ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία
Μεταπτυχιακού Διπλώματος Ειδίκευσης

«*Simulating mobility in a Realistic Networking Environment*»

Δημήτριος Χαρούλης

Επιβλέπων: Γεώργιος Κ. Πολύζος

ΑΘΗΝΑ, ΙΟΥΛΙΟΣ 2012

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like, first of all, to thank my supervisor Professor George C. Polyzos for giving me the chance to work on this topic as well as for any support he provided to me in accomplishing this work. Always being friendly and motivating his students, he has created a pleasant environment mixed with plenty of creativity.

I wish also to thank Dr. Konstantinos Katsaros and Ph.D. student of our department Xenophon Vasilakos for narrowly collaborating with me and sharing their useful comments and ideas related to this research area. I could not omit the rest members of Mobile Multimedia Laboratory (MMLab) as they were always helpful and friendly, and especially Dr. Pantelis Fragoudis for always being interested in students' work and providing valuable advice to them (as well as to me).

A separate reference is needed to be made for my friends Yiannis T., Christos A. and Spyros P. for all the moments we had throughout this M.Sc. program, and for their invaluable support by any means.

Last, but not least, i want to thank my family for being next to me all these academic years by encouraging me and supporting my choices.

Abstract

The convergence between wireless networking and the Internet has made IP the dominant networking protocol for mobile networks. Despite its great success, the TCP/IP stack presents some inherent characteristics that do not allow it to respond to some of the challenges that imposes current (Inter)networking. One of them is mobility support in IP networks which is given great importance both by research and industry community as we are moving towards All-IP networks.

Despite being mobile-unfriendly, IPv4 was the first version of the Internet Protocol (IP) to support mobility in network layer. The protocol designed for this work is Mobile IP that functions more like an add-on solution to the problem of mobility. The next version of IPv4, i.e. IPv6, was designed in such a way that would allow some of the deficiencies of the previous version to be overcame. As such, and bearing in mind the evolution towards All-IP networks, it has a better provisioning to support IP mobility. Mobile IPv6 (MIPv6) is the most representative protocol proposed, with its hierarchical flavor (Hierarchical MIPv6) taking a similar approach in an effort to improve its performance characteristics.

The goal of this master thesis is to present a realistic head-to-head performance analysis comparison between MIPv6 and HMIPv6. This is done by using the extensible implementation of MIPv6 (xMIPv6) for the OMNET++ simulation environment. The implementation mostly includes the modifications and supplements needed in order to provide the HMIPv6 functionality and giving the possibility to interoperate with MIPv6. We conduct our simulations over a realistic network topology leading to a series of interesting conclusions with respect to HMIPv6 performance merits under realistic assumptions.

Greek Abstract

Η σύγκλιση μεταξύ των ασύρματων τεχνολογιών και των τεχνολογιών Διαδικτύου έχει δώσει στο Πρωτόκολο Διαδικτύου (IP) κυρίαρχο ρόλο σε ότι αφορά την δρομολόγηση σε κινητά δίκτυα. Παρά την μεγάλη επιτυχία που γνώρισε το μοντέλο της στοίβας πρωτοκόλλων IP/TCP, υπάρχουν κάποια χαρακτηριστικά που δεν του επιτρέπουν να ανταποκριθεί στις απαιτήσεις που επιβάλλουν οι σύγχρονες ανάγκες (Δια)δικτύωσης. Μια από αυτές τις απαιτήσεις έχει να κάνει με υποστήριξη κινητικότητας σε δίκτυα IP, κάτι στο οποίο έχει δωθεί ιδιαίτερο ενδιαφέρον, τόσο από μέρους έρευνας αλλά και της βιομηχανίας, καθώς υπάρχει η τάση το πρωτόκολλο IP να αποτελέσει το βασικό πρωτόκολλο δικτύωσης ανεξαρτήτως αρχιτεκτονικής δικτύου (All-IP).

Παρά το γεγονός ότι υπήρχαν αδυναμίες για την υποστήριξη κινητικότητας σε IP δίκτυα, στο IPv4 έγινε η πρώτη προσπάθεια για υποστήριξη κινητικότητας σε επίπεδο δικτύου. Το πρωτόκολλο που σχεδιάστηκε για το σκοπό αυτό είναι το Mobile IP το οποίο αποτελεί λύση προσθήκης στο πρωτόκολλο IP. Στην επόμενη έκδοση του IPv4, δηλαδή του IPv6, η σχεδίασή της έγινε με τέτοιο τρόπο να ξεπεραστούν κάποιες από τις αδυναμίες που υπήρχαν πριν. Υπό αυτό το πρίσμα και έχοντας υπόψην την εξέλιξη προς All-IP δίκτυα, το IPv6 έχει προβλέψει και είναι πιο κατάλληλο για την υποστήριξη κινητικότητας. Το πρωτόκολλο Mobile IPv6 (MIPv6) είναι το πιο αντιπροσωπευτικό προτόκολλο που έχει προταθεί, με το Hierarchical MobileIPv6 (HMIPv6) να είναι είναι μια παρόμοια εκδοχή του πρώτου με καλύτερα ωστόσο χαρακτηριστικά.

Σκοπός αυτής της διπλωματικής εργασίας είναι να παράσχει μια ρεαλιστική σύγκριση μεταξύ των δύο προαναφερθέντων πρωτοκόλλων, του MIPv6 και του HMIPv6. Για το λόγο αυτό έγινε χρήση του πακέτου xMIPv6, που παρέχει την υλοποίηση του MIPv6 στο περιβάλλον προσομοίωσης του OMNET++ με τέτοιο τρόπο που δίνει τη δυνατότητα να γίνουν επεκτάσεις σε αυτό. Η υλοποίησή μας κατά κύριο λόγο περιλαμβάνει τις αλλαγές και προσθήκες που έπρεπε να γίνουν ώστε να υποστηρίζεται το HMIPv6 και να μπορεί να υπάρχει εναλλαγή με το MIPv6 όποτε αυτό απαιτείται. Τέλος διενεργήθηκαν πειράματα πάνω σε μια τοπολογία με ρεαλιστικά χαρακτηριστικά, οδηγώντας σε ενδιαφέροντα συμπεράσματα σε σχέση με τα οφέλη του HMIPv6 όταν λειτουργεί υπό ρεαλιστικές συνθήκες.

1. Introduction

Internet was created in times where the main goal was to support military and research purposes. This had a great impact on the design philosophy of the protocols used and as a result there is a close relation between these protocols and the initial objectives of the Internet [1]. However, since then there has been great evolution making the Internet an important component of mainstream society. We have moved to a point where it constitutes the main platform for commercial activities and broadband communications. As a result, there has been an increase in the number of different kinds of stakeholders which has been accompanied by the formation of a "tussle" environment [2].

This shift imposes new requirements on the Internet's technical architecture something which suggests revisiting some of the original design principles (such as end-to-end arguments) or even adopting new ones [2] [3]. This does not necessarily imply that the original Internet architecture suffered from bad design, but rather was oriented to meet different objectives. If it was not for Internet's great success, there would be no such need to improve its current architecture. In this context, the networking community has put into the foreground a discussion on how to move the field -and Internet itself- forward; either by following evolutionary approaches or clean-slate ones [4].

Over the past few years there has taken place a great increase concerning the number of portable devices connected to the Internet. As wireless technologies got cheaper, the bigger became the market of wireless communications, as well as the number of wireless networks that provided Internet connectivity. These trends have caused great attention to be shown on supporting mobility to such devices, i.e. the ability not to lose connection in application-level while changing point of attachment as they move on the Internet.

The convergence trend between Internet technologies and wireless networking has resulted in the usage of IP as the networking protocol for both fixed and mobile networks. However, mobility was not an issue provisioned by IP as initially IP networks aimed at providing end-to-end communication between hosts that had a fixed point of attachment on their local network. The main problem that exists is the dual role that IP addresses present. First, they are used to identify a specific end-system and second, are also used to find a route for packets destined to an end-point. This reality creates a contradiction for mobile computing, as on one hand there is the need to have stable IP addresses so that end-hosts are stably identifiable on the Internet, while on the other hand if the address is stable packets destined to a mobile node will end essentially to the same place despite of changing its point of attachment to the Internet.

Several approaches have been adopted in order to provide mobility in current Internet. The main differentiation between these approaches is related to the range of mobility each supports. On one hand, there are micro-mobility protocols that aim to provide mobility in a certain administrative domain, while on the other hand there are macro-mobility protocols dealing with mobility among different administrative domains. Mobile IP was proposed by the Internet Engineering Task Force (IETF) in order to provide global mobility at the network layer and offer mobile users a seamless computing environment as they roam through the Internet. Although its version for IPv6 (Mobile IPv6) represents a key element for future All-IP wireless networks, it has not yet been widely deployed as there are some technical obstacles, including routing issues, security, and handover performance as well. As a result, many protocols have been proposed trying to enhance its performance and functionality, sometimes extending or even co-operating with it.

In this work, we aim to perform a performance comparison between MIPv6 and its enhancement of Hierarchical MIPv6, in order to quantify the improvements it proposes. We use a simulation environment to evaluate each protocol, having designed a realistic scenario. The remainder of this thesis is organized as follows. We first provide an overview on the literature concerning mobility, both for IP-based Internet and future network architectures. Then a short description is given for MIPv4 and common features of the IPv6 in order to provide a better understanding of MIPv6 and HMIPv6 that follow next. The next section provides the description of the simulation scenario along with an analysis of the results. Finally we conclude and refer to plans on future work related to this topic.

2. Literature Overview

As the Internet evolved, one of its primary requirements that emerged was mobility support. The main problem related to IP mobility is the coupling of identity with location that is inherent in IP architecture. As a result, most approaches try to decouple these two properties in order to support mobility, having some of them providing quite good solutions. In the following lines we describe the main approaches that have been followed in order to provide mobility in current Internet architecture, as well as how mobility issues are addressed by the most well-known future Internet architectures.

2.1. Mobility in current IP-based Internet

An important part of research has been concentrated in a variety of approaches that provide mobility in different layers of the TCP/IP stack. The most significant protocol is Mobile IP with its first version being implemented for IPv4 (MIPv4 [5]). However its later version for IPv6 (MIPv6 [6]) receives bigger acceptance than its predecessor, as it inherits the benefits of the new IPv6 protocol. In MIPv6, mobility is supported at the network layer. Whenever a Mobile Node (MN) attaches to a foreign network, it assigns a new (local) address -Care-of-Address (CoA) - and informs its Home Agent (HA) -a router in its home network that intercepts packets to MN while it is away- about this new address. The concept is that it uses two addresses in order to provide the decoupling between identification and location. The address formed while in the home network -Home Address (HoA)- is used to define the MN's id, while the CoA is used to define the location of the MN in the visited network. As a result, packets destined to the HoA of the MN are routed to its home network, and if it is away, HA intercepts them to the CoA. The opposite route is followed when the MN send packets destined to its Correspondent Nodes (CNs). MIPv6 provides a native mechanism (unlike MIPv4) to handle this problem of triangular routing, by informing its CNs about the CoA it formed (Route Optimization). However, there are still problems concerning the overhead caused by packet encapsulation due to tunneling and the fact that it handles micro-mobility the same way it handles macro-mobility. For the last reason there have been enhancements to the protocol that handle micro-mobility in a more flexible way (such as Hierarchical MIPv6 [7]) and other exclusively micro-mobility protocols (such as Proxy MIPv6 [8]) that interoperate with MIPv6 in order to overcome its local mobility deficiencies.

Another effort to provide mobility, in transport layer this time, is the End-to-End Approach [9]. This is the first approach that utilizes the DNS service in order to track a mobile node's location. In this proposal, mobile nodes are identified by a domain name which is stable and they use Dynamic DNS in order to update DNS servers with the new addresses they form. To maintain TCP connections unaffected by roaming, a TCP Migrate option is used, so that MNs and CNs are

able to replace the IP addresses and ports in TCP 4-tuple in the middle of communication. The main problem here is that this scenario cannot work when both communication nodes are roaming simultaneously.

There has also been work to provide mobility in application layer, based on the signaling mechanism provided by SIP [10]. When a MN uses SIP-based mobility [11] it first uses normal SIP signaling procedure in order to establish a session with a CN. Then, each time the MN changes its IP address, it is responsible to inform its CN(s) about this change by sending RE-INVITE messages that reveal this new address. The home SIP server is also updated with the new location of the MN. However, the problem here is that this is not a suitable mechanism to maintain TCP connection while MNs move.

A different approach is that of Host Identity Protocol (HIP [12]) as it adds an additional layer (Host Identity layer) between the transport and network layers. The Host Identities are used to identify end-hosts, no matter if changes happen to their point of attachment on a network. These Host Identities are used by transport protocols and as a result communication is transparent to IP address changes. However, it is necessary that CNs get informed of IP changes, something which is done using UPDATE messages.

Except for the proposals that handle mobility in different layers of the TCP/IP stack, or even interpolating it with extra layers, IP multicast has been considered another solution to the issue of IP mobility. It presents some quite attractive characteristics as it is its inherent decoupling of identity from location that is offered by multicast addresses. Moreover it gives the possibility for more efficient use of network resources as there is no need to transmit duplicate packets when sending to more than one hosts at the same time. The approach of multicast mobility is based on the creation of multicast trees that expand their leaves in the visited network of a MN, thus offering the advantage of fast local handovers. However, despite the significant amount of research conducted on this area ([13], [14], [15], [16], [17]) it has not yet been widely used. Some of the main reasons include the fact that there are no benefits by partialy supporting IP multicast on the Internet, as well as the fact that there is not a commercial service to promote the deployment of this service model. More deployment issues for the IP multicast can be found in [18].

For a complete overview of proposed solutions for mobility support on the Internet since the early 1990s, the intrested reader can refer to [19].

2.2. Mobility in future Internet architectures

There is a significant body of research during the last years concerning content-centric or information-centric networking architectures. Such studies aim to improve current Internet's performance and overcome the deficiencies that it presents [20]. As expected, one of the issues

that these architectures meet is that of mobility. Below we describe briefly how mobility is addressed by some of the most known future Internet architectures.

Internet Indirection Infrastructure (i3) [21] is an overlay architecture that offers a rendezvous-based communication abstraction in order to solve the problems caused by point-to-point communication. Instead of sending a packet immediately from source to destination, packets are associated with an identifier which is used by receivers in order to indicate their interest to get it. Senders send packets to a specific rendezvous-point (infrastructure nodes), while receivers issue triggers on specific packet identifiers. Mobility is supported as by using these identifiers to obtain delivery of packets, the change in IP address is transparent to the sender. Moreover since each packet is routed to its rendezvous-point based on its identifier, no additional operation need to be invoked when there is a movement from the sender's part.

ROFL [22] (Routing on Flat Labels) is a routing algorithm based on Chord [23] in order to support both intra-domain and inter-domain routing. In case of intra-domain routing, a Chord overlay is formed within an autonomous system, while in case of inter-domain routing the Canon [24] scheme is used to allow for the creation of inter-domain paths, always following the existing routing policies. The concept here is that routing is based on flat labels, something that decouples network location from host identities. As a result, it merits all the advantages of this separation such as mobility, multihoming and stable identities.

DONA [25] is a clean-slate redesign just for Internet naming and name resolution, based on an overlay network of Resolution Handlers. DONA proposes an identification scheme that uses flat, self-certifying names in order to replace the DNS naming resolution that is responsible for corresponding names (URIs) to locations (IP addresses). This new "finding" mechanism, along with its advantages of facilitating the deployment of network caches, the establishment of multicast delivery trees and of the fact that it enables locating the nearest copy of the content by employing anycast, can support mobility in a more effective way by using current Internet's mobility solutions.

CCNx [26] is a research project, based on CCN architecture [27], that aims to provide a redesign of the Internet architecture with a content-centric view. This architecture introduces "Interest" packets that are used by consumers when asking for "Data" packets that include the desired information. Here a hierarchical naming scheme is followed, enabling aggregation of content names and as a result this reduces the forwarding state to be stored. CCNx supports mobility by providing caching mechanisms, by giving the ability to nodes to transmit "Interest" packets simultaneously from multiple interfaces and by having its transport layer designed to operate on top of unreliable packet delivery services.

Finally, another notable research project that aims at providing a new clean-slate Internet design based on the publish-subscribe communication paradigm [28] is PSIRP [29]. In PSIRP, each piece of information is labeled by using flat identifiers and ows a scope that defines the access rights on it or the context of the information. Mobility here is considered as a two-dimensional problem; the first dimension concerns the scale of mobility (micro or macro mobility) while the second one has to do with the way it is handled by the architecture (static or dynamic way). However, PSIRP handles mobility in a way that considers it to be a common feature which means that there are plenty of design decisions aiming at natively supporting it.

3. Background

In this section a description of Mobile IPv4 is given, as well as of the most important features of IPv6, in order to provide a better understanding on the way mobility is handled by MIPv6 and HMIPv6.

3.1. Mobile IP(v4)

Mobile IPv4 (MIPv4 [5]) is the first effort to solve the problem of mobility at the network layer. This approach seemed to provide the important benefit of application transparency which means that there is no need to modify applications in order to become mobile-aware. Moreover it does not suffer from scalability issues since it is based on IP, and is designed to allow mobile users to stay connected and maintain ongoing sessions by maintaining a permanent IP address. Mobile IP extends IP by allowing the mobile devices to use two IP addresses; the first to play the role of a (permanent) identifier and the second to be used for routing.

3.1.1. Functional entities and terminology

The following functional entities are in use in Mobile IPv4:

- **Mobile Node**: A host or router that changes its point of attachment from one (sub)network to another. A MN can continue to communicate with other Internet nodes as it changes location by using its permanent IP address.
- **Home Agent**: A router on the home network of a MN that intercepts packets to it while away from the home network, and keeps its location information.
- **Foreign Agent**: A router on a network that is visited by MN that cooperates with the Home Agent in order to deliver packets destined to it while in that network.

The table below provides definitions for some of the most commonly used terms in Mobile IP:

Table 1 - Mobile IP Terminology

Home Address (HoA)	*An IP address that is assigned for a long period of time to the Mobile Node and remains unchanged no matter if its location changes.*
Home Network (HN)	*A network that has a prefix that matches the prefix of the MN's Home Address. As a result traffic destined to HoA will end to*

	MN's Home Network
Foreign Network (FN)	*Any network except for the MN's Home Network*
Care-of-Address (CoA)	*The termination point of the tunnel that is set-up by Home Agent when intercepting packets to a MN away from its Home Network. Two types of care-of-addresses are defined: a "foreign agent care-of-address" is an address of a Foreign Agent with which the MN is registered; a "collocated care-of-address" is the local address assigned to an interface of the MN while in a foreign network.*
Correspondent Node (CN)	*Any host (fixed or mobile) with which the MN is communicating*
Agent Advertisement	*Messages used by Mobility Agents (Home and Foreign Agents) in order to advertise their presence on their links. They are created by adding an extension to ICMP Router Advertisements.*
Mobility Binding	*The association of a HoA with a CoA, together with the remaining lifetime of the association*

3.1.2. Mobile IP Overview

In this section a description is given for the three main functions that are part of the protocol. These are:

- **Agent Discovery**: Home and Foreign Agents advertise their availability for the links they provide services
- **Registration**: The process when a MN registers its care-of-address with the Home Agent while away from its home network.
- **Tunneling**: The set-up of a bi-directional tunnel from the Home Agent to the MN's care-of-address.

3.1.2.1. Agent Discovery

Both Home and Foreign Agents advertise their presence on their links by sending Agent Advertisements, which the MN listens to in order to determine whether it is located in its home network or if it has moved to another. Rather than waiting for receiving Agent Advertisement, the MN is capable of triggering mobility agents to transmit them by sending Agent Solicitation messages. Agent Advertisements carry information that specify whether an agent is a Home or

Foreign one (even both), its address, the type of tunneling and encapsulation provided, as well as the duration of the roaming period in a certain network.

When the MN realizes that it is connected to a Foreign Network, it acquires a care-of-address the type of which depends on the existence of a Foreign Agent. In case it is a foreign agent CoA, then it is the Foreign Agent that decapsulates traffic tunneled by the Home Agent and then forwards it to MN. The advantage of this method is that in this scenario such addresses can be used by other MNs too. In contrary, collocated CoAs are uniquely used by a MN that is also responsible for decapsulating packets destined to it.

3.1.2.2. Registration

This is a mechanism to enable MNs to communicate their current reachability information to their Home Agent. Registration sets-up or modifies a mobility binding at the Home Agent, by associating the MN's Home Address with its Care-of-Address for the specified lifetime. More specifically it is used by mobile nodes in order to:

- request forwarding services from their HA or FA while in a foreign network
- inform their HA for their CoA
- renew a registration that is about to expire
- deregister when returning home

While the MN is still at its Home Network, it is configured with is Home Address and the IP address of its Home Agent. When it visits a foreign network, the MN uses them combined with the information that it takes from Router Advertisements -or Agent Advertisements in case there is a FA- in order to form a registration request. Then it adds the registration request to its pending list and sends it to the HA, either through the FA (which first validates it) or directly in case it uses a collocated CoA and there is no requirement to use the FA.

When the HA receives the registration request, in its turn, validates the message and authenticates the MN in order to ensure that it originated form its network. If registration request is valid, the HA sets-up a mobility binding with the specific CoA, creates a tunnel towards that CoA, and forms a routing entry in order to intercept packets destined to MN's HoA through the tunnel. In the next step, the HA sends a registration reply to the CoA which means that in case it is a foreign agent CoA it will be received by the MN through the FA. FA validates registration replies and if no problems exist it adds the MN to its visitors' list, creates a tunnel to the HA and adds the necessary routing entries to forward packets to the MN and its HA.

Finally, when the MN receives the registration reply validates it and ensures that it comes from its HA. If validation is confirmed, then the MN can be sure that its mobility agents are informed

about its location information. Also, in case it uses a collocated CoA a tunnel to its HA must be established. Reregistration can take place when the registration lifetime is about to expire in order to update the existing mobility binding.

3.1.2.3. Tunneling

The MN uses its HoA as the source address of packets it sends to its correspondent nodes, thus giving the impression of being in its Home Network and making roaming transparent to them. Data traffic destined to the MN is routed to its Home Network where its HA intercepts packets to the CoA for which there is a mobility binding. This is done through the tunnel established after the registration procedure. While in foreign network the MN is given the possibility to route packets addresses to correspondent nodes either directly – or directly through the FA in case of a foreign agent CoA-, or it can follow the route through the established bidirectional tunnel.

The problem that is presented in the first occasion is that the source address of packets is topologically incorrect since it is the MN's HoA and if routers in foreign network implement ingress filtering, packets will be dropped. This is solved by reverse tunneling which indicates that outgoing traffic from the MN should be routed through the HA.

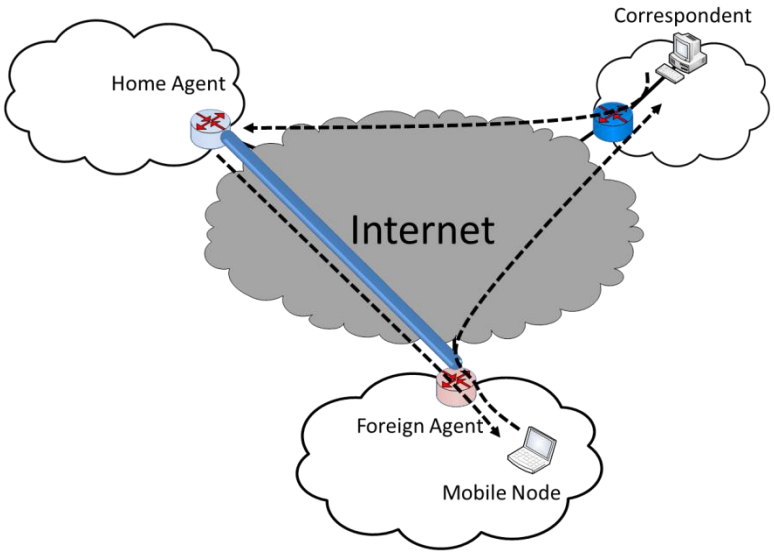

Figure 1 - Direct Forwarding

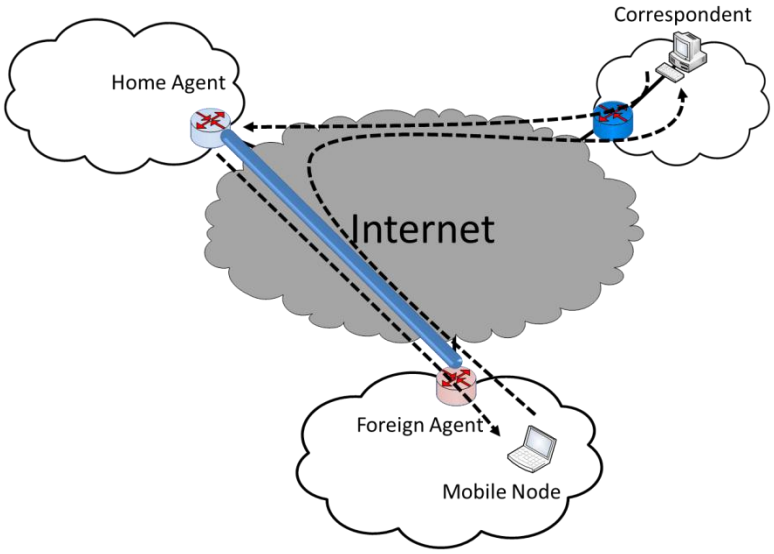

Figure 2 - Reverse Tunneling

3.2. Internet Protocol version 6 (IPv6)

IPv6 [30] is the latest version of the Internet Protocol aiming at replacing its predecessor IPv4. IPv4 is currently the basic mechanism in the TCP/IP stack to provide communication in global Internet and the fact that it has remained almost unchanged since it was first used in late 1970s, indicates that its design was powerful and flexible. However, Internet's evolution accompanied by its immense growth suggested that IPv4 should be replaced by a more efficient protocol. The main motivation for this change is lack of address space, as it was proved that 32-bit addresses cannot meet future requirements. Moreover other issues have emerged such as security, policing, resource handling etc. mainly imposed by new application needs.

3.2.1. IPv6 Features

IPv6 maintains most of the features that contributed to the success of IPv4. In reality, its philosophy remains the same, although it is designed to operate in a more efficient and flexible way. The main changes that are introduced by IPv6 can be grouped into 7 categories [31]:

- **Larger Addresses**: IPv6 uses an address space of 128 bits that does not seem to be easily exhausted in predictable future.
- **Extended Address Hierarchy**: Instead of having 2 levels like IPv4 (the first to define networks and the second hosts), in IPv6 more levels are introduced so that it can define a hierarchy of ISPs, as well as hierarchy within a domain.
- **Flexible Header Format**: Unlike the concretely fixed size of the IPv4 header, IPv6 introduces headers that can support a set of optional extensions.

- **Improved Options**: Except for the existing options in IPv4, IPv6 provides additional ones.
- **Provision for Protocol Extension**: IPv6 design is oriented to constitute a protocol that will allow for adding extra functionality and will not be hard to change.
- **Support for Autoconfiguration and Renumbering**: IPv6 provides mechanisms that facilitate computers on an isolated network to assign themselves addresses without any need of router or manual configuration. Also it allows a network administrator to renumber networks dynamically.
- **Support for Resource Allocation**: IPv6 provides two facilities for pre-allocation of network resources; one that provides a flow abstraction and another that resembles Differentiated Services in IPv4.

3.2.2. IPv6 Mechanisms

In this part it is considered essential to provide a short description of the IPv6 mechanisms that underlie mobility in IPv6 networks. A description is given for the address configuration mechanisms in IPv6 (stateless [32] and stateful [33]), as well as for Neighbor Unreachability Detection and Address Resolution that are included in Neighbor Discovery [34] specification.

3.2.2.1. Address Autoconfiguration

IPv6 enables network interfaces to acquire more than one network addresses. Address configuration specifies the process of creating a valid address on a certain network interface and it includes two main approaches, stateless and stateful address configuration.

Stateless address configuration enables host to generate their addresses by combining the prefixes advertised by local routers with their interface identifiers. Without advertised prefixes, hosts can only form a link-local address that allows them to communicate on their link. However, before link-local addresses are assigned to the specific network interface, a mechanism is activated called Duplicate Address Detection (DAD) in order to certify the uniqueness of the address. If link-local is unique, then by using the right prefix a node can assign other types of addresses (global unicast, site-local etc.) that are unique too.

In stateful address configuration, hosts acquire their address configuration information from a server. Such servers specify the addresses that can be used by each hosts and keep archive of these associations. This mechanism can be recognized as DHCPv6.

3.2.2.2. Neighbor Discovery

The Neighbor Discovery (ND) protocol enables IPv6 nodes to learn the link-layer addresses of their neighbors and keep track of their reachability, as well as discover routers that will forward their packets. The basic messages used in Neighbor Discovery are the following:

- **Router Advertisement**: Periodically generated messages by routers, in order to advertise their availability on their links.
- **Router Solicitation**: This message is sent in order to immediately generate Router Advertisements from a router, rather than waiting for its time to come.
- **Neighbor Solicitation**: This message is sent by an interface in order to determine the link-layer address of a neighbor or that it is still reachable. These messages are also used during Duplicate Address Discovery.
- **Neighbor Advertisement**: This message is sent in response to a Neighbor Solicitation. It is possible for a node to send unsolicited Neighbor Advertisements in order to inform its neighbors for changes in its link-layer addresses.

Neighbor Unreachability Detection verifies that two-way communication with a neighbor node exists. The host sends a neighbor solicitation to a node and waits for a solicited neighbor advertisement. In case a solicited neighbor advertisement is received, the node is considered reachable. If there is no immediate response, the host can repeat this process before it declares a neighbor unreachable. Else if a neighbor is found to be unreachable, the corresponding neighbor cache entry is deleted.

The Address Resolution procedure in IPv6 corresponds to ARP mechanism of IPv4. The host sends a neighbor solicitation to a solicited-node multicast address and waits for a response for a period of time. If one is received, then the link-layer address contained in the neighbor advertisement is cached and any queued packets are sent to the address. If there is no response, the host repeats this process up to three times before it declares that a neighbor is unreachable.

4. Mobile IPv6 (MIPv6)

The new version of the Internet Protocol (IPv6) gave new opportunities in supporting mobility for IPv6 nodes. The Mobile IPv6 protocol [6] takes advantage of the enhancements provided by IPv6 and provides transparent routing of packets for IPv6 nodes. In MIPv6 each MN is always identified by its Home Address, no matter if it changes its current point of attachment on the Internet. While away from its home network, a MN is always associated with a Care-of-Address that indicates its current point of attachment. The main advantage that it provides, in opposition to MIPv4, is an inherent mechanism that allows IPv6 correspondent nodes to learn and cache the CoA of a MN, which is then associated with its HoA, and packets can be sent directly to MN thus avoiding triangle routing.

4.1. Functional entities and terminology

The following functional entities are in use in MIPv6:

- **Mobile Node**: A node that can change its point of attachment from one link to another, while remaining reachable by using its HoA.
- **Home Agent**: A router on the home network of a MN that intercepts packets to it while away from the home network, and keeps its location information.

We observe that, unlike IPv4, there is no need for a Foreign Agent in the visited network. However it is necessary for MIPv6-aware nodes to implement some additional data structures. These are the following:

- **Binding Cache (BC)**: This data structure is maintained by Home Agents and Correspondent Nodes that want to support Route Optimization, i.e. the ability that packets destined to a MN will be routed directly to it and not through the Home Agent. Information kept in Binding Caches includes the HoA of the MN for which is the BC entry, its CoA, as well as the remaining lifetime for that entry.
- **Binding Update List (BUL)**: This data structure is maintained solely by Mobile Nodes and records information for each Binding Update (see terminology next) sent either to a HA or a CN. For multiple Binding Updates sent to the same destination only the most recent is kept. Information that is kept in each entry of the BUL includes the destination address of the Binding Update, the HoA for which that Binding Update was sent, the current CoA when the MN sent it, as well as the remaining lifetime of that binding.
- **Home Agents List (HAL)**: This data structure is maintained by each HA, keeping information about each router on the same link acting as a HA. It is used by the Dynamic

Home Agent Address Discovery mechanism that will be described next. Every HA maintains a separate Home Agents List for each link on which it provides service. Each entry in the HAL includes the following fields; the link-local address of the HA on its link, one or more of its global IP addresses, the remaining lifetime of the entry, as well as the preference value for this HA.

Terms needed in order to describe basic MIPv6 functionality remain the same as in **Table 1**.

4.2. Mobile IPv6 Overview

The main procedures that need to be described in order to provide a good understanding of how MIPv6 works is Home Agent Registration, Route Optimization and Home Agent Discovery. We will consider that MNs configure their IP address with stateless address configuration and that CNs support Route Optimization.

4.2.1. Home Agent Registration

While a MN is still at its Home Network, it receives Router Advertisements from its HA and configures its IP address according to the prefixes advertised. When it moves to a Foreign Network, the MN receives Router Advertisements from the router on its link that has an unknown prefix and understands that it has left its Home Network. Then the MN starts serverless address autoconfiguration and after it performs Duplicate Address Detection it assigns it on the specific interface. Now the MN has its CoA ready for use and starts the Binding procedure.

The MN sends a Binding Update to its Home Agent containing an IPv6 Destination Option (Home Address Option) that carries its HoA. The HA validates the BU and if no problems exist, gets from the source address of the BU the new CoA of the MN and creates a new Binding Cache entry. In the next step the HA replies with a Binding Acknowledgement that is destined to the MN's CoA, but carrying a Routing Header containing MN's HoA. The HoA will be used by the MN to replace the CoA on the Destination Address field of the BU, so that traffic seems as if the MN was still at its Home Network. If the Binding Acknowledgement was valid too, the MN adds (or updates if there was a previous entry) a Binding Update List entry and informs the rest of the nodes in BUL by sending them Binding Updates.

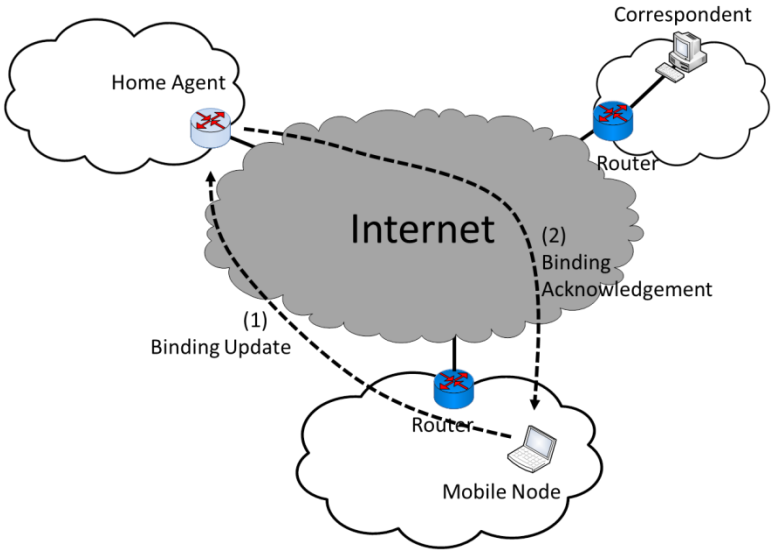

Figure 3 - Home Agent Registration

4.2.2. Route Optimization

After the HA adds or updates an entry in its Binding Cache, it intercepts packets destined to the corresponding MN by tunneling them to its CoA. Normally the MN uses its HoA as the source address of the traffic it sends to its Correspondent Nodes, except for some cases of short-term communication where it uses its CoA. When the MN uses its HoA as the source address, it has two ways to transmit packets. The first one is by Reverse Tunneling which means that packets will be tunneled first to the HA with outer source address the MN's CoA. At the HA, packets will be decapsulated and sent to the CNs. However this approach presents the same problem as in MIPv4, called Triangular Routing.

The second way, called Route Optimization, gives a solution to this problem provided that Correspondent Nodes have route optimization support (as we suggest). In this occasion, when the MN first receives a packet from a CN that it has not a binding with, it starts the Return Routability (RR) Procedure. RR begins by sending two messages to the CN, one directly to it (CoTI) and one through the Home Agent (HoTI). The purpose of this is to assure the CN that the MN is really the one that claims (HoTI message must be validated by HA). Then the CN responds to each of these messages with a CoT and HoT message that will be routed directly and through the HA respectively. By combining information carried by both CoT and HoT messages, the MN sends a Binding Update to the CN providing this information in order to authenticate itself. When the CN receives this BU and checks that it is valid, adds an entry on its Binding Cache and responds with a BA. The MN receives the BA and if it is valid too, adds an entry to its Binding Update List. Now that Route Optimization is enabled, CNs can send packets directly to the MN by using Type 2 Routing Header, while the MN uses the Home Agent Address Option.

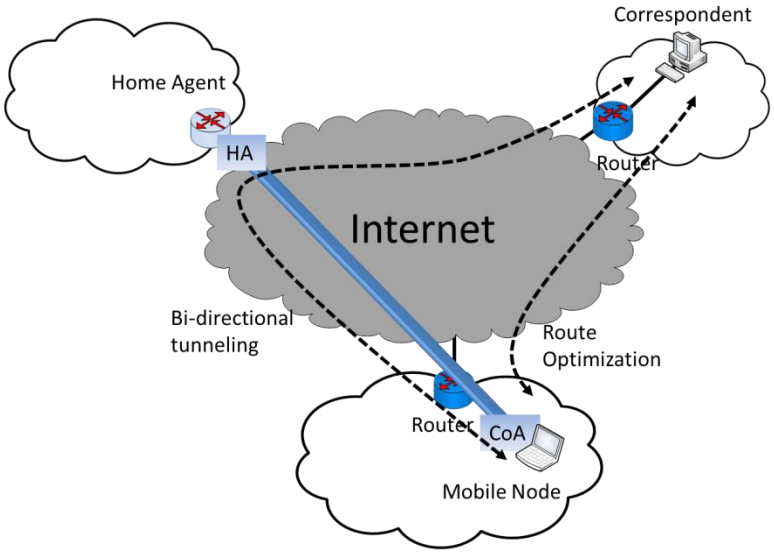

Figure 4 - Route Optimization

4.2.3. Home Agent Discovery

There may occur circumstances where the MN does not know the IP address of its HA. This can happen if nodes on its home link have been reconfigured while the MN has been away from home, causing the router operating as the MNs home agent to be replaced by another router. MIPv6 has defined the Dynamic Home Agent Discovery mechanism to deal with these situations. This procedure allows the MN to dynamically find routers serving as HAs on the MNs home network.

The MN attempts to find a designated HA by sending an ICMP Home Agent Address Discovery Request message to the home agent anycast address on its home network. It uses its CoA as the source of this message. All home agents serving this subnet receive the message and should reply with one of its global unicast addresses to the MN's CoA, thus letting the MN find its IP-address.

4.3. Comparison between MIPv6 and MIPv4

MIPv6 design presents a list of benefits that originate from the experience gained from the previous version of MIPv4, as well as from the advantages that IPv6 provides. Although MIPv6 has in common many features that exist in the Mobile IP version for IPv4, its main difference is that it is integrated into IPv6 rather than extending it. Practically this is achieved as mobility support in IPv6 is provided clearly in IP layer by use of Destination Options and Mobility Headers that enlarge the IP packet. On the other hand, in IPv4 mobility is supported by new types of messages originated from transport layer (UDP signaling).

The major differences between MIPv6 and MIPv4 are the following ones:

- Mobile IPv6 operates in any location on the Internet as there is no need for a special router, as it is a Foreign Agent in MIPv4.
- Support for Route Optimization is fundamental part of the protocol, rather than a nonstandard set of extensions. It can be also efficiently handled by routers implementing ingress filtering.
- MIPv6 utilizes IP Security for all security requirements for Binding Updates, unlike MIPv4.
- MIPv6 implementation is more robust and simplified due to the existence of Neighbor Discovery mechanism that removes any concern related to the link layer, unlike in MIPv4 where there is ARP.
- The inherent feature of Route Optimization along with the usage of IPv6 Routing Headers, rather than using IP encapsulation, reduces the resulted network overhead compared to MIPv4.

5. Hierarchical MIPv6 (HMIPv6)

Hierarchical MIPv6 [7] is an extension of MIPv6 that also allows for efficient local mobility handling, unlike MIPv6 that was developed only with global mobility in mind. HMIPv6 uses MIPv6 to handle global mobility, while local handovers are managed locally and in a transparent way. This protocol is designed to reduce the amount of signaling between a Mobile Node, its Home Agent and its Correspondent Nodes, as well as reduce handover latency while a MN performs handovers on the same site.

5.1. Functional entities and terminology

HMIPv6 introduces a new entity called Mobility Anchor Point (MAP) that is responsible for handling movements of a MN while in a local site. A Mobility Anchor Point is a router located in a visited network and acts like a local Home Agent for the MN. One or more MAPs can exist within a visited network. Home Agent and Correspondent Node operations are not affected by the new protocol (in relation to MIPv6), while minor extensions are needed to the Mobile Node operation.

The following table provides definitions for the most common terms introduced by HMIPv6:

Table 2 - HMIPv6 Terminology

Access Router (AR)	*The MN's default router that is on the same link while in a visited network. Access Routers are configured to advertise MAPs' prefixes (including their own) that can provide service to them.*
Regional Care-of-Address (RCoA)	*A CoA allocated to the MN, based on the MAP's advertised prefix by the Access Router.*
On-Link Care-of-Address (LCoA)	*A CoA configured on a MN's interface based on the prefix advertised by its default router (AR).*
Local Binding Update (LBU)	*The MN sends a Local Binding Update to the Mobility Anchor Point in order to establish a binding between the LCoA and RCoA.*

5.2. Hierarchical MIPv6 Overview

When the MN enters a MAP domain it will receive Router Advertisements from its Access Router containing information about one or more local MAPs (MAP Discovery phase). Such information is included in the MAP Option, a Neighbor Discovery Option, with more significant fields being MAPs' global addresses, the distance (in hops) from the MAP and a preference indicator. At this point the HMIPv6-aware MN is able to configure its CoAs. It forms an On-Link CoA (LCoA) that indicates the location of the MN on the local network, and a Regional CoA (RCoA) based on the selected MAP prefix that will be used to provide transparency as it moves under this MAP domain (the protocol enables more than one RCoAs to be formed, belonging to different MAPs).

After the MN has assigned these addresses to its network interface, it sends a Local Binding Update to its MAP in order to create a binding between its LCoA and RCoA. The procedure is similar to the MIPv6 binding but now the MN uses as a HoA its RCoA, while it uses as a CoA its LCoA. If the MAP validates this binding it replies with a Binding Acknowledgement. Following a successful registration with a MAP, a bi-directional tunnel is established between the MN and the MAP in order to tunnel all traffic destined to, or originating from the MN. What remains now is the registration of the MN's RCoA with its HA and other entries in its Binding Update List. For these Binding Updates the MN uses its HoA in the Home Address Option and the RCoA as the CoA in the source address field.

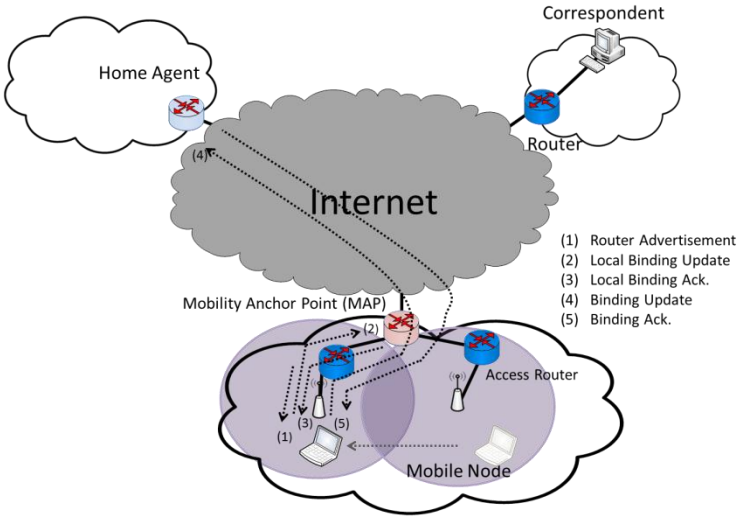

Figure 5 - HMIPv6 Signaling

As a result, all traffic destined to the MN's RCoA is intercepted by the MAP and tunneled to its LCoA. Moreover, all traffic originating from the MN is tunneled first to the MAP. The outer header contains the MN's LCoA in the source address field and the MAP's global address in the destination address field. As for the inner header, contains the RCoA as source address and the CN's address as destination. The profits gained from HMIPv6 are based on the fact that the RCoA does not change as long as the MN remains inside the same MAP domain. In case the MN changes an AR in the same location only the MAP must be informed of its new LCoA, which makes mobility transparent to CNs it communicates with.

Finally, when the MN moves into a new MAP domain, it may request from its previous MAP to forward packets to its new LCoA in order to reduce losses concerning the packets that are already transmitted towards its previous RCoA. This is to provide smoother inter-MAP handoffs, however it may be blocked by network administrators in case the new LCoA is outside a MAP's domain.

6. Performance Analysis

6.1. Simulation Setup

In order to carry out the performance comparison between MIPv6 and HMIPv6 we worked on the open-source OMNeT++ simulation platform [35]. We used its 4.1 release and installed it into a machine running Ubuntu 10.04.3. The packet used was xMIPv6 [36] which is an extensible Mobile IPv6 simulation model based on the INET framework. The INET framework is an open-source communication networks simulation package for the OMNeT++ environment. It contains models for several networking protocols and this feature is used to provide realistic results, as mobility protocols have to operate under the interference factor imposed by other protocols of the TCP/IP stack.

In our simulation we used a simple network topology however it was designed to be large enough to acquire realistic measurements. **Figure 6** below depicts the network topology for the simulation scenarios.

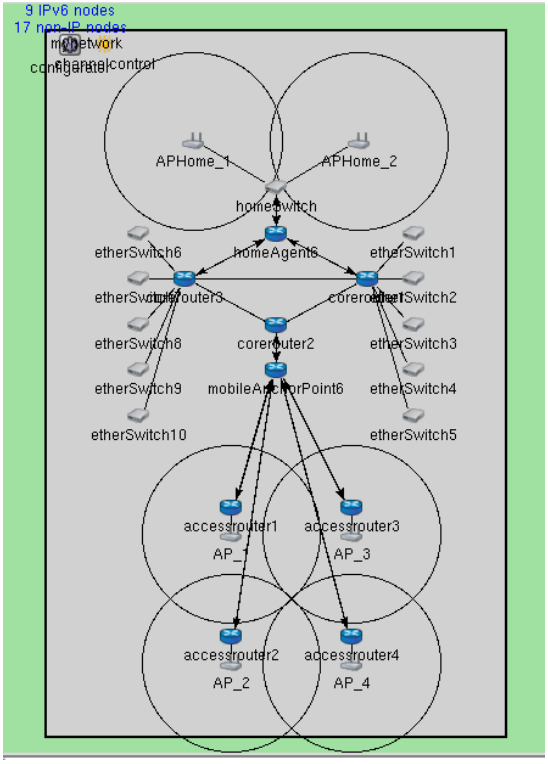

Figure 6 - Simulation Network Topology

6.1.1. Network topology

The chosen scenario is composed by the home network, the foreign network, a set of correspondent nodes' networks and core routers that model Internet by adjusting link delays. The home network consists of two access points, while in the foreign network we have four access points, each connected to a different access router. The Mobility Anchor Point operates as a casual router in case no HMIPv6-aware nodes exist.

The micro-mobility domain (MAP, access routers and access points) has been designed to provide coverage to an area of about 400 square meters, having each access point to have a range of approximately 150 meters. Each wireless device (access point and mobile nodes) owns an IEEE802.11g radio interface, with neighboring APs configured to be synchronized in different channels. When HMIPv6 scenarios considered, access routers are configured with the global IPv6 address of the MAP and propagate it through their Router Advertisements, extended with the MAP Option. In reality too, this configuration is done manually as there is not yet a protocol that allows MAPs to communicate such information to their access routers. Wired links inside the MAP domain are modeled as 100 Mbps Ethernet links with 0.3ms delay. The links between the home network switch and the home network APs, as well as between the other switches and correspondent nodes, are also modeled as 100 Mbps Ethernet links with 0.3ms delay. For the rest of the network topology, same bandwidth is used but link delay is increased on each link to 2ms.

6.1.2. Simulation scenario

Our results are based on multiple scenarios (30 iterations for each) of having initially one MN receiving traffic from its CN, that starts from the home network and then roams among the four access points of the visited network. The number of total MNs inside the foreign network, as well as CNs, is increased in each different scenario by 10 in order to see how the initial MN is affected by the presence of the others inside the visited network. To acquire more realistic results, half of these MNs send data to CNs out of the visited network, while the others receive data from CNs. As a result, the initial MN will have to receive packets from shared router queues, as well as compete with other MNs that send traffic using the same access point it is associated with. In our simulation all moving MNs have the same handoff rate, performing 3 handoffs per minute with an average speed of 10m/s.

The type of sources used in our simulations, are two different UDP CBR sources. The first one is based on a simple application scenario where the CN of the initial MN sends UDP datagrams resembling traffic generated from a VoIP application that uses G.711 codec sampling at 20ms. This generates 50 frames of data per second, each frame containing 160 bytes of payload. For the rest of mobile nodes inside the visited network, we use the second UDP source and have half of them receiving traffic while the others send traffic to their CNs. For this source, as ITU-T specification for conventional speech suggests [37], we consider an average talk spurt of

38.57% for their communication and we create a network workload corresponding to the bi-directional VoIP traffic for these communication pairs (i.e. each sender, either it is a MN inside the visited network or a CN form outside, transmits 18 packets per second). As a result, we can study the performance metrics as observed by the initial MN receiving VoIP traffic corresponding to "on" periods of its transmitter, but affected by the background workload created by the other nodes.

Finally, all simulations are having a duration of 140 seconds and a warm-up phase of 35 seconds, that allows for MNs to move from the home network to the foreign one and register with their Home Agent. As a result performance metrics deal only with a scenario where MNs move in one foreign network, i.e. without returning home or visiting other foreign networks.

Table 3 - Simulation Parameters

Simulation duration	*140 sec*
Warm-up period	*35 sec*
Number of interfering MNs	*0(10)…50*
MNs speed	*10m/s*
Handover rate	*3 handovers/min*
Delay for core links	*2 ms*
Delay for Ethernet links	*0.3 ms*
VoIP packet payload	*160 bytes*
VoIP traffic towards initial MN	*90 kbps (approx.)*
VoIP background traffic (per transmitting node)	*35 kbps (approx.)*

6.1.3. Performance metrics

The goal of this performance comparison is to evaluate the improvements that HMIPv6 offers in comparison to the simple MIPv6.The parameters we study are the following:

Handoff Latency : Handoff latency is the time that elapses between the last packet that a MN received through its old CoA in MIPv6 (or LCoA in HMIPv6) and the first packet after it has moved to another network and has formed a new CoA (or LCoA). During this period no packets

are received and this packet drop results to a disruption in communication. Seamless roaming requires that users and applications do not experience loss of connectivity or any noticeable interruption in traffic. However this depends on various parameters having mainly to do with the mechanisms used in order to acquire Layer-2 and Layer-3 connectivity, as well as the time needed to create new (or update) mobility bindings (registration delay). In our simulations active scanning is used for a MN in order to associate with its access point, while for address configuration, stateless address autoconfiguration is used and more specifically Optimistic Duplicate Address Detection (ODAD). In [38] the interested reader can find a set of different MIPv6 handover extension schemes along with their performance evaluation. In our simulations we study handoff latency for the VoIP source received by the initial MN, while the number of MNs inside the visited network increases.

Packet Loss: Packet loss is defined for a receiving MN as the number of lost packets during the handover period. Although it may be assumed that they are proportional to handover latency, this is not always true as this number can be affected by network congestion and the queuing/bursting mechanisms on each router. Packet losses may happen to the Home Agent when it has not yet established a mobility binding with a MN after it has left home network, to a MN's previous Access Router, as well as to its previous MAP if it receives packets for a MN that has previously deregister from it. In our simulations we study the total number of packets losses for the VoIP source received by the initial MN, while the number of MNs inside the visited network increases.

Signaling Load: Signaling load is defined as the number of Binding Updates and Binding Acknowledgements transmitted during the simulation. In our simulations we study signaling load for the total of MNs inside the foreign network as they have the same handoff rate (3 handovers per minute). In the case of HMIPv6 we do not need to make the separation between signaling load inside and outside the MAP domain, as roaming takes place in one MAP domain and thus no signaling is required to be transmitted outside.

6.1.4. Implementation Restrictions

In xMIPv6 implementation, there were some features that limited us to design the simulation scenario in a specific way. As also mentioned in xMIPv6 overview in [36], Neighbor Discovery should be improved in order to support mobility in a better way. It was found that only Duplicate Address Discovery was implemented and there was not effective usage of Neighbor Cache. This means that when a MN that is sending traffic to its correspondents does not use its newly formed CoA as it should, but the previous one. This led to having MNs that send traffic to CNs without performing handoffs, but on the other hand having fixed positions evenly distributed among the foreign network's access points. Only the MNs that receive traffic from CNs are in position to roam.

Another restriction is that the implementation of xMIPv6 enforces usage of Route Optimization and thus packets are not sent through the tunnel between a MN and its HA. Moreover there was a problem with the association of a MN under a new access point. In case the MN disassociates with its previous AP and gets to an area that there is coverage by more than one APs, simulation crashes and this is due to lack of an algorithm for access point selection in Wi-Fi environment. As a result, we were urged to provide our MNs mobility traces so as to avoid entering areas with coverage by multiple access point, which in our topology means that MNs do not move near the center of the area that cover the four access points of the visited network.

6.2. Simulation Results

In this section we study the mentioned performance metrics for the simulation scenario we described in the previous section.

6.2.1. Handover Latency and Packet Loss Evaluation

We present here the results concerning the impact of the number of MNs competing with our initial MN, on the parameters of handover latency and packet loss. The values used in the graphs correspond to the mean values of the performance metrics (after 30 repeats of the simulation) from the point of view of the initial MN.

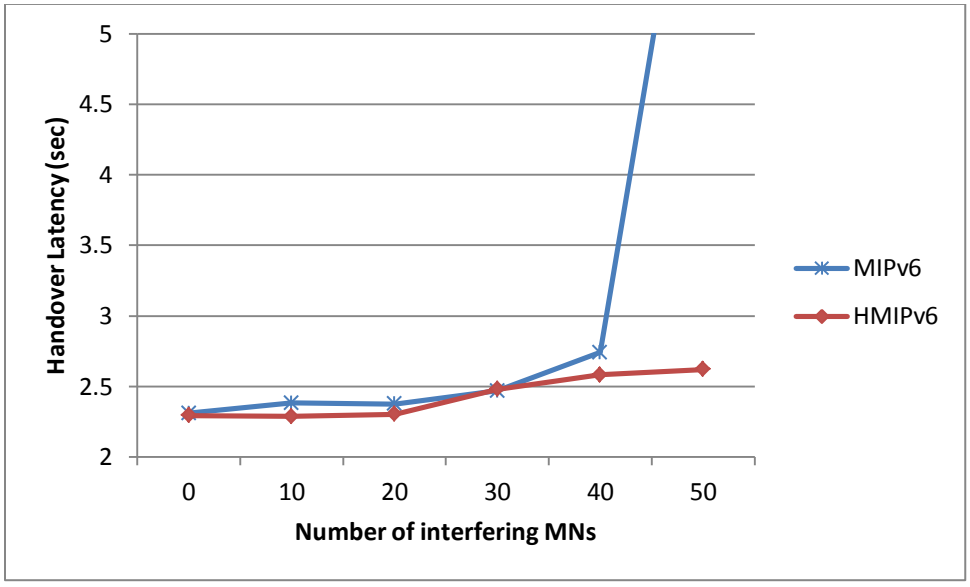

Figure 7 - Impact of number of MNs on handover latency

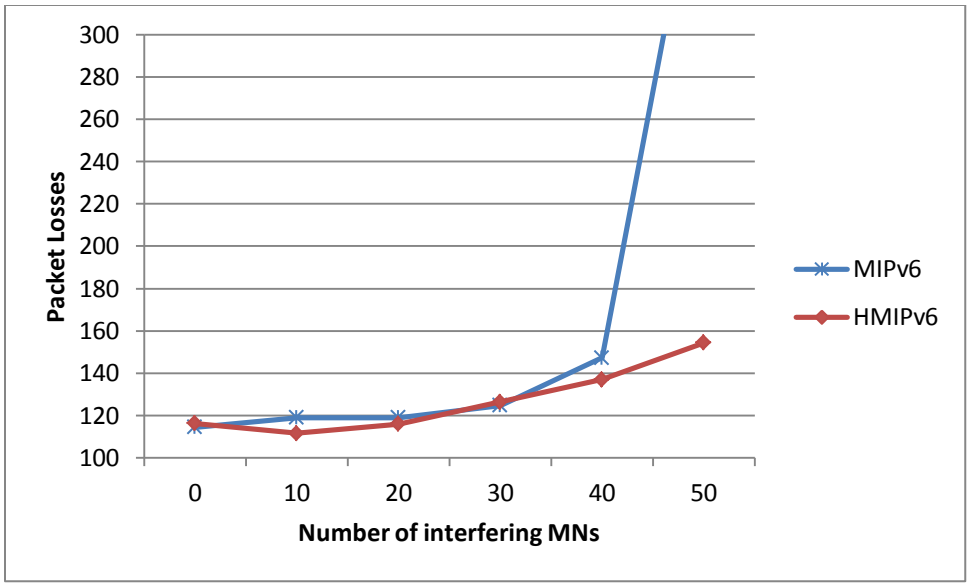

Figure 8 - Impact of number of MNs on packet loss

As we can observe, for a small number of MNs the results we obtain seem to follow our expectations. For up to 20 MNs, HMIPv6 handover latency and packet losses outperform MIPv6 ones, since the dominant factors that affect them have to do with the delays imposed by the wired links and packet processing by routers. In HMIPv6 the MN needs only to send its (Local) Binding Updates to the MAP, in contrast with MIPv6 where BUs need to be sent both to the HA and its CN outside the MAP domain. However an exceptional situation takes place when the number of interfering MNs reaches 30 inside the foreign network. This is a case presented also in [39], indicating that there can be a point where MIPv6 performs slightly better than HMIPv6. On this point, the delay imposed by the tunneling mechanism of the MAP, as well as the link and channel delay because of the additional load of 40 bytes in each encapsulated packet inside the MAN domain, lead to HMIPv6 worst performance. Despite that, it is in our assessment that MIPv6 outperformance can be reversed in case of longer distance between the home and foreign network, and higher traffic in core routers as well. This is to be empowered by the effect that has on our metrics the increase to 40 or 50 MNs inside the foreign network. We observe now that HMIPv6 clearly outperforms MIPv6 metrics, having a much smaller impact than MIPv6, both in handover latency and packet loss. Of course there is a degradation in HMIPv6 performance due to link delays caused by the increase in traffic inside the MAP domain, however it is not the same as in MIPv6 scenarios where BUs have to be processed by a number of busy core routers and traverse wired links with increased traffic, thus delay.

6.2.2. Signaling Load Evaluation

In this section we provide the results concerning the signaling load (number of Binding Updates and Binding Acknowledgements transmitted) due to handovers inside the foreign network by all MNs (unlike in previous metrics that we used only the initial MN as a reference point).

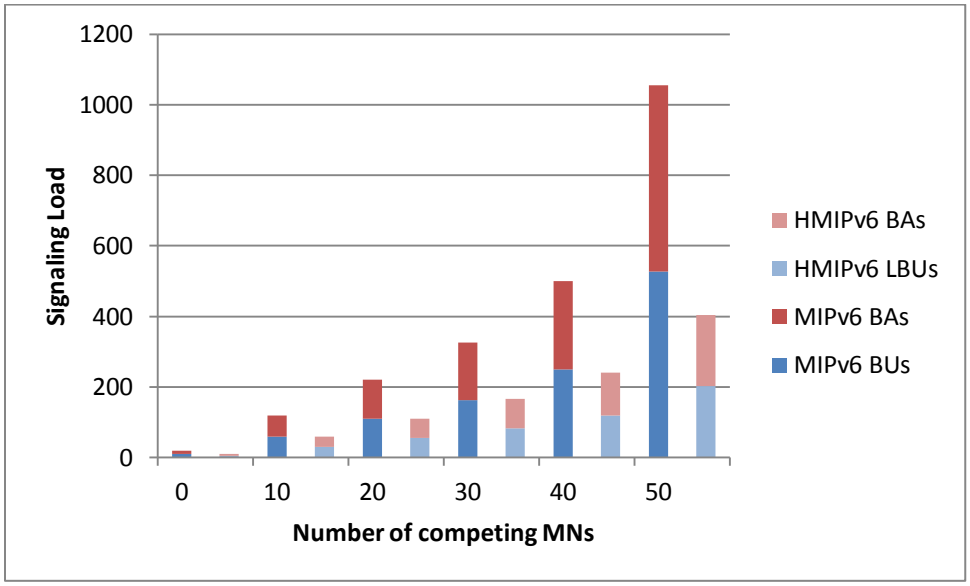

Figure 9 - Signaling Load

One of the advantages of HMIPv6 is the fact that when a HMIPv6-aware MN performs a local handoff inside a MAP domain, it needs to inform only its MAP about a change in its point of attachment by sending a (Local) Binding Update with its new LCoA. This is of significant importance especially when the number of CNs in its Binding Update List is big. Unlike HMIPv6, when a MN supports MIPv6 needs to inform each time it changes point of attachment both its HA, as well as all its CNs. This results to having BUs transmitted over the Internet, which in their turn generate BAs from the HAs and CNs too. This signaling overhead may prove crucial in case MIPv6 meets a wide deployment on the Internet, and is caused by the fact that micro-mobility is handled the same way as macro-mobility. However, also when HMIPv6 is supported we can have BUs transmitted to HAs and CNs but this is the case when a MN changes MAP domain or it needs to refresh the binding lifetime for a BUL entry.

In our simulations we have one CN for each MN. This means that we expect that the signaling load in MIPv6 will be double than in HMIPv6. This assumption is met for having up to 30 interfering MNs inside the visited network. After this point, it may be necessary for both protocols to retransmit BUs as they do not always receive a BA in time (retransmission timer is

set to 1 sec). This is because collisions may take place in the wireless link as MNs compete to transmit packets to their access point, as well as because there is much traffic in routers and packets have to wait in their queues. The last seem to be the dominant factor in MIPv6 retransmission of BUs, as depicted by the great increase in signaling load when having 50 interfering MNs.

7. Conclusions and Future Work

MIPv6 has a significant role to play in future All-IP wireless networks, as it represents the basic protocol that will provide mobile users the ability to roam between different domains. In this thesis we provide a performance comparison between MIPv6 and its basic enhancement of HMIPv6 through a study via simulation. We used the OMNeT++ simulation framework and worked on xMIPv6 package that provides an extensible Mobile IPv6 simulation model on top of INET. For our purposes a set of improvements was made on this packet (especially in order to enable multiple handovers between different networks) as well as we extended it with the implementation of HMIPv6.

Specifically, we performed a "stress-test" between these protocols and studied how handoff latency and packet losses are affected by increasing the number of interfering mobile nodes inside a foreign network, as well as the total signaling load produced in each case. Realistic conditions were taken into account for our simulation scenarios in order to obtain accurate results. Competition among MNs for the wireless medium, existence of core routers with increased link delays, layer-2 and layer-3 protocol interactions with MIPv6 and HMIPv6, as well as usage of realistic VoIP sources, are only some of them.

In our results, HMIPv6 proves its better performance in relation to MIPv6. In general, the fact that it handles local mobility in a flexible way, unlike MIPv6 that handles it the same way as global mobility, brings it to an advantageous position. However, the fact that it burdens packets inside the MAP domain with the additional 40 bytes of the encapsulation header due to tunneling, creates more workload inside the foreign network which means greater competition for the access medium and faster achievement of saturation point (especially on wireless links). Taking also into account the packet-processing delay due to the tunneling mechanism on the MAP, there can be a point that MIPv6 slightly outperforms HMIPv6. Soon after that, HMIPv6 gains again in terms of handover latency and packet loss as in MIPv6 registration delay is significantly increased because of the busy core routers. Finally, it was clear that HMIPv6 provides a more light signaling mechanism, both in terms of reducing the number of packets that need to be transmitted and traffic sent to the core network as well.

Several micro-mobility protocols have been implemented in order to provide mobility in a particular administrative domain. Some of them are in position to interoperate with MIPv6, such as Proxy Mobile IPv6, thus providing improvements to MIPv6 performance. Significant research has also been made in providing mobility for future network architectures and paradigms such as Publish/Subscribe. Since mobility appears to be a necessity in future networking environments it is very important to provide a performance comparison between

these approaches. Consequently, this field can be offered for lots of research to be conducted on proposed approaches as well as conceiving new ones.

Acronyms

AP Access Point

BA Binding Acknowledgment

BU Binding Update

CCN Content Centric Networking

CN Correspondent Node

CoA Care of Address

CoT Care-of Test

CoTi Care-of Test Init

DONA Data-Oriented and beyond Network Architecture

HA Home Agent

HoA Home Address

HIP Host Identity Protocol

HMIPv6 Hierarchical MIPv6

HoT Home Test

HoTi Home Test Init

i3 Internet Indirection Infrastructure

LCoA On-Link Care-of Address

MAP Mobility Anchor Point

MIP Mobile IP

MN Mobile Node

RCoA Regional Care-of-Address

RO Route Optimization

ROFL Routing on Flat Labels

SIP Session Initiation Protocol

Bibliography

[1] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," *Computer Communication Review*, vol. 18, no. 4, pp. 106-114, August 1988.

[2] David D. Clark, John Wroclawski, Karen R. Sollins, and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," in *SIGCOMM*, Pittsburgh, 2002, pp. 347-356.

[3] Marjory S. Blumenthal and David D. Clark, "Rethinking the Design of the Intrnet: The End-to-End Arguments vs. the Brave New World," *ACM Transactions on Internet Technology*, vol. 1, no. 1, pp. 70-109, August 2001.

[4] Jennifer Rexford and Constantine Dovrolis, "Future Internet Architecture: Clean-Slate Versus Evolutionary Research," *Communications of the ACM*, vol. 53, no. 9, pp. 36-40, September 2010.

[5] C. Perkins. (1996, October) IP Mobility Support. RFC 2002.

[6] D. Johnson, C. Perkins, and J. Arkko. (2004, June) Mobility Support in IPv6. RFC 3773.

[7] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier. (2008, October) Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC 5380.

[8] Ed. S. Gundavelli et al. (2008, August) Proxy Mobile IPv6. RFC 5213.

[9] Alex C. Snoeren and H. Balakrishnan, "An End-to-End Approach to Host Mobility," in *ACM MobiCom*, Boston, 2000, pp. 155-166.

[10] J. Rosenberg et al. (2002, June) SIP: Session Initiation Protocol. RFC 2543.

[11] H. Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," *ACM SIGMOBILE Mobile Computer Communications Review*, vol. 4, no. 3, pp. 47-57, July 2000.

[12] R. Moskowitz, P. Nikander, Ed. P. Jokela, and T. Henderson. (2008, April) Host Identity Protocol. RFC 5201.

[13] Kimberly Keeton, Bruce A. Mah, Srinivasan Seshan, Randy H. Katz, and Domenico Ferrari, "Providing Connection-Oriented Network Services to Mobile Hosts," in *MLCS Mobile & Location-Independent Computing Symposium on Mobile & Location-Independent Computing Symposium* , Berkeley, 1993, pp. 8-8.

[14] J. Mysore and V. Bharghavan, "A new multicasting-based architecture for internet host mobility," in *ACM/IEEE international conference on Mobile computing and networking*, New York, 1997, pp. 161-172.

[15] A. Helmy, M. Jaseemuddin, and G. Bhaskara, "Efficient micro-mobility using intra-domain multicast-based mechanisms," *ACM SIGCOMM Computer Communications Review*, vol. 32, no. 5, pp. 61-72, November 2002.

[16] A. Festag, H. Karl, and A. Wolisz, "Investigation of multicast-based mobility supprt in all-IP cellular networks," *Wiley Wireless Communications and Mobile Computing*, vol. 7, no. 3, pp. 319-339, March 2007.

[17] George Xylomenos and George C. Polyzos, "IP Multicast for Mobile Hosts," *IEEE COMMUNICATIONS MAGAZINE*, vol. 35, no. 1, pp. 54-58, January 1997.

[18] Christophe Diot, Brian Neil Levine, Bryan Lyles, Hassan Kassem, and Doug Balensiefen, "Deployment Issues for the IP Multicast Service and Architecture," *IEEE Network*, vol. 14, no. 1, pp. 78-88, January/February 2000.

[19] Z. Zhu, R. Wakikawa, and L. Zhang. (2011, July) A Survey of Mobility Support in the Internet. RFC 6301.

[20] Andrea Detti and Nicola Blefari-Melazzi, "Network layer solutions for a content-centric Internet," in *Trustworthy Internet*.: Springer, 2011, ch. 27, pp. 359-369.

[21] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana, "Internet Indirection Infrastructure," *IEEE/ACM Transactions on Networking*, vol. 12, no. 2, pp. 205-218, April 2004.

[22] Matthew Caesar et al., "ROFL: Routing on Flat Labels," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4, pp. 363-374, October 2006.

[23] Ion Stoica et al., "Chord: a scalable peer-to-peer lookup protocol for internet applications," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 17-32, February 2003.

[24] Prasanna Ganesan, Krishna Gummadi, and Hector Garcia-Molina, "Canon in G Major: Designing DHTs with Hierarchical Structure," in *ICDCS '04 Proceedings of the 24th International Conference on Distributed Computing Systems*, Tokyo, 2004, pp. 263-272.

[25] T. Koponen et al., "A data-oriented (and beyond) network architecture," in *SIGCOMM '07 Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, New York, 2007, pp. 181-192.

[26] CCNx. [Online]. https://www.ccnx.org/

[27] Van Jacobson et al., "Networking named content," in *CoNEXT '09 Proceedings of the 5th international conference on Emerging networking experiments and technologies*, Rome, 2009, pp. 1-12.

[28] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, no. 2, pp. 114-131, June 2003.

[29] PSIRP project. [Online]. http://www.psirp.org

[30] S. Deering and R. Hinden. (1998, December) Internet Protocol, Version 6 (IPv6) Specification. RFC 2460.

[31] Douglas E. Comer, "Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th Edition)," in *Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th Edition)*., 2000, ch. 33.7.

[32] S. Thomson and T. Narten. (1998, December) IPv6 Stateless Address Autoconfiguration. RFC 2462.

[33] Ed. R. Droms et al. (2003, July) Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315.

[34] Narten T., Nordmark E., and Simpson W. (1998, December) Neighbor Discovery for IP Version 6 (IPv6). RFC 2461.

[35] (2012, July) OMNeT++. [Online]. http://www.omnetpp.org/

[36] (2012, July) xMIPv6 Project. [Online]. http://www.kn.e-technik.tu-dortmund.de/de/forschung/ausstattung/xmipv6.html

[37] ITU-T, "Artificial conversational speech," Recommendation p.59 1993.

[38] Johnny Lai, Y. Ahmet Sekercioglu, Norbert Jordan, and Andreas Pitsillides, "Performance Evaluation of Mobile IPv6 Handover Extensions in an IEEE 802.11b Wireless Network Environment," in *ISCC '06 Proceedings of the 11th IEEE Symposium on Computers and Communications* , Cagliari, 2006, pp. 161-166.

[39] Xavier Pérez-Costa, Marc Torrent-Moreno, and Hannes Hartenstein, "A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 4, pp. 5-19, October 2003.