PMIPv6 protocol in a virtual IPv6 Wireless Mesh Network testbed and evaluated important information as signaling and handover costs, latency, packets loss and RTT delay. It is shown that it takes no more than 1.5 times of RTT between two MNs for setting up routes with inter-clusters communication support. This is quite reasonable as it happens only once for each communication. In consideration of the handover performance, we found that a TCP session is more impacted by mobility than a UDP session due to the congestion control. Besides, as the handover latency depends also on the movement detection time, we believe that in the future a link-layer based movement detection will be considered as one approach for reducing the handover latency in PMIPv6. As regards RTT and TCP throughput, PMIPv6 with RO can provide smaller RTT, thus increase the resulting TCP throughput.

From this initial study, we can conclude that we have the major components for fulfilling the requirements of future advanced mobile networking researches, suitable for different types of applications. In particular, we have addressed Public Safety and emergency mobile communications scenarios. The proposed WMN can be deployed at the disaster site as an infrastructure backbone or a coverage extension of fixed network. With the added value of scalability and mobility features, it can be used by rescue teams for easily moving inside the disaster area while keeping their ongoing communications. The vertical and horizontal scalability is provided to the emergency mobile network deployed at the disaster site, allowing the network to enlarge without impacting mobile terminals. One possible application of this work is the fast deployment of a mobile and wireless communication environment as in the CHORIST project [14], a FP7 project for integrating Communications for enHanced envirOnmental RISk management and citizens safeTy. Another application is to spontaneously structure the communication backbone of community based networks as in the French AIRNET project of the ANR - Agence Nationale pour la Recherche [15]. The proposed developments are integrated in the framework of Eurecom’s Open Source Platform “OpenAirInterface” [16].

Our future work will concentrate on optimizing the handover process using link-layer based movement detection and early movement detection.

8. Acknowledgements

Eurecom's research is partially supported by its industrial members: BMW, Bouygues Télécom, Cisco Systems, France Télécom, Hitachi Europe, SFR, Sharp, STMicroelectronics, Swisscom, Thales.

9. References

[1] I. F. Akyildiz and X. Wang, “A Survey on Wireless Mesh Networks”, IEEE Comm. Magazine, vol. 43, no. 9, 2005, pp. 23–30.

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6”, IETF RFC 5213, August 2008.

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

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

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

[6] 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.

[7] H.N. Nguyen, C. Bonnet, “Scalable proxy mobile IPv6 for heterogeneous wireless networks”, International Workshop on Mobile IPv6 and Network-based Localized Mobility Management, I-Lan, Taiwan, September 2008.

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

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

[10] H.N. Nguyen, C. Bonnet, “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] Virtual Network User Mode Linux Home page http://www.dit.upm.es/vnumlwiki/index.php/Main_Page.

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

[15] AIRNET Project Home Page, http://www.rnrt-airnet.org/

[16] OpenAirInterface Home Page, http://www.openairinterface.org

Authors

Huu-Nghia Nguyen

He graduated from Hanoi University of Technology (HUT) in 2002 for the Engineer of Information Technology. He received the MS degree in Computer Science from the Francophone Institute for Computer Science (IFI). During his master internship at Eurecom in 2005, he worked on the 3GPP Multimedia Broadcast Multicast Service (MBMS), within the scope of the FP6 DAIDALOS project. Since 2006, he has been pursuing his PhD thesis at Eurecom. His research interests cover mobility management and multi-homing support for an Always Best Connected vision.

Christian Bonnet

He joined Eurecom as an associate professor in 1992. Since 1998 he is at the head of the Mobile Communications Department of Eurecom. He has been involved in numerous research projects related to advance mobile networks in the field of Ad Hoc and Mesh Networks, QoS and Ipv6 mobility management: (IST) MULTINET, CHORIST, UNITE, DAIDALOS, Moby Dick, (RNRT) COSINUS, AIRNET, SAMU, PLATON, @IRS++. He co-authored more than 100 publications in international conferences and magazines.

Giuliana Iapichino

She received her MSc in Electronics Engineering with specialization in Telecommunications from University of Catania, Italy, in 2005. In 2006, she was a research intern at the European Space Agency – ESTEC, the Netherlands, working on QoS provisioning for multimedia services on all-IP based hybrid networks. In 2007, she joined Eurecom, France, where she is currently a Ph.D. student in the Mobile Communications Department. Her research interests cover ad hoc mobility in satellite and terrestrial networks for Public Safety and Crisis Management applications.