Télécom Paris (ENST)
Institut Eurecom

THÈSE

Pour Obtenir le Grade de Docteur
De l'Ecole Nationale Supérieure
Des Télécommunications

Spécialité: **Réseaux et Informatique**

Farouk BELGHOUL

Mécanismes de Gestion de Mobilité Généralisée dans un Système Hétérogène Fixe/Mobile

Date de Soutenance: 29/06/2005

Composition du Jury :

Prof. Jean-Jacques Pansiot	Rapporteur
Prof. Noemi Simoni	Rapporteur
Prof. Guy Pujolle	Examinateur
Doct. Yan Moret	Examinateur
Mr Massimo Lucchina	Examinateur
Prof. Christian Bonnet	Directeur de Thèse

Acknowledgment

First and foremost, I would like to thank my supervisor Prof Christian Bonnet for his encouragement and support over the past years. He gave me a lot of freedom with my research as well as the possibility to implement our work in Eurecom Platform and to present my results in several international conferences.

I wish to express my gratitude to Yan Moret who helps me so much with my research, simulation work, and publication reviewing.

I am grateful to the members of my doctoral committee for their time, support and useful comments.

My work with Christian Bonnet, Yan Moret and Eurecom Platform team gave me the chance to gain a valuable experience. I also want to thank all the staff in the Mobile Communications Department and Institut Eurecom for their warm reception. We have spent so much wonderful time together. I will never forget them.

I which to thanks all Eurecom PhD candidate especially in mobile communication department, Maxim, Mari, Navid, Souad, Younes and all the team for their help and support for last three years.

I have a special gratitude to my family. I want to thank my father and Mother, my sister Lynda, my brothers Tarek, Khaled, Djameleddine for their constant and unconditional love and support all the time.

This paragraph would of course be incomplete if I didn't mention Leslie who gave me her infinite support and love. I am grateful to her for enriching my life.

Abstract

Today, mobile users are facing the fact that many heterogeneous radio access technologies coexist, ranging from wireless LANs to cellular systems. No technology has emerged as common and universal solution. On the other hand, the Internet Protocol becomes the universal network layer over wireline networks. Moreover it can be used on the top of all wireless radio technologies, which makes the current trends today toward the design of All-IP wireless and wireline networks, where radio cells are under the control of IP access routers for signaling and data transmission. General mobility mechanisms are introduced in Internet Protocol to manage internet-network node movement, regardless of wireless technologies heterogeneity.

Mobile IP has long been considered as the facto standard in providing handover and mobility management in internet protocol. However, as the demand of wireless mobile devices capable of executing real times applications increases, it has necessitated to extend mobile IP with better handover techniques to minimize session disruption. That includes providing a new handover technique which cause reduced data loss, minimize additional end-to-end data transmission delays and improve end-to-end services.

In this dissertation we first examine, evaluate and analyze existing IP-based handover management approaches. We will identify the causes behind each handover performance and therefore device a set of guidelines for the development of new IP-based handover mechanisms.

We propose then, a set of mechanisms to handle soft handover in IPv6 protocol. This approach coexists with mobile IPv6, extends-it with mobile node multihoming management, bidirectional asynchronous IPv6-flows duplication and merging and, in certain case, improves the overall Quality of wireless connection. The performance of soft handover is evaluated through a home-made simulator and compared with the performance of basic Mobile IPv6 and fast handover bicasting.

Finally, in order to validate this approach, the dissertation describes the design and the implementation of a multi-interfaces mobile node prototype and a mobile IPv6 soft handover testbed. The results of experiences measurements on real time traffics are discussed in the last chapter.

Résumé

Le support de la mobilité dans les protocoles réseaux existants est devenu primordial, à cause du nombre croissant d'utilisateurs de terminaux mobiles désirant garder une connexion constante au réseau, tout en se déplaçant librement à travers des segments de réseaux d'accès sans fil hétérogènes.

Le protocole de routage dominant dans les architectures réseaux filaires est IP « Internet protocole ». Ce protocole est en passe de dominer aussi le mode des réseaux sans fils. Ainsi, il est naturel d'introduire des mécanismes de gestion de mobilité basés sur IP, dont un processus de handover (passage d'une point d'accès radio à une autre point) efficace et flexible afin de garantir aux utilisateurs une qualité de service minimale de transmission des donnés. En effet, un handover inefficace génère de la latence, de la gigue et des pertes de paquets. La transmission des données est affectée et dégrade la qualité de services de l'application utilisant les services du réseau.

Dans cette thèse, nous examinons et analysons d'abord la complexité et l'efficacité des principales techniques de handover et de gestion de mobilité basée sur IP. Les résultats de cette analyse seront ensuite exploités pour présenter finalement notre proposition de soft handover basé sur IPv6. Cette solution permettra l'extension de mobile IPv6 avec une gestion efficace, transparente et locale du multihoming. Bien sur la duplication des flux est bidirectionnel entre le réseau et le mobile et permet un changement de point d'accès au réseau sans perte de données.

Nous analysons ensuite les performances de notre approche à travers des résultats de simulations. Ces simulations sont effectuées dans un simulateur développé par notre équipe nommé Gemini2. Cette partie inclut également une comparaison des performances par rapport au fast handover bicasting et Mobile IPv6 basique.

Finalement, le dernier chapitre de la thèse inclut notre expérience de l'implémentation d'un prototype mobile multi interfaces et un testbed mobile IPv6 soft handover. Cette implémentation a comme but principal la validation de nos travaux. Ce banc de test nous permettra, en plus, d'analyser les performances du soft handover dans des conditions réelles et avec différents types d'applications et de flux multimédia.

Contents

List of Figures

List of Tables

Glossary

2G	Second Generation
3G	Third Generation
4G	Fourth Generation
AP	Access Point
AR	Access Router
BA	Binding Acknowledgement
BC	Binding cache
BU	Binding Update
CoA	Care of Address
CN	Correspondent Node
D&M	Duplication and Merging
DAD	Duplicate Address Detection
DCT	Duplication control Table
FBU	Fast Binding Update
GPRS	General Packet Radio Service
GSM	Global system for mobile communication
HA	Home Agent
HiperLan	High Performance Local Area Network
HoA	Home Address
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
IP	Internet Protocol
IPv4	Internet protocol version 4
IPv6	Interne Protocol version 6
L1	Layer 1
L2	Layer 2
L3	Layer 3
LCoA	Local Care of Address
MAC	Media Access Control Layer
Madv	Merging Advertisement
MCT	Merging Control Table
Mobile IP	Mobile Internet Protocol
MIPL	Mobile IP for Linux

MN	Mobile Node
MPEG	Moving Picture Experts Group
Msol	Merging Solicitation
PCoA	Primary Care of Address
RCoA	Regional Care of Address
RFC	Request For Comments
RtAdv	Router Advertisement
RTP	Real-Time Transport Protocol
Rtsol	Router solicitation
RTT	Round Trip Time
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network

CHAPTER 1

I. Introduction

The recent years have seen a rapid development of mobile communication systems. A variety of new wireless radio access technologies such as, UMTS, IEEE WLAN, HYPERLAN and Bluetooth are replacing and augmenting existing GSM radio technology. Therefore, these technologies are not compatible with each others, and each wireless technology provides a tradeoff between coverage range, data rates and costs. On this diversity basis, next mobile networks generation will offer services where users can move freely almost anywhere and communicate with any one, any time, using one or more available services. They support, of course, different radio access technologies and different type of mobility. Users can at any moment manage their connections to fit their application requirements and use the best available and most suitable wireless access technologies. To allow that, future mobile devices will be equipped with more than one network interface in parallel. These interfaces can be from homogenous access radio technologies or can be heterogonous. Using such devices, users can adapt their connection to the current environment and connect many interfaces simultaneously or switch between different technologies if beneficial.

The main goal of mobile communication system is to give the user the freedom of choosing its most suitable communication service at any moment. Mobile communication systems will certainly use IP protocol as universal and common network layer to facilitate the heterogeneous wireless access technologies interconnection and allow the convergence of wireline and wireless communication systems. That will push towards the design of an All-IP wireless and wireline networks, where heterogeneous access wireless networks and mobile devices are under the IP control for signaling and data transmission. In such environment, a true dynamic mobility scenario has to allow the change of mobile user's connection to the network several times during a single applications session. Moreover, in a heterogonous environment, any user is free to roam its current connection to the network between available access points several times in a session and regardless of their heterogeneity (of course the mobile device has to support desired wireless access technologies).

The grade of service continuity during "the change of mobile user's connection to the network" (referred to as handover in remains of this dissertation) is crucial to determine the global efficiency of communication

systems. With the deployment of an all-IP mobile communication system, the current increasing demand of IP based multimedia data traffic services compare to the basic voice traffic is encouraged. Regarding the IP based multimedia traffic quality of services requirements compared to voice traffic, new service and communication continuity parameters might be expressed in terms of no data loss, minimal, stable and uniform information transmission delays before and during the handover. This new communication system has to offer, at any moment the best available services to users and propose more sophisticated IP-based handover mechanisms to assure a certain quality of services for dominating multimedia IP traffic in addition to basic voice service continuity. In following, we give some mobile communication systems terminologies and definitions useful for the understanding of remains of this dissertation

1. Terminology

Today, many heterogeneous radio access technologies coexist, ranging from wireless **local area networks** (IEEE 802.11 [1][2], Hiperlan [3][4], Bluetooth [5][6]) to outdoor **cellular networks** (GSM [7][8], GPRS [9], WCDMA [10][11]). These radio technologies are typically not compatible with each others, which make it difficult to perform roaming from one radio network to another. These wireless networks were developed and were evolving independently (e.g., from 802.11/802.11g, from 2G to 3G), but they still have a set of common characteristics and concepts such Wireless cell or coverage area. **Wireless cell** or **coverage area** can be defined as the basic service portion of most of Wireless networks. Each one is under the control of an **Access Point** (AP). An access point is a dedicated node that provides wireless communication services within the coverage area of wireless cell. A set of access points distributed in the coverage area of the network allow the wireless device namely **Mobile Node** (MN) to keep connection to the fixed network through wireless connections. One of the main characteristic of wireless access technology is the **maximal range** between the AP and the MN, within this range the MN can receive data from the AP. the area covered by this range is called wireless cell. When the MN is in the center of the cell, the reception quality of wireless connection is optimal, as the MN move away from the cell center; the connection quality degrades progressively toward a complete disconnection outside of the coverage area. When the MN moves out of coverage area of an AP1 and enter the range of a new access point AP2. It disconnects from AP1 and establishes a connection with AP2 that is what we call **handover**.

Figure I-1 shows a MN performing handover in the border of two coverage areas. A handover is a process that allows the MN to roam from one access point to another while communicating. It transfers the management of MN connection from one access point to another. Both of degradation of wireless connection signal quality when the MN move out of coverage area, and MN disconnection when performing handover, can introduce data loss, additional end-to-end transmission delays and jitters, which perturb the communication.

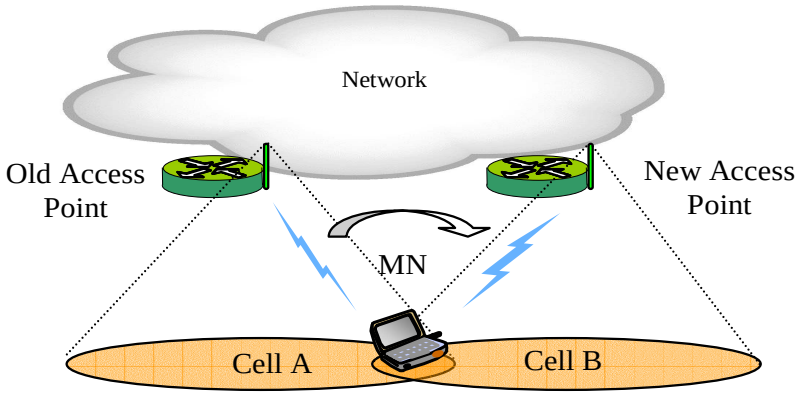


Figure I-1 MN Handover between two APs

2. Problem Overview

As stated earlier, next generation networks are expected to integrate many heterogeneous radio access technologies, ranging from indoor wireless LANs to cellular systems. The main reason is that no solution has emerged as universal solution. In the other hand, Internet Protocol (IP)[13][14][15][16][17] is becoming the universal network-layer protocol over all wireless systems, and it is used on the top of all these radio access technologies. That makes the current trend today toward the design of All-IP wireless and wireline networks [18][19], where radio cells are under the control of IP access routers for signaling and data transmission. Mobile IP [20][21] has long been considered as facto standard in providing IP mobility. However, as the demand of wireless mobile devices capable of executing real time applications increases, it has pushed for the development of better IP based handover techniques. The goal is providing a reduced data loss, end-to-end transmission delays and better Quality of services (QoS) support [22]. Several solutions have been designed to improve the QoS in the core of IP-based network, and many others to manage IP-based handover in order to re-establish the IP traffic flow quickly and minimize the service disruption delay that occurs during IP based handover.
In this dissertation, we propose a set of IP based mechanisms to extend mobile IPv6 with bidirectional IP-based soft handover; such solution allows the MN's session to progress without any interruption and perturbation when it moves from one radio cell to another regardless of their access technologies. To allow an integration of soft handover in mobile IPv6, we have to fix and resolve the following issues:

- The MN must be able to maintain data connection simultaneously with multiple APs at the same time.
- The network and the MN are able to manage the multiple MN connections to the network when using Mobile IPv6 (multihoming)

- The network must be able, somewhere, to intercept and duplicate IP flows sent by corresponding node to the MN through different ARs
- The MN duplicates IP-flows and route them through different access routers to the network
- The network and the MN correctly merge duplicated flows in a single copy, that can be correctly routed to transport and application layers.
- Finally, these mechanisms have to coexist with existing Mobile IPv6 mechanisms. Duplication and merging process should be completely transparent to upper and lower network layers and applications

In addition to the pure problem of soft handover management in IP protocol, which still remains unresolved as explained above. Proposed scheme can be a solution to the general problem of the management of end-to-end quality of service for data communication based on radio transmission. More generally, even when using QoS management mechanisms in the core of the network, there is still a need for improving wireless data communication between a mobile node and IPv6 core of the network, especially in borders of wireless cells. It is an object of present mechanisms to improve the quality of service of wireless data communications using the end-to-end path redundancy and diversity. Particularly for mobile nodes located in the border areas with poor radio coverage from both old and new access routers.

3. Outline of the Dissertation

The aim of All-IP networks is to allow ubiquitous IP-based access by IP-based MN, with special emphasis on the ability to use a wide variety of wireless and wireline technologies, to access the common information infrastructure. The development of such a mobile device with multiple physical or software-defined interfaces is expected to allow users to switch between different radio accesses technologies. With the extension of basic mobile IPv6 mechanisms using multihoming mechanisms support and soft handover approach, it is possible to eliminate packet loss and reduce jitters and end-to-end transmission delays, which provides a clear advantage to data traffic requiring high level of service. The remainder of this dissertation is organized as follows:

Chapter 2 provides an overview of IPv6 main features and mobility management problems in IP-based networks. We also present main existing intra-technology roaming mechanisms.

Chapter 3 contains a description and analytical analysis of main solutions to manage mobility in Internet protocol; we will focus our analysis in handover management mechanisms.

Chapter 4 describes our mobile IPv6 soft handover mechanisms. We describe the control plane with the introduction of D&M agent and multihoming management. We depict then, the data plane, which allows bidirectional interception, duplication and merging of IPv6 flows.

Chapter 5 analyzes the performance of the IPv6 soft handover in a home made simulator Gemini2. First, simulations evaluate the handover performance gains, and then compare its performance with mobile IPv6 and fast handover bicasting.

Chapter 6 contains first, a proposition of D&M agent deployment scheme and protocol. This hierarchical architecture is analyzed than, through simulations

Chapter 7 presents our experiences in the implementation of an IPv6-based test bed that support Mobile IPv6. We implement the Duplication &Merging agent in this test bed and additional mechanisms in access routers that allows a dynamic broadcasting of D&M information's. We implement also a Multi interfaces MN that support soft handover. This testbed allows us to evaluate the performance of soft handover in real network using real time applications.

Finally Chapter 8 outlines remarks and summaries of our work and contributions. We discuss the general experience learned about the design of an IPv6 based soft handover mechanisms and outline some directions for future research.

4. PhD Related publications and Applications

Journal Papers

- Farouk Belghoul, Yan Moret, Christian Bonnet « Mécanismes de Handover pour les réseaux IP sans files" " Technique et Sciences Informatiques, TSI " journal, Revue des sciences et technologies de l'information Vol. 24, No 1/2005.

- Farouk Belghoul, Yan Moret, Christian Bonnet "Prototype Implementation and evaluation study of Mobile IPv6 soft handover mechanisms " to be Submitted to WILEY Wireless Communication and Mobile Computing .June 2005

- Fethi fillali, Farouk Belghoul, Christian Bonnet & All "" An Open, Pluggable, and Flexible Software-Radio Platform for Heterogeneous Wireless Networks" to be submitted to ACM Mobile Networks and Applications (MONET) June 2005.

International Conferences Papers

- Farouk Belghoul Yan Moret, Christian Bonnet "A Multilevel Hierarchical topology of DM agents for MIPv6 Soft handover " World Wireless Congress SanFrancisco, USA 2004 PP 56-60

- Farouk Belghoul Yan Moret, Christian Bonnet " Performance comparison and analysis on MIPv6, fast MIPv6 bi-casting and Eurecom IPv6 soft handover over IEEE802.11b " 59 IEEE VTC, MILAN 2004 Vol.5 PP 2672- 2676

- Farouk Belghoul Yan Moret, Christian Bonnet " Performance analysis on IP- based soft handover across ALL-IP wireless networks" IWUC, PORTO, Portugal 2004

- Farouk Belghoul Yan Moret, Christian Bonnet " IP-based handover management over heterogeneous wireless networks" LCN 2003, 28th Annual IEEE Conference on Local Computer Networks, October 20-24, 2003, Bonn, Germany PP 772- 773

- Farouk Belghoul Yan Moret, Christian Bonnet "Eurecom IPv6 soft handover:" ICWN 2003, International Conference on Wireless Networks- June 23th - 26th, 2003 - Las Vegas, USA PP 169-174

Applications

- GEMINI2: a wireless and wireline simulator written in C++. It supports IEEE802.11b, Ethernet, IPv6, MobileIPv6, Fast Handover, Soft handover, multihoming, and multi-interfaces mobile.

- Mobile IPv6 Soft handover platform: a soft handover on 802.11b platform test, based on Linux 2.4.18 and MIPL 0.9.3, that support multihoming and multi interfaces mobiles.

CHAPTER 2

II. State of the Art

This chapter gives first a short overview of handover classification in existing mobile communication systems; with special emphasis on the new requirements of handover designs for All-IP wireless networks. In this context of All-IP mobile communication system, the main features and functionalities of the latest version of Internet Protocol (IPv6) are presented. We specially focus in useful mechanisms to understand the mobility management in Internet Protocol in the remainder of this dissertation. We depict the IP nodes autoconfiguration mechanisms, IP packets tunneling and the opening of the IPv6 protocol to the future development via the option headers. That leads directly to the fundamental mobility problem in Internet Protocol. The problem is clearly defined and the requirements for the design of mobility schemes are elaborated. Finally, mobile IP, the classical solution for mobility support in IP is proposed.

1. Handover in Mobile Communication Systems

Handover in existing mobile communication systems differs greatly, and many classifications of handover following different criteria have been done. In following, we summarize general handover types and their classification criteria

- Topology and location of access points

  Local Handover. In a local handover the mobile node roams between two access points that belongs to the same network, or the same domain.

  Global Handover. In a global handover the mobile node roams from an access point to a new one that not belongs to the same network or domain.
- Access points wireless technologies

  Horizontal handover. It is a handover between access points using the same wireless access technology. A typical example is handover between two access points using UMTS access technology.

Vertical handover. It is a handover between access points using heterogeneous wireless networks such as handover between WCDMA access point and IEEE 802.11 access point.

- Handover initiation

  Mobile-initiated handover. The mobile node, as well as the target access point takes the handover decision. Usually the mobile node triggers the handover when the quality of the current signal decreases under a given threshold.

  Network-initiated handover. In this approach, the Network is able to determine the appropriate new access point of the mobile node, and uses this information to initiate the mobile node handover.

- Number of simultaneous connections to access points

  Hard Handover. Called also break-before-make, in this handover family used in WLAN, WCDMA or TDMA [12], the MN can keep connection through only one access point. The mobile node disconnects from the old access point than initiates connection through the new one to perform a handover.

  Soft Handover. In the soft handover, the MN can communicate simultaneously with more than one access point, in our example, the old and the new access points. This handover can be seamless but it requires an overlapping region between the old and the new access point to. An additional benefit of soft handover is that the duplication of connection in overlapping area can improve the global quality of mobile connection of the mobile node to the fixed network. The connection is duplicated by sending and receiving the same data through two access points

In second generation mobile networks (GSM), the hard handover was designed for voice traffic. It is achieved via a change of the channel used by the mobile node. The system continually measures the level and the quality of the signal received from the neighbor cells. As soon as the current communication quality goes below a certain threshold, the network decides to change the mobile node radio channel. It chooses another one with a better quality of signal. This procedure was optimized for data voice traffic with strong traffic synchronization mechanisms which allow the reconstruction of lost traffics when performing the handover. Note also that the QoS requirements were not heavies because of the permissibility of human ear.

The massive success of 2G technologies is pushing mobile networks to grow extremely fast as ever-growing mobile traffic puts a lot of pressure on network capacity. In addition, the current strong drive towards new applications, such as wireless Internet access and video telephony, has generated a need for a universal standard at higher user bit-rates. This led the definition of third generation 3G digital cellular systems, standardized in Europe by ETSI (European Telecommunication standards Institute) as UMTS (Universal Mobile telecommunications Systems). Considering third generation networks, in addition to the traditional hard handover mechanism, the soft handover concept is introduced. In the CDMA network such as IS-95 [23], the mobile station can be connected to multiples base station simultaneously. A centralized selection and distribution unit (SDU) is responsible for data distribution in the downlink. It creates and distributes multiples streams of the same data over layer2 circuits to the direction of the mobile terminal through different base station. A strong synchronization mechanism is required, duplicated packets of data arriving from

different radio gateways to the MN, must arrive in the same time, to allow the Mobile to combine them in a single copy, which reduces the overall packet loss. On the other hand, compared with the conventional hard handover, soft handover has the advantages of smoother transmission and less ping-pong effects. As well as leading to continuity of the wireless services, it also brings macro diversity gain to the 3G system. For the purpose of next all-IP heterogeneous mobile communication networks, and the convergence wireless and wireline, the increasing demand of IP based multimedia data traffic services compare to the basic voice traffic is encouraged. Regarding the IP based multimedia traffic quality of services requirements compared to voice traffic, the introduction of new IP efficient handover mechanisms seem to be the most suitable solution to allow a session continuity even when the MN change its point of attachment to the network, regardless of their radio access technologies and with minimal QoS. In chapter III we will detail existing solutions to manage handover in internet protocol. But note that there is no already standard to extend the IP mobility management with soft handover mechanisms.

2. Internet Protocol Next Generation

The latest version of the Internet Protocol, namely Internet Protocol Version 6 or simply IPv6 [24][25], is a very promising network layer. It is the core of new communication possibilities and services in the future networks. The IPv6 version of the Internet network substantially differs from the known IPv4 version and provides additional features and new possibilities. The main need to imagine a new version of Internet Protocol appears with the fast growing of IP networks and the limitation of address space in IPv4 [26]. This section describes the other important innovations of IPv6 over IPv4. Because of the complexity of IPv6, our focus lies on its features which can be used in mobility management and therefore the understanding of the remainder of this dissertation.

2.1. Expanded Addressing Capability and Autoconfiguration Mechanisms

In order to solve the problem of the limited address space of IPv4 and in order to offer a deeper addressing hierarchy and simpler address configuration mechanisms, the Internet addressing capabilities have been increased from 32 bits in IPv4 to 128 bits in IPv6. This address space extension in IPv6 requires a new address format. The new preferred form is the hexadecimal notation *"X:X:X:X:X:X:X:X"*. *'X'* is a group of 4 hexadecimal numbers, each one represents a piece of 16 bits of the IPv6 address (e.g., "fe80:202:0000:0000:0000:7654:fedc:3210"). Since, it is assumed that an IPv6 address can contain many successive groups of zero, a special compressed representation were defined. The special notation "::" can be used once in the address, it indicates a multiples successive groups of zeros, (e.g., the above IPv6 address can be represented by "fe80:202::7654:fedc:3210" as described in Table 1). IPv6 address is the only way to identify an IPv6 node in the network, IPv6 routing mechanisms are based on this address to route correctly data to the destination node. IP address merges in a single key both identification and

location of each component of the Internet Protocol. Any IPv6 address can be classified into one of three categories: Unicast, anycast and multicast address.
The unicast address uniquely identifies an interface of an IPv6 node; any IPv6 packet sent to a unicast address is delivered to the corresponding interface. This kind of address is split in his turn into two forms, link-local address and site-local address.

- The link-local address is the address that is exclusively used within the boundaries of a link and is defined on the basis of the Interface IDentifier (IID) [27] assigned to the interface. The IID must be unique on the link and is derived from the hardware interface card address, the form of a Link-local address is "FE80::X:X:X:X".
- The Site-local address is designed for networks that are not reachable from the outside, they have only local routability scope, and any IPv6 packet with site-local address will not be routed outside the corresponding networks. The format of site-local address is "FEA0::X:X:X:X".

The multicast address identifies a group of IPv6 interfaces. Unlike repeated unicast transmission of packets to multiple nodes, all members of the multicast group process a packet sent to a multicast address.
The anycast address is a new kind of address introduced in IPv6. It is a mixture between unicast and multicast addressing principles, this address identify a group of interfaces; a packet sent to an anycast address will be delivered to the nearest interface of the anycast group. The Table1 illustrates valid examples of IPv6 address in long and compressed notations.

IPv6 address format	Long notation example	Compressed notation
Unicast link-local	FE80:0:0:0:12e0:18ff:fea8:abde	FE80::12e0:18ff:fea8:abde
Unicast Site-local	FEA0:0:0:0:12e0:18ff:fea8:abde	FEA0::12e0:18ff:fea8:abde
Multicast address	FF02:0:0:0:0:0:0:1	FF02::1
Loop-back address	0:0:0:0:0:0:0:1	::1
Unspecified address	0:0:0:0:0:0:0:0	::0

Table 1 Examples of IPv6 address notations

Neighbor Discovery protocol (ND) [28] is the process used in IPv6 to allow nodes discovery on the same link. This protocol allows each node to discover its neighbor's link-layer addresses, find routers, learn about further link properties and auto-configure its own valid IPv6 address. The procedures involved in address autoconfiguration are as follows:

- Parameter Discovery, used to discover particular parameters and/or options concerning the link, including prefixes.
- Address Configuration, used for automatic configuration of an interface's address.
- Duplicate Address Detection: an algorithm used to check that an address to be assigned is not already in use.

There are five different ICMPv6 [29][30] messages for this protocol: Router Solicitation, Router Advertisement (RtAdv), Neighbor Solicitation, Neighbor Advertisement, and Redirect. The most important message for the remained of the dissertation is the router advertisement. Each IPv6 node can advertise a Router Advertisement Message within its different interfaces. This message advertises neighbors about the node presence in the network and its Internet parameters. The format of an RtAdv message is depicted in Figure II-1.

<table>
<tr><td>Type</td><td colspan="3">Code</td><td>Checksum</td></tr>
<tr><td>Hop limit</td><td>M</td><td>O</td><td>Reserved</td><td>Router Lifetime</td></tr>
<tr><td colspan="5">Reachable Time</td></tr>
<tr><td colspan="5">Retransmit Time</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

Figure II-1 Router Advertisement Packet Format

The hop limit field specifies the max hop limit of the router advertisement message, the M and O flags are used for the stateful address autoconfiguration mechanisms, Router lifetime indicates the life time of the message in seconds, the reachable time is assumed to be the time, in seconds, that the router is considered is reachable after getting the reach ability confirmation, the retransmission time define the message advertisement frequency. The options field is used by router advertisement daemon to advertise optional message. The RtAdv message can be generated periodically by the router within a retransmit time, or can be an answer to an RtSol message. In fact when an IPv6 node enables a link with a router, it may wait for router advertisement message or can generate RtSol message, which requests the router to generate RtAdv message immediately rather than waiting a total Retransmit Time delay.

The attachment of a mobile node to an IPv6 network is greatly facilitated by a set of mechanisms named address auto-configuration mechanisms. They allow every mobile node, or any communicating device, to configure its own IPv6 address in its new sub network. These mechanisms are based on combination of the unique interface Identifier and a set of information received from the access point serving as physical attachment link, through an RtAdv message. IPv6 defines both a stateful and stateless address autoconfiguration mechanisms. Stateless autoconfiguration [31] takes place automatically as soon as the mobile node interface is enabled. This one starts the autoconfiguration process by registering in the multicast group "FF02::1" which identifies all of the nodes in the same link so that it can receive messages originating from the routers using this destination address. The station then sends a RtSol message with destination address field is set to the all-routers multicast address "FF02::2" in this message. The AP responds with a RtAdv, one or more AP prefix options can be specified in this message. At this moment the mobile node can start stateless configuration

protocol to build its valid IPv6 address by concatenating the address supplied to it by the prefix option with its unique IID (Figure II-2). This only applies if the prefix is not too long, and otherwise will be ignored. After a mobile node has obtained a unicast address using stateless address autoconfiguration, it must check that it is unique before assigning it to the interface. To do so, the mobile node applies the Duplicate Address Detection (DAD) protocol. It sends a Neighbor Solicitation message in which the source address field is set to the unspecified address and the destination address field is set to the solicited-node multicast address. If the same unicast address has already been assigned to another node, the latter will respond with a Neighbor Advertisement. If the mobile node receives this message, it disables the use of the address that has just been obtained.

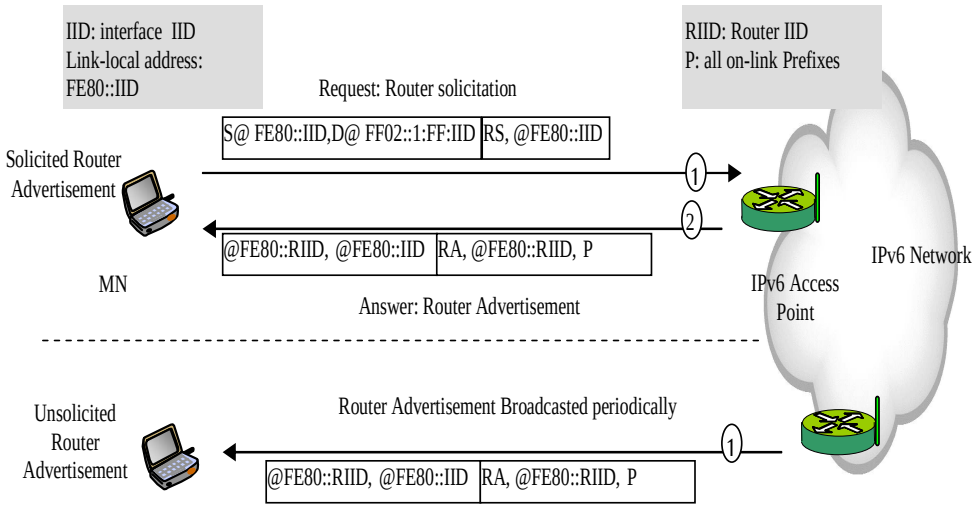


Figure II-2 Address autoconfiguration mechanisms

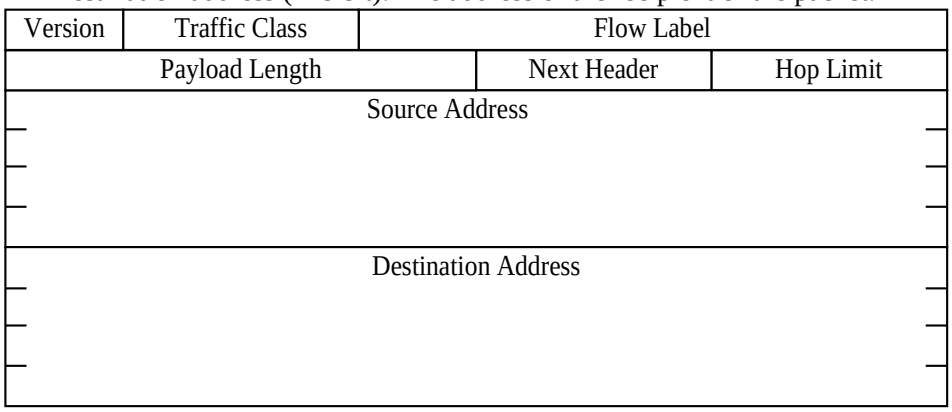
In the stateful autoconfiguration model, the mobile node obtains interface addresses and/or configuration information and parameters from a server. Servers maintain a database that keeps track of which addresses have been assigned to which node. The stateful autoconfiguration protocol allows IPv6 nodes to obtain addresses, other configuration information or both from a Dynamic Host Configuration Protocol (DHCP) server [32].

2.2. Simplification of the Header Format

In order to simplify and reduce the cost of Internet protocol packet routing and processing, the IPv4 header format have been changed. The new IPv6 header [25] has a fixed total length of 40 bytes as shown in figure II-3. In this figure we compare an IPv6 packet header to an IPv4 header, which includes 12 fields in its 20 byte of length. Some fields of the IPv4 header have been removed or become optional. This way, packets can be handled faster and easier. The

IPv6 header consists of two parts, the basic IPv6 header (as illustrated in Figure II-3) and optional IPv6 extension headers. The usage of the fields conveyed by the IPv6 header is summarized in following.

- Version (4 bit): Indicates the protocol version, and will thus contain the number six to denote IPv6 protocol.
- Traffic class (8 bit): This field is used by the sending source and routers to identify the packets belonging to the same traffic class and thus distinguish between packets with different priorities and allow Quality of Service management in routing mechanisms.
- Flow label (20 bit): Label for a data flow.
- Payload length (16 bit): Indicates the total size of the packet data field.
- Next header (8 bit): Identifies the type of header immediately following the IPv6 header. Which can be an option header as explained in next paragraph
- Hop limit (8 bit): Decremented by one by each node that forwards the packet. When the hop limit field reaches zero, the packet is discarded.
- Source address (128 bit): The address of the IP node originator of the packet.
- Destination address (128 bit): The address of the recipient of the packet.



(a) (IPv6)

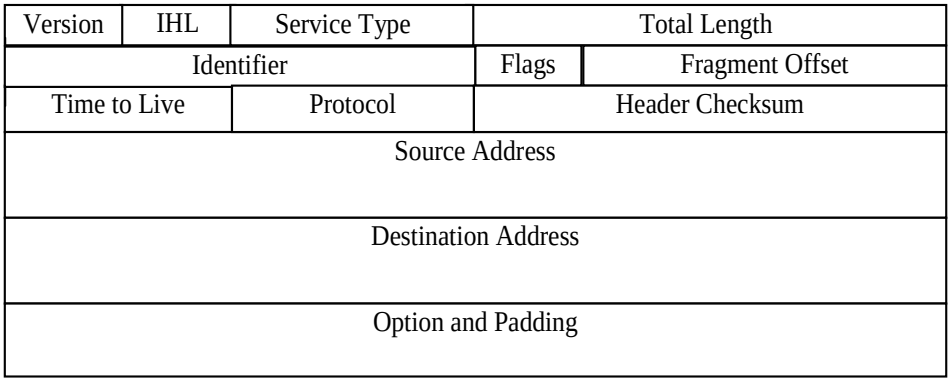


Figure II-3 IPv6 (a) Compared to IPv4 Packet headers

Note that additional header fields besides the source and destination address in IPv6 were reduced to only 6 scattered over 40 bytes compared to the IPv4 header, which carries 10 fields in 20 bytes. In particular, the Header Length (the length of the IPv6 header is fixed to 320 bytes), the Identification, the D- and M-flags, the Fragment Offset and the Header Checksum field from IPv4 header were dropped or made optional in IPv6 extension headers. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the header itself is only twice the size.

2.3. Improved Support for Extensions and Options

In IPv4, options fields were integrated into the main IPv4 header. Within IPv6, they are handled as Extension headers. Extension headers are optional and only inserted after the IPv6 header. As a direct consequence, forwarding IPv6 packets becomes much more efficient. New options that will be defined in the future can be integrated easily. The basic format of an extension option header is depicted in the following figure.

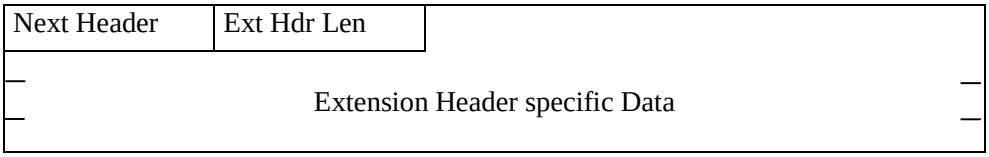


Figure II-4 IPv6 Extension Header Format

An IPv6 packet can have more than one type of extension header; each next header type is determined by the Next Header field of the previous packet header or extension header. These packets headers will be processed only in the destination node, and in the order of their occurrence, except the hop-by-hop extension header. All routers in the packet delivery path can process the hop-by-hop header, so it must be in the first position. The figure shows how option headers can be used:

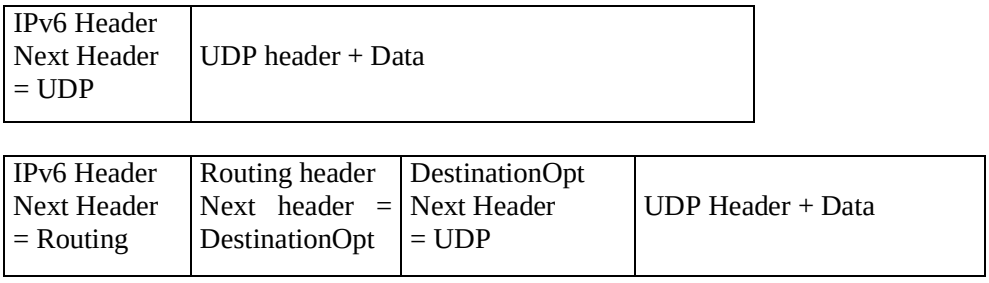


Figure II-5 Example of the use of IPv6 extension headers

Any full IPv6 implementation has to support the following packet header extensions:

- **Hop-by-Hop**: this header is processed by every passed IPv6 router, it holds optional information relevant for these routers on the packet way to the destination. The information that carries the Hop-by-Hop option or destination option is structured on one or more TLV (Type-Length-Value).

Option Type	Opt Length	Option Data

Note that one or more TLV can be inserted in each option header.

- **Destination Option**: This option header is quit similar to the hop-by-hop option header; the difference is that the destination option conveys special option that requires processing only in the destination node.
- **Routing Header**: This option holds information that specifies a set of routers that the IPv6 packet has to visit along the path to the destination node. This option corresponds to the source routing in IPv4. The routing header has the following format:

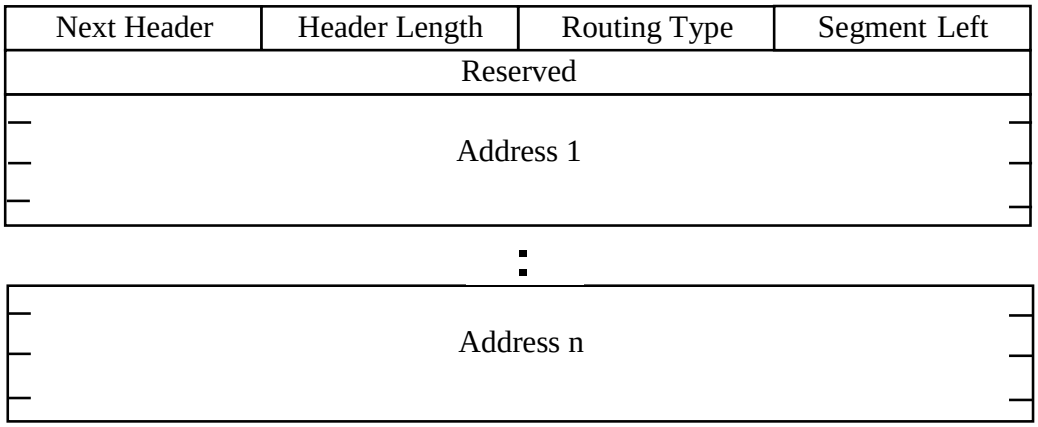


Figure II-6 Format of an IPv6 Routing Header

The “segments left” field specifies the number of explicitly defined router that the packet has to visit.
Figure II-7 is a practical example of the forwarding of an IPv6 packet with a routing header .the followed IPv6 packet should be routed from mode @ to @’, over the intermediate routers @1 and @2. When processed the node swaps the destination address and segment left address and decrements the segment left.

- **Fragment option header**: When the global IPv6 packet size is larger than the Maximum Defined Transfer Unit (MTU) of a connection, the fragment

header is used for the fragmentation of the packet to smaller fragments and then to reassemble these fragments

- **Authentication**: this header is used to ensure the integrity and the authentication for the IPv6 packets during a session between sender and receiver [33].
- **Encapsulation:** an encapsulation header guarantees confidentiality (between source and destination) for the reminder of the packet.
-

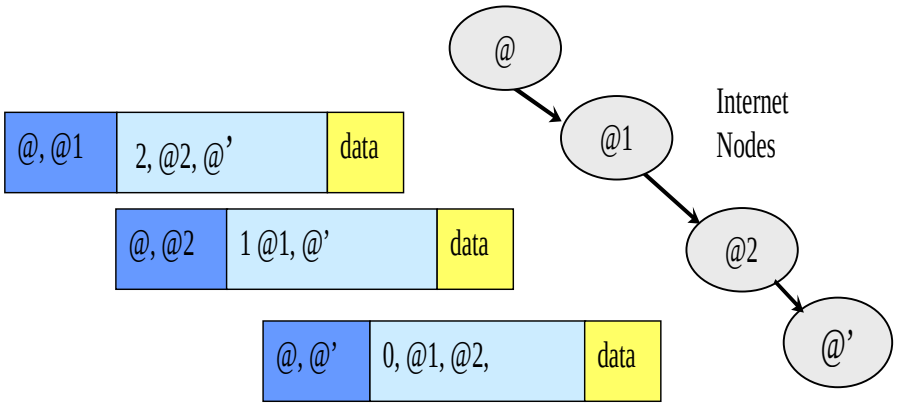


Figure II-7 Source Routing in IPv6.

For the purpose of our dissertation, a special option for destination header has been defined in our IPv6 stack, named Duplication Information Option. This header will be detailed in the third chapter; it can be processed only by received node, and will be exploited in our proposed mechanisms to mange packets duplication and merging in MobileIPv6 soft handover.

2.4. IPv6 in IPv6 Packet Encapsulation ”IPv6 Tunnels”

IPv6 tunnels are an IPv6 concept that will be used frequently in the rest of this dissertation. The IPv6 tunneling [34] is a technique for establishing a "virtual link" between two IP nodes for transmitting data packets as payloads of other IPv6 packets, using a new IPv6 header, source and destination address, as described in Figure II-8 . In this figure all IPv6 packets sent by node @1 to node @2 are intercepted by router S and tunneled to router R. This one decapsulates received packets and route them to the final destination @2. This IPv6 "virtual link", named an IPv6 tunnel, appears as a point-to-point IPv6 link by which packet is encapsulated and carried as payload within another IPv6 packet. The tunnel is unidirectional and the two IPv6 nodes are identified by their IPv6

unicast addresses. The tunnel sender-node encapsulates IPv6 packets forwarded or intercepted from other nodes or just itself and forwards the resulting new packets through the tunnel. The receiver-node decapsulates tunneled packets at reception; it applies, then, the basic IPv6 routing process to the resulting initial packets.

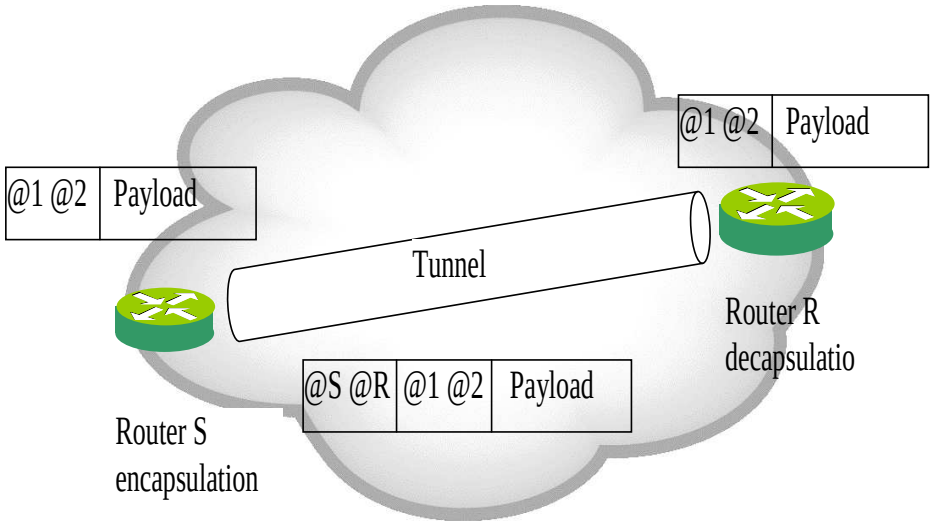


Figure II-8 example of IPv6 tunnel

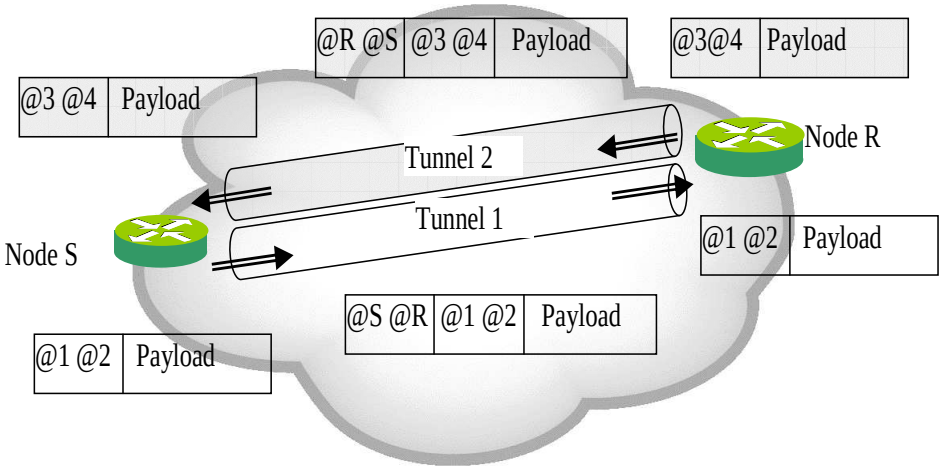


Figure II-9 Bi-directional IPv6 tunnel

In our soft handover approach, we will use a bi-directional IPv6 tunneling to carry data between the mobile and the network. Such as concept, is achieved by merging two basic unidirectional tunnels. We need to configure two tunnels; each in opposite direction to the other, the sender node of first tunnel is the receiver node of the second tunnel as indicate the figure II-9.
In the encapsulation process, a new IPv6 header is added to the original packet, the source field of the added IPv6 header is filled with an IPv6 address of the tunnel sender node. The destination field is filled with an IPv6 address of the tunnel receiver node. The resulting packets from encapsulation are than sent automatically to the receiver node. The encapsulated packets sent through the tunnel are then routed by intermediate routers in the tunnel way, according to the basic IPv6 routing mechanisms. The following figure depicts the format of an encapsulated packet.

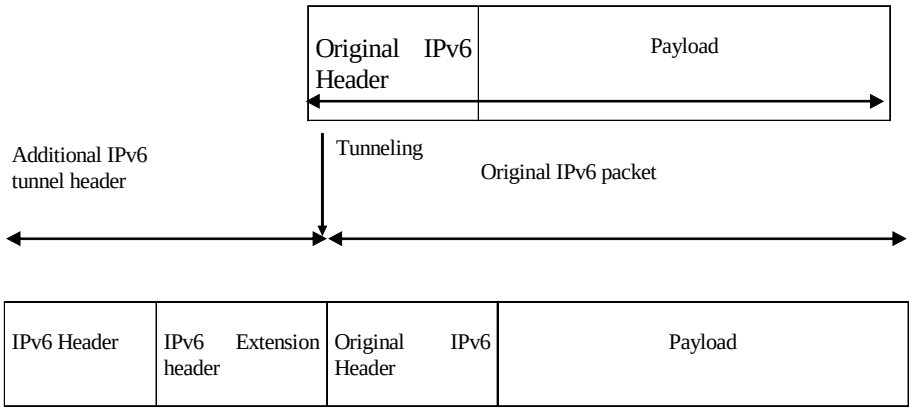


Figure II-10 Packet encapsulation

3. Internet Protocol and Mobility Requirements

As detailed in previous paragraph, Internet Protocol (v4, v6) has traditionally been designed for fixed networks. Each correspondent node is assumed to get connection to the network through the same link in a fixed subnetwork. A fixed IP address identifies the link of correspondent node in the network and allows IP packet to be routed correctly to the destination node. The IP address, considered as a base of an Internet networks, merges in a single key both identification and location of each components of the Internet Protocol.
The mobility management problem appears when a fixed node in the IP network becomes mobile while communicating with another node, and moves from its old location to a new sub network, by performing a handover from one access point to another one. The direct consequence is that its old IP address becomes topologically incorrect. Moreover any current correspondent node, without additional IP mobility information, will continue to use this erroneous IP address to identify the mobile node, and all packets sent by the correspondent node will

use this obsolete address as destination address. Intermediate routers in the core of the network will, logically, route sent packets to the old location of the mobile using the IP normal routing mechanisms. As direct consequence, all packets sent after the mobile node movement will be simply lost, as illustrates the scenario in Figure II-11.

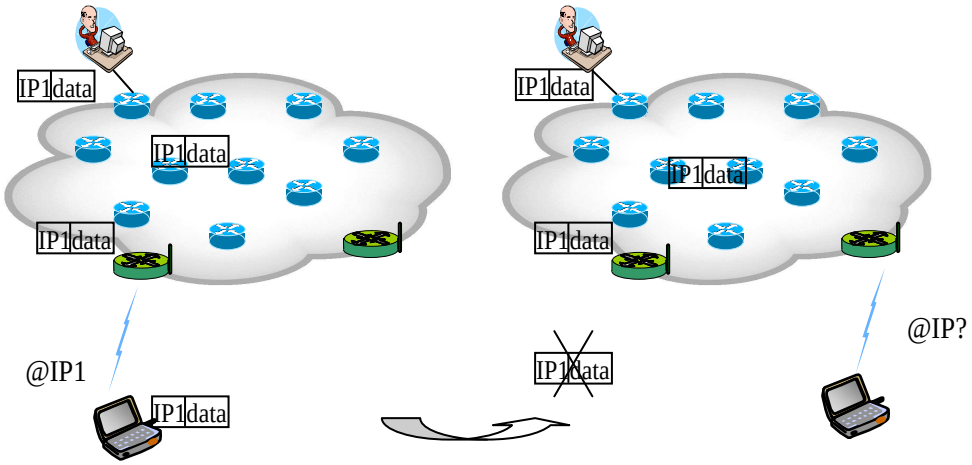


Figure II-11 IP packets loss as consequence of Mobile movement

Therefore, the first natural solution that can be proposed to resolve this problem is to assign automatically a new topologically correct IP address to the mobile node after each physical handover. This address will correctly identify the mobile at its new location in the network, so it can be reachable at this address. Unfortunately this solution is not sufficient, to understand the reason, we take a look to an application which generates data over an IP- based network; For example, if an application establishes a TCP or UDP session between a correspondent node and mobile node through Internet Protocol, it takes the IP addresses of correspondent and the mobile as node-id for application session. If the mobile nod moves during this session, it changes its connection to the network from an old access point to a new one that can be not in the same subnetwork. If we apply the early solution, the mobile node will get a new IP addresses automatically to identify its new location, however the session can not be continued, the mobile–id in application session does not longer match the new subnetwork of the Mobile node. All packets sent from correspondent node to the mobile node during this session after mobile movement will be simply lost. The use of IP address as key to identify the mobile and its location in Internet network is the fundamental mobility problem in Internet Protocol, we need solution that guarantee that any mobile node can be able to receive its ongoing communication in any place and, the most important, maintain its application session continuity after a physical handover.

Any IP based mobility management scheme shall support the mobile node initial identification and registration, physical handover detection, allow new IP

address configuration, introduce an address registration mechanisms to keep trace of mobile location from the IP view (introduce a dynamic address binding), and extend IP routing mechanisms to forward mobile destined IP packets to its real location at any moment.

- The initial registration and identification is a process by which a network becomes aware of the existence of a special IP node with mobility capability and its associated user. When a Mobile node becomes active (i.e., is turned on) in a network, it shall be registered with the network. This process comprises sending an identity registration request from the Mobile Node to the network, and performing an AAA (i.e., authentication, authorization, and accounting) process by the network. This registration process should occur when the user turn on its mobile node in the network or when it performs handover to a new administrative domain (there is new entity to mange the mobility in the new network).

- A physical handover detection mechanism in network layer is a process by which the IP layer of the mobile node becomes aware of the occurrence of physical handover. If there is no interaction between the IP layer and the link layer of the mobile node, it is necessary to introduce IP based mechanisms allowing the mobile to check, regularly, the IP sub-net address of its access point, and detect any elements that can indicate a physical handover and, if possible, the type of the handover.

- After detecting a handover, the mobile node needs to process an IP address Configuration mechanism. This is the process by which the mobile updates its IP address as a consequence of handover either within the same administrative domain or in different administrative domains. As an Mobile node moves between two different sub-networks or networks, it needs to acquire a new IP address, possibly new default gateway, subnet mask, etc. as well, and to reconfigure itself accordingly as described in previous paragraph.

- Dynamic address registration and binding is a process for allowing a mobile to maintain a constant identifier (e.g., a constant URL) for application in upper layer, regardless of its point of attachment to the network (e.g., its IP address). In such as process, after initial identification of the mobile node in the mobility administration entity of the network, as consequence of a handover, the mobile have to register its new IP address within the entity. The results are that the mobile node can maintain its initial identifier as universal identifier regardless of its point of attachment. Needless to say that such as process require an additional special singling mechanisms

- Mobile node binding address management and packets redirect is a process by which the network stores and updates the mobile location

database and supports location/redirect services if IP packets to the mobile node. This service is essential for any open session during and after a mobile handover. The requirements of location management are accuracy, being up to date, and simplicity of database and confidentiality of the location information. So we need to introduce a new entity in the network that can manage mobile nodes mobility location and packets redirection

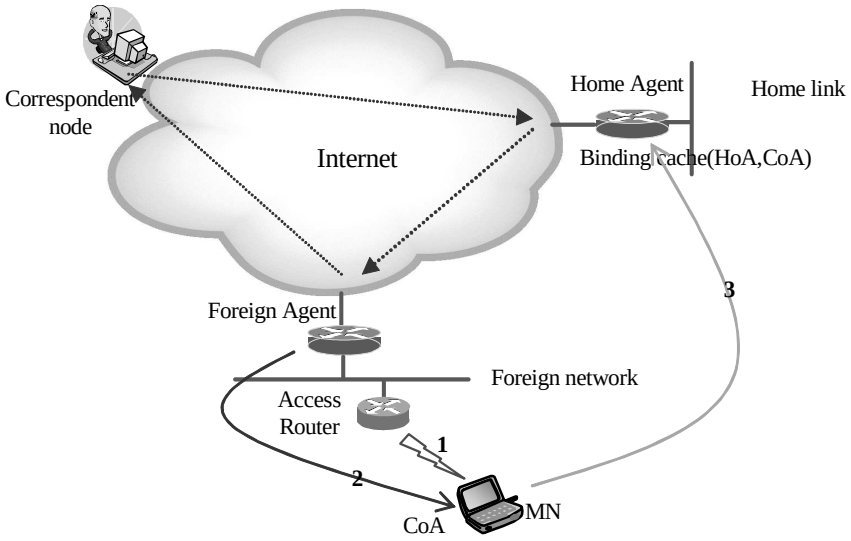
.

3.1. Mobile IP

Mobile IPv4 [20][21] or simply mobile IP or MIP is the oldest and the simplest way to introduce mobility management in the Internet Protocol. Its simplicity and scalability gives it a growing success. Several Internet drafts and publications have proposed various improvements for Mobile IP [36][37]. The basic principle of this approach is the use of a couple of addresses to identify the mobile node and manage its movements. Mobile IP and its successor mobile IPv6 define the following basic entities that will be used across the dissertation to refer to its features. The Figure II-12 illustrates the main features.

- Mobile Node: A mobile node (MN) is an Internet node or a host that can change its point of attachment to the Internet from one network to another while maintaining any ongoing communications.
- Home Address (HoA): A mobile node home address is an IPv6 address that has been assigned to the mobile node permanently. This home address does not change when the mobile node moves from one network to another. This address will not change usually. A mobile nodes Home address will only change under certain circumstances. Any application uses this address to identify the MN regardless of its location.
- Home Link: In the core of the Internet network, a home link subnetwork addresses space is used as base-network for mobile nodes. The IP prefix of the home link allows the definition of the mobile nodes home address
- Home Agent: a home agent (HA) is a router with at least one network interface on the mobile nodes home link. It is responsible of keeping MN addresses binding and packets redirection, when the MN is away from its home network.
- Foreign Link: a foreign link is any network to which a mobile node is connected to, away from its home network.
- Access router: an access router (AR) is the last router between the network and the mobile node, i.e. the mobile node has link layer connectivity to the core of the network through the access router.
- Care-of Address: a care-of address (CoA) of a mobile node basically refers to the second IPv6 address of the mobile node. The care-of address associated with a mobile node is the IPv6 address, which the mobile node has, when it is visiting a foreign link. In mobile IPv6, the care-of-address is always a collocated one, which is an IPv6 address temporarily assigned to an interface of the mobile node itself. Only one mobile node can use a particular care-of address at a time.

- Binding Update: It is a signaling message issued by the MN. It contains the new CoA and information in a MN's registration request
- Binding Cache: The binding cache is a table maintained by each home agent and correspondent node (only in Mobile IPv6) that contains the current bindings for mobile nodes. Each binding cache entry contains the main following information:
    - The home address for the mobile node
    - The care of address for the mobile node
    - The lifetime of the binding cache entry
- The binding update list is maintained by a mobile node to record the most recent binding updates sent for the home agent and correspondent nodes (only in Mobile IPv6). A binding update list entry contains a set information such :
    - The address of the node to which the binding update was sent
    - The home address for the binding update
    - The care of address sent in the last binding update and the remaining lifetime of the binding entry.



1. MN Connection and foreign agent discovery

2. Foreign Agent attributes a CoA to the MN

3. MN registers its CoA within its HA.

Figure II-12 Mobile IP network architecture

When a mobile node becomes active (i.e., is turned on) in a network, it gets a home address from the home link. All correspondent nodes will use this address as mobile identifier in network layer. Each time the MN connects itself to a foreign network, it obtains a new temporary IP address, the Care-of-Address, which is valid IP address in the new sub-network. This address is given by the Foreign Agents (FA), which is a special router that manages the mobile node connected to the foreign link. The MN must inform, than, it's Home Agent (HA) of this new address by the registration process, the HA can create, than, a binding between the MN home address and its new CoA. The HA stores all MNs bindings in special table termed Binding Cache (BC). It is used to locate the mobile at each moment. When a correspondent send packets to the MN it uses its home address, located in the HA sub network, so this one will be able to intercept and encapsulate MN destination packets towards the suitable FA or access router, in an IPv4 tunnel, as illustrated in Figure II-12.

4. Conclusion

In this chapter, general classification of existing handover approaches in mobile communication systems was presented. Considering the trend towards All-IP mobile systems and the convergence wireless-wireline networks, a new IP based handover approach needs to be designed. As same as the raisons that push to the design of soft handover in WCDMA, the new IP-based approach has to allow a better handover management regardless of the heterogeneity of wireless technology to fit the QoS requirement of future-dominating IP multimedia traffic. Thus, the main features and functionalities of the latest version of Internet Protocol (IPv6) were presented, with special emphasis in mobility management related features. Our focus lied in autoconfiguration mechanisms, data tunneling and the opening of the IPv6 protocol to the future development.
We illustrated that Interne Protocol was developed for fixed communication systems. Then, the first step toward All-IP mobile communication systems, which is IP extension to support efficiency mobility management were discussed. That led finally to the presentation of mobile IP, the classical solution for mobility support in Internet Protocol.

CHAPTER 3

III. Analytical Study of IP based Handover Management Protocols

1. Introduction

As seen in Chapter 1, Internet Protocol (IPv4 and IPv6) is considered as the universal routing solution in wireline and wireless networks, it can be used on the top of all radio access technologies, That make the introduction of mobility management mechanisms on IP the perfect solution to keep application sessions and manage efficiency and transparently mobile node movement through different access points to the network, regardless of their radio access technologies. In The Internet-based core network, such as radio access points are under the control of special IP routers for signaling and data transmission, named IP access routers. Each access router manages the application access to one or more radio cells. One of the most important metrics in IP based mobility protocol is the handover management. Compared to the wireless handover described in II.1, an IP handover is the global process that shifts the management of mobile node IP connection to the network, from an IP old access router to a new one. Such process introduces MN disconnection, the delay D of global mobile node IP disconnection, as shows Figure III-1, is the delay needed by the mobile to perform the wireless handover (Δ) and the IP additional delay (τ).τ is the necessary latency to detect the handover in IP layer, obtain a new IP address and finally register its new address within the network. This disconnection delay can introduce packet loss, retransmission, additional end-to-end transmission delays and jitters for the current communication session.

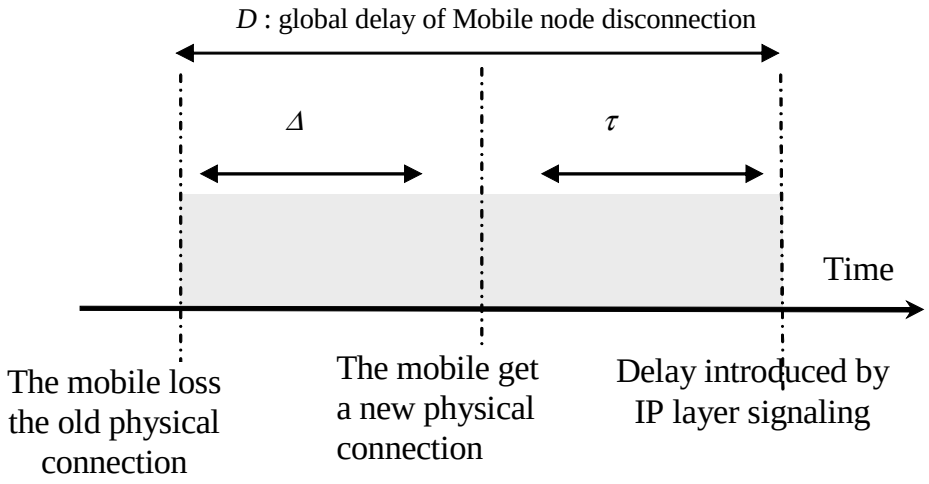


Figure III-1 IP handover delay

In this chapter, we will depict the main solutions to manage mobility in Internet protocol; we will focus our analysis in handover management mechanisms. Many propositions were done to improve the poor performances of basic mobile IP handover. Hierarchical mobile IP, fast handover and fast handover bicasting are part of the same family of solutions. It aims to reduce the mobile node IP disconnection (τ) during the handover in order to minimize the number of packet loss and thus, reduce session perturbations. On the other hand, we have the smooth handover which is part of the second family. The goal of this solution is to minimize the overall packet loss during a handover, without reducing handover delay. The network buffers all packets destined to the mobile node. After a handover, lost packets are simply retransmitted to the mobile node at its new location.

The goal of this theoretical analysis is to show the consequences and he effects of the different IP handover techniques on an open transmission session between a correspondent node located in the core of the network and the mobile node. This one has at least one radio interface, can move and change its point of attachment to the network. The correspondent node is connected to the network through a wireline interface. The scenario used in this analysis consists of an application in the correspondent that generates a continued and unidirectional UDP [35] flow to the mobile. The effects of handovers generated by mobile movements are analyzed through end-to-end UDP packets transmission delay, packet loss ratio and jitters as direct consequence of the handover. We define jitters as the variation in end-end transmission delays of two successive UDP packets. In order to simplify our handover analysis, we suppose that an IP access router controls only one radio cell. We suppose also, that the radio access point is the same node as the IP access router and there is no congestion in access routers.

2. Mobile IP

In following, the basic mobile IP handover process as described in previous chapter is analyzed. Figure III.2 shows us packets routing, and events happening during this basic mobile IP handover. We notice that to simplify the analysis we consider that foreign agents are located in the two access routers A (old AR) and B (new AR). The time space represented by horizontal axis, where we can find the temporal state evolution of MN, access routers A and B, and the CN. The vertical axis represents IP packets routing. As mentioned before in analysis scenarios, the CN sends packets to the MN home address; they are intercepted by HA, which tunnels them to the corresponding AR (FA) using the binding cache information. Finally the designed AR decapsulates and delivers these packets to the MN.

In mobile IPv6, each time the MN performs a handover, the global IP handover disconnection delay is,

$$D_{MIP4} = \Delta + \Phi_{MIP4} + \Omega_{MIP4} \qquad [1]$$

Δ , as defined in Figure III-1, is the delay of physical handover or MN wireless roaming between old and new access routers A and B. It depends on the used radio access technology. Φ_{MIP4} is the delay needed by the mobile to detect the physical handover and to obtain the new CoA from the FA. Finally, Ω_{MIP4} is the delay taken by the MN to register its new CoA in the HA. It's almost the delay of Round trip turn (RTT) between the MN and the HA. We notice that the value τ in Figure III-1, is the sum of Φ_{MIP4} and Ω_{MIP4}.
During the period of time D_{MIP4}, all packets that CN send the MN will be simply lost. Thus from equation [1], we conclude that the number of lost packets because the handover is,

$$N_{MIP4} = Th.(\Delta + \Phi_{MIP4} + \Omega_{MIP4}) \qquad [2]$$

With, *Th* is thought to be the packets emission throughput from CN toward the MN. Finally, for the packets end-to-end transmission delay, after a handover, the CN sends packets first to the home link; the HA intercepts and tunnels them to the foreign link of the MN, The results is an indirect and non optimal routing of the packets named triangular routing [67], as described in Figure II-12. The transmission delay is characterized by the formula,

$$T_{MIP\ 4} = T_{CN,HA} + T_{HA.nAR} + T_{radio} \qquad [3]$$

With, $T_{x,y}$ is packet routing delay form IP node *x* to node *y*, and T_{radio} is on air radio transmission delay of packet between the AR and the MN. The jitters introduced by the handover is,

$$J_{MIP4} = \left| T_{CN,oAR} - T_{CN,nAR} \right| + J_{radio} \qquad [4]$$

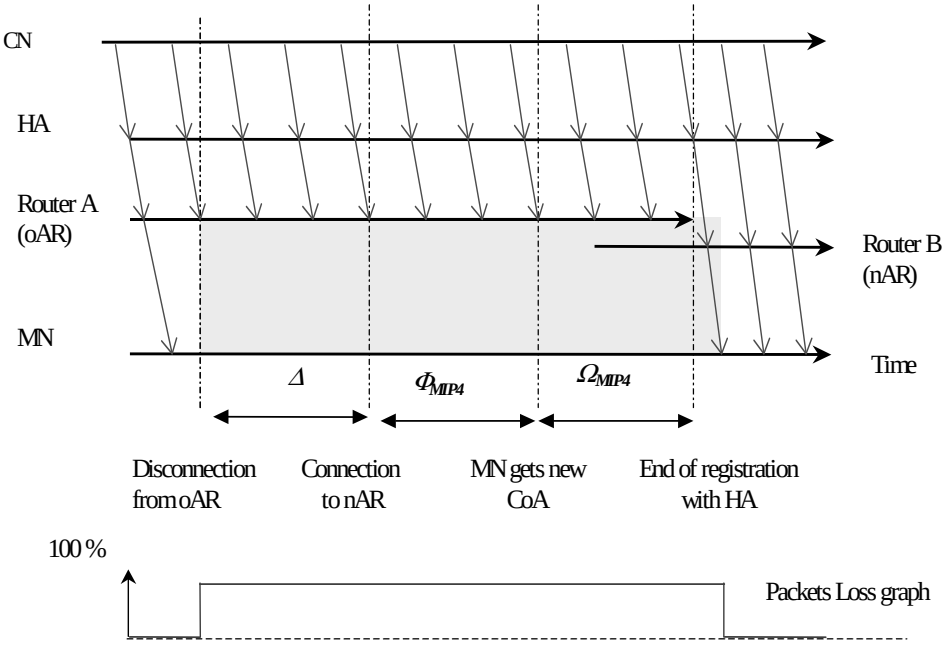


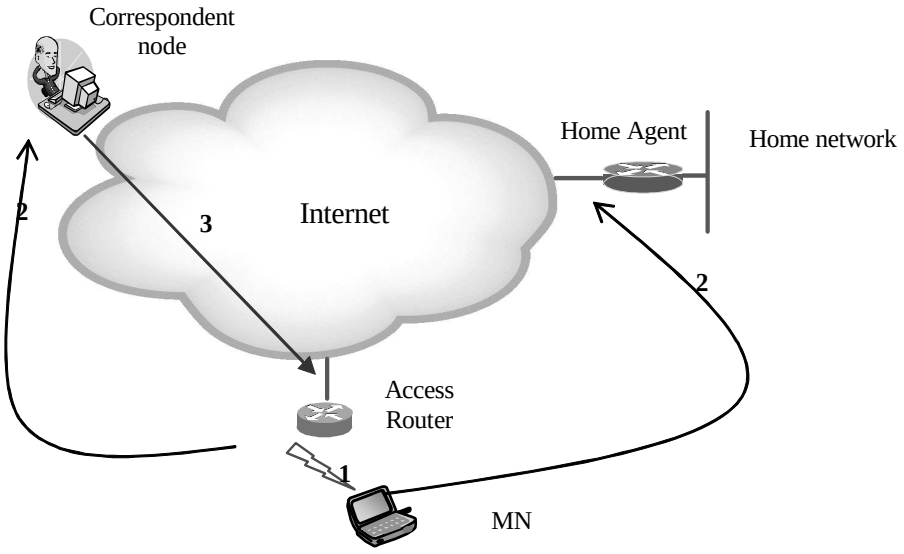
Figure III-2 Temporal diagram of Mobile IP handover

3. Mobile IPv6

Mobile IPv6 [38][39] is the natural evolution of Mobile IP. It supports many improvements of Mobile IP and exploits advanced features of IPv6, as described in chapter II.2. In mobile IPv6, each MN is able to create quickly its own care of address using IPv6 automatic address configuration or stateless address auto configuration mechanism, so foreign agents are not needed. Larger range of address is also available for mobile node in IPv6, which eliminate the problem of address shortage in IPv4.

One of the main evolutions of mobile IPv6 compare to mobile IPv6 is the introduction of native mechanisms to fix the triangular routing anomaly in mobile IP, by the introduction of an additional registration message [40].

When performing a mobile IPv6 handover, the MN can send directly the binding update, with its new CoA, to its corresponding nodes in addition to the HA. Thus, they can learn and create locally a binding entry between the new MN's CoA and its Home address. They send packets directly to the new MN location, without additional routing through the home network, which fix triangular routing problem as shows Figure III-3.



1. MN Connection, CoA auto-configuration

2. MN registers its COA with both HA and its CNs.

3. CN send packets directly to MN location

Figure III-3 Mobile IPv6 Network

Figure **III-4** shows that the consequence of the new direct routing process in mobile IPv6 is the reducing of the end-to-end packets transmission delays in mobile IPv6 compare to mobile IPv4.
In fact we have,

$$T_{MIP\ 6} = T_{CN\ ,nAR} + T_{radio} \quad [5]$$

With,

$$T_{CN\ ,nAR} < T_{CN\ ,HA} + T_{HA\ .nAR}$$

This implies that,

$$T_{MIP\ 6} < T_{MIP\ 4}$$

This improvement in transmission delay has of course a cost. After each handover the MN has to send multiples registration messages to all its correspondent nodes, which introduce additional signalling overhead in the air and in the core of the IP network.

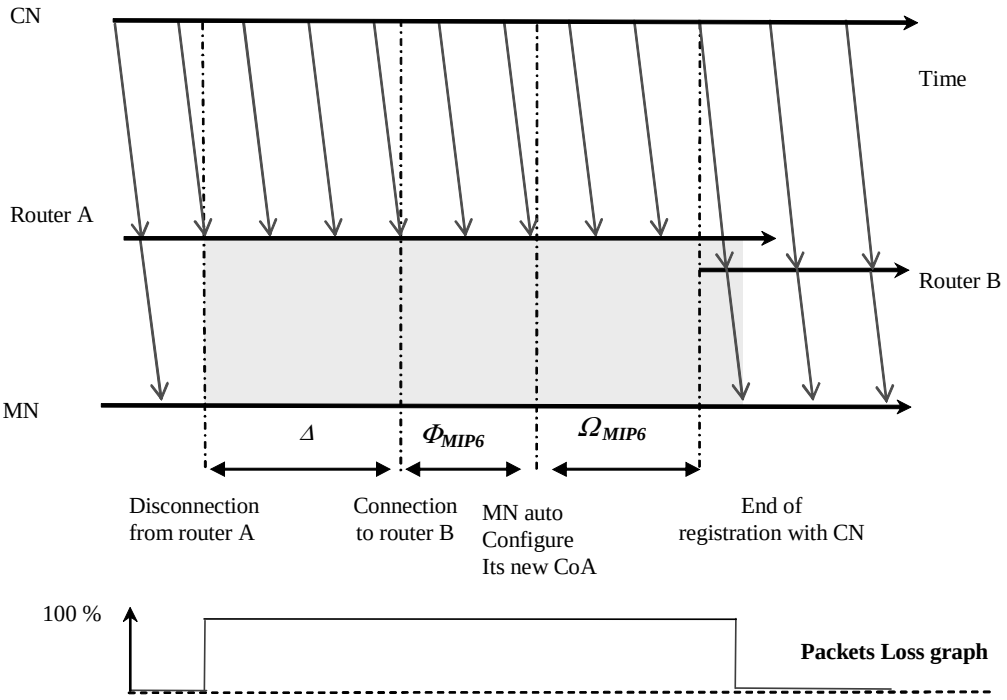


Figure III-4 Mobile IPv6 handover process

In the other hand, mobile IPv6 inherits from mobile IPv4 the big disadvantage of packets loss in Handover; As we can see in packet losses graph, the packets sent by the CN between the moment that the MN leave the old network, to the end of registration process, given by following equation are simply lost.

$$D_{MIP6} = \Delta + \Phi_{MIP6} + \Omega_{MIP6} \quad [6]$$

The number of packet loss is,

$$N_{MIP6} = Th.(\Delta + \Phi_{MIP6} + \Omega_{MIP6}) \quad [7]$$

With Φ_{MIP6} is the MN handover detection and CoA autoconfiguration delays. Ω_{MIP6} is the registration delay of this new CoA, almost a RTT between MN and CN. The jitters value is same as in Mobile IP,

$$J_{MIP6} = \left| T_{CN,oAR} - T_{CN,nAR} \right| + J_{radio}$$

4. Hierarchical Mobile IP

The hierarchical mobile IPv6 protocol [41][42][43] is a straight extension of Mobile IPv6 to support efficiently the Micro-Mobility, or the intra-site mobility [44]**.** This micro mobility protocol is designed for environments, where mobile nodes change their points of attachment to the network, within the reduced area, so frequently that the basic mobile IP mechanisms introduce significant network overhead and long disconnection delays. The base of this solution is that the CN communicating with MN will be only aware of the intra-site MN mobility (macro-mobility) [45], the intra-site movements are managed locally and are completely hidden for current CNs and HA.

This solution is based on the use of a hierarchical home agents architecture named Mobility Agents (MA).The goal is to handle locally mobile IPv6 registration, binding management and packet rerouting for decreasing signaling load and latency over the wired IP network. The registration is local, thus, it reduces the latency of the registration process in case of local mobility.

In hierarchical mobile IP, the network is divided in domain, each domain has its own mobility agent, the domain contains regions with Gateway Mobility Agent per region and in each region we can have multi hierarchical sub region with hierarchical MA of each sub region. The MN that connects for the first time to a domain, register only one time with HA, Any further movement of the MN inside the domains will be transparent for HA, movement within region are hidden for domains MA...etc. Each MA in the hierarchy must maintain an entry in visitor's list for all MN connected to the Leaf MA at the hierarchy. Then bindings are established between the hierarchical MAs.

When MN performs a local handover, the registration is local. It is only forwarded to the first MA that already has a binding for this MN. The upper levels of the hierarchy are not aware of the mobile's movement since they don't have to change their MN binding, as describes in figure III-5. This figure shows a hierarchical network structure and MN different CoAs. The local mobility under each subnetwork is managed within MA1 or MA2. Inter subnetwork mobility requires a binding update within HA and CN.

Any MN micro-mobility movement (intra-site), introduces a local registration of CoA within the nearest local MA, no binding update is required with CN. Ω_{HMIP} is the registration delay in a hierarchical architecture; it is the RTT between the MN and the MA. In a micro mobility, the MA is located closer than a CN, so we have,

$$\Omega_{HMIP} < \Omega_{MIP6}$$

The hierarchical architecture is based on mobile IPv6, so physical movement detection and the CoA autoconfiguraion delays are the similaire,

$$D_{HMIP} = \Delta + \Phi_{MIP6} + \Omega_{HMIP}$$

Thus, packet loss as handover direct consequence is,

$$N_{HMIP} = Th.\left(\Delta + \Phi_{MIP6} + \Omega_{HMIP}\right) \text{ [8]}$$

From [7] and [8], we can conclude that,

$$N_{HMIP} < N_{MIP6}$$

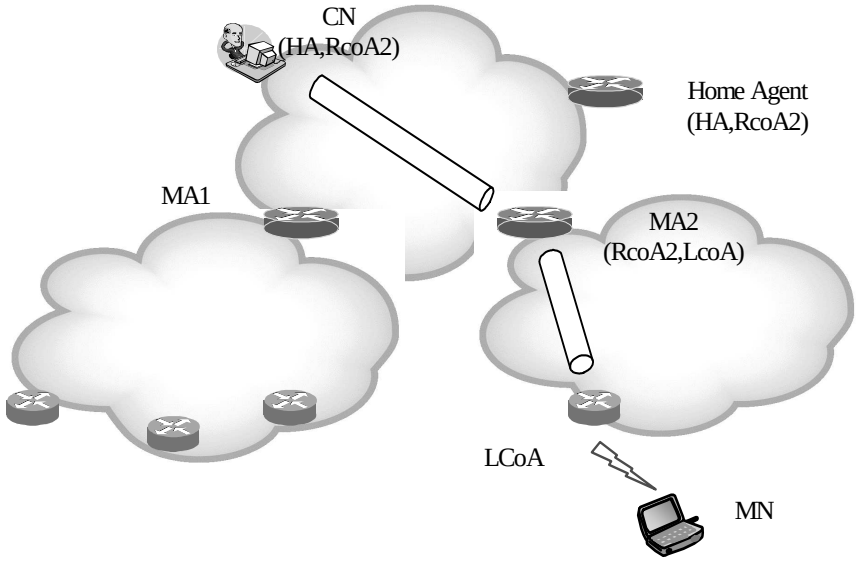


Figure III-5 Hierarchical mobile IPv6 (one level)

In the other hand, the introduction of MAs and successive tunnels encapsulation and encapsulation between them, introduce additional packet end-to-end transmission delay T_{HMIP}, we have

$$T_{HMIP} = T_{CN,MA1} + \sum T_{MAi.MAi+1} + T_{MAn.nAR} + T_{radio} \quad [9]$$

And,

$$T_{CN,MA1} + \sum T_{MAi.MAi+1} + T_{MAn.nAR} \geq T_{CN,nAR}$$

Thus

$$T_{HMIP} > T_{MIP6}$$

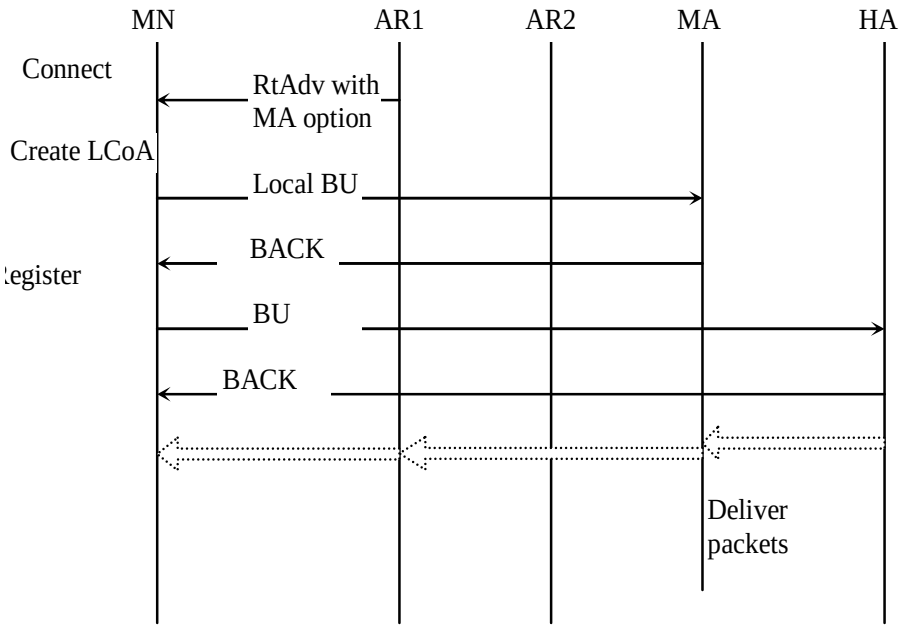
Packets end-to-end transmission jitters in hierarchical mobile IPv6 handover is,

$$J_{HMIP} = \left| T_{MAn,oAR} - T_{MAn,nAR} \right| + J_{radio}$$

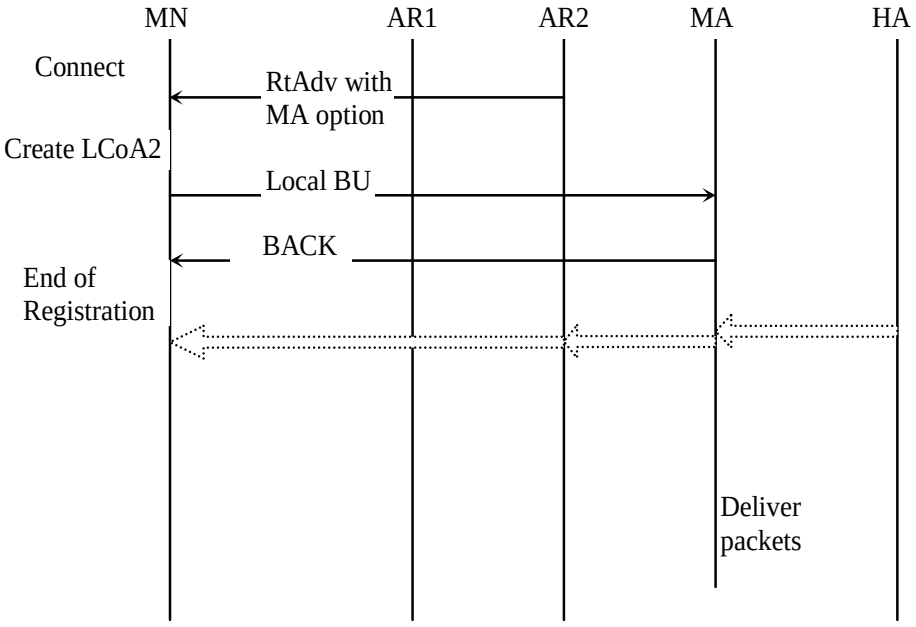
If we consider the supposition of non congested network and the fact that wireless jitters is generally much more important than wireline jitters, we will have,

$$J_{HMIP} \approx J_{MIP6} \approx J_{HMIP4}$$

The figure III-6 depicts the intra and intra sites handover signaling schem3s in hierarchical mobile IP network.



Inter-site mobie node handover to AR1



Intra-site mobie node handover from AR1 to AR2

Figure III-6 Hierarchical handovers signaling

5. Smooth Handover

Smooth Handover [46][47][48] , is part of another family of mobile IP-based handover approach which tries to reduce data losses because of MN handover. This solution can be used either with mobile IPv4 or mobile IPv6. The main idea of this approach is to buffer, in the network, and than retransmits all packets that the CN sends to MN during the handover disconnection. It is done by the introduction of additional buffering mechanisms in access routers.

To perform such idea, access routers have an IP data packet memory space where they can buffer any received data packets before forwards it to the MN. The MN performs handover from the old access router A (oAR) to the new access router B (nAR), when the network layer in MN detects the connection with the nAR, and start registration process, its notify to the nAR the IP address old access router (oAR). The new access router (nAR), than, requests the oAR to create a tunnel from the oAR to itself. The oAR uses this tunnel to forward all buffered packets destined to the MN, to the nAR, which sends them to the MN. The oAR is not aware of the delay of MN disconnection, so it has no information about which packets were already received by the MN, so it forwards all buffered packets to the nAR. As results, the MN can receive duplicated packets through old and new AR.

An optimized smooth handover buffering mechanisms was proposed in [49][50]. To reduce duplicates packets sent to the MN, when the mobile roams to the new network, the MN gives the IP headers of the last packets it received to the nAR. This one includes them in its forward request to the oAR, which answers by forwarding only the lost packets. The use of hierarchical FAs architecture also can be used to reduce the mobile IP registration overhead of a local handover.

In figure III-8 we illustrate the data flows exchange between a CN and MN during smooth handover, with buffered packets tunneling, from old AR to the new one at the end of registration process.

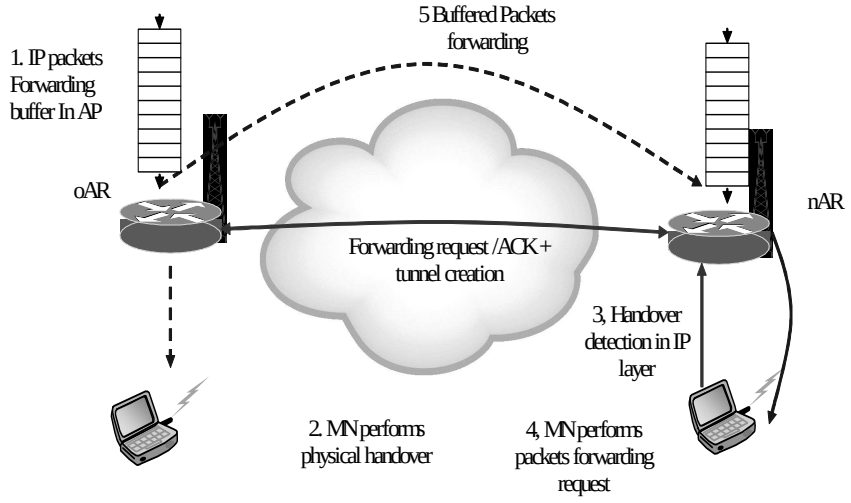


Figure III-7 Smooth handover process

First, the MN disconnection delay, is exactly similar with Mobile IPv6 handover global delay D_{MIP6}, given by equation [6]. In the same time, the number of lost packets is considerably reduced,

$$N_{Smth} = \max(0, B - Th.D_{MIP6})$$

With, B is the size of buffer access router buffer. If the size B is larger than the number of packets sent by CNs and buffered in oAR: $B >= Th.D_{MIP6}$.
This mechanism can avoid packet loss. On the other hand, these additional buffers in ARs and buffered-packets tunneling between ARs after the handover, introduces additional end-to-end transmission delay and much more jitters in the handover.

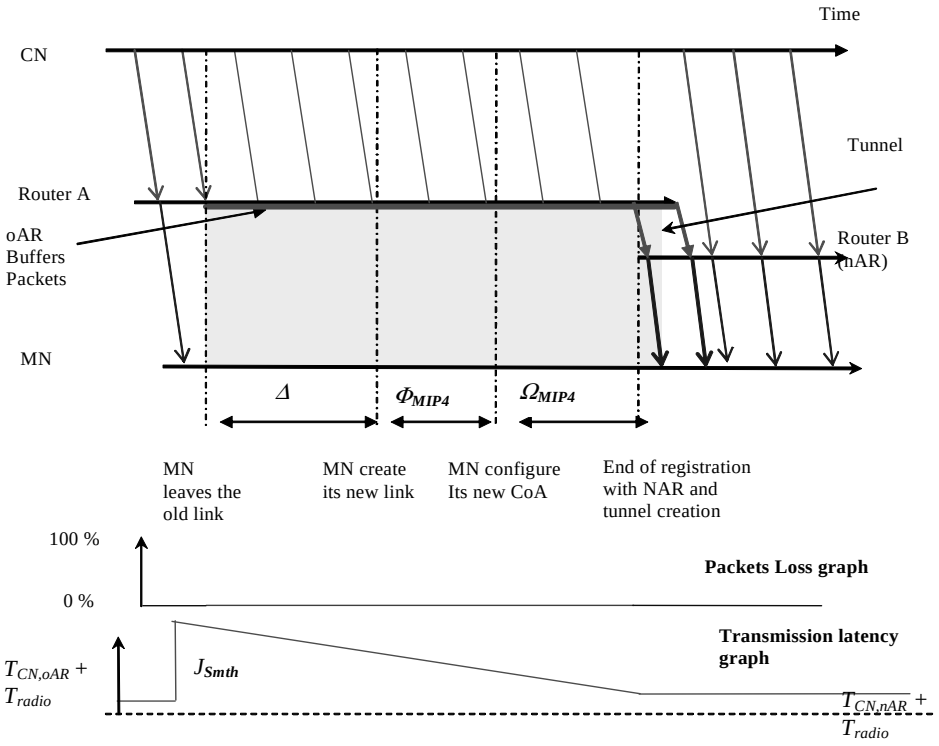


Figure III-8 Smooth Handover data flows

The new end-to-end transmission delay of buffered packet in oAR at handover is,

$$T_{Smth} = T_{CN,oAR} + x.D_{MIP6} + T_{oAR,nAR} + T_{radio}$$

with $0 \leq x \leq 1$. the value of x depends on the moment that packets arrive to AR compare to handover beginning. For packet arriving at the handover beginning, the value of x is equal to 1 and this packet will be buffered during all handover delay (D_{MIP6}).

The transmission delay of packets without handover is similar to mobile IPv6,

$$T_{Smth} = T_{CN,nAR} + T_{radio}$$

The jitters introduced by the handover is,

$$J_{Smth} = D_{MIP6} + T_{oAR,nAR} + J_{radio}$$

and,

$$T_{oAR,nAR} \geq \left| T_{CN,oAR} - T_{CN,nAR} \right| \text{ and } D_{MIP6} > 0$$

so,

$$J_{Smth} > J_{MIP6}$$

We can conclude that the smooth handover can avoid or minimize packets loss because of the handover, but in the other hand, it introduces additional end-to-end transmission delay and important jitters. This solution cannot be suitable for real time application.

6. Fast Handover

Mobile IPv6 Fast Handover [51][52][53] and fast handover Bicasting [54][55] improve basic mobile IPv6 handover mechanisms by reducing the MN global disconnection delay in order to reduce the number of lost packets and, thus, minimize perturbations in current application sessions.

One of the main problems with mobile IP in handover management is the heavy and long MN physical movement detection in network layer: this is only achieved with IPv6 mobility mechanisms as the router Advertisement and router solicitation Request. Fast handover assumes an interaction between the network layer (layer 3) and Mac layer (layer 2) to remove layer 3 handover latency. This allows anticipating the physical handoff, and provides the MN with the possibility to configure its new CoA and start registration with the new AR by the way of the old AR. As results, the MN performs IP handover and physical handover simultaneously and can be able to receive data immediately after performing physical handover.

The basic principle of this solution is that shortly before the MN will be at the point to initiate a physical handover to a new AR, the IP layer receives the handoff events information as ”triggers” from the Mac layer. Using this information the network can determine the IP address of the nAR to which the MN will get to attach next. It sends this information to the MN, which forms a new CoA using Address auto configuration. The MN can perform than physical handover and oAR will tunnels all MN destined packets to the new MN address. As soon as the MN establishes a physical connection with the nAR, it can start

receiving data, and initiates its registration with home agent and current CNs through its old access router. The Figure III-9 depicts soft handover steps.

Fast handover bicasting is the evolution of the basic fast handover approach. The main difference is in data transmission between ARs and MN during the handover process. During the fast handover process it is not possible to know in advance precisely when the MN will physically detach from the old AR and connects to the new AR. Therefore, it is not simple to determine the correct and exact moment to start IPv6 packets tunneling between old AR and new AR, which has an impact on how smooth the handover will be. In addition to packet loss generated by MN physical handover, addition packets loss will occur if the forwarding is performed too late or too early.

In order to avoid that old AR starts packets tunneling to the MN new location before the physical handover, or to reduce the packet loss, the old AR sends the new location information to the MN, it can then, duplicate and bi-cast IPv6 packets to the MN's old and new CoAs.

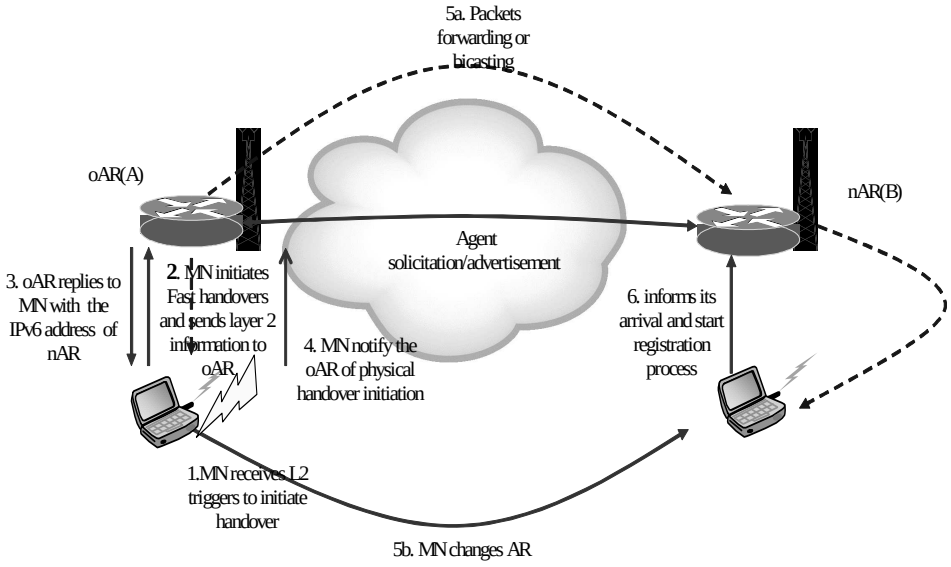


Figure III-9 Fast handover process

From the Figure III-9, we can see that fast handover mechanism reduces sensibly the MN global IP disconnection compared to basic Mobile IPv6, but it cannot avoid completely the packets loss. In fact during the physical disconnection, there is no way for the MN to receive any packets. Without buffering mechanisms, there are no mechanisms to recovers lost packets and they will be simply lost. The number of lost packets depends on the delay of physical handover, $N_{Fast} = Th.\Delta$

In the other hand, the inexistency of smooth handover buffering mechanisms can be positive, the end-to end transmission delay during the handover is largely reduced; the maximum delay is registered for packets tunneled from oAR to the nAR and than to the MN, it is given by,

$$T_{Fast} = T_{CN,oAR} + T_{oAR,nAR} + T_{radio}$$

But after performing the registration with CN, the delay is optimized to,

$$T_{Fast} = T_{CN,nAR} + T_{radio}$$

the maximum jitters is

$$J_{Fast} = T_{oAR,nAR} + J_{radio}$$

The conclusion is ,

$$J_{Smth} > J_{Fast} \geq J_{MIP6}$$

The Figure III-10 describes data flows dursing a fast handover process.

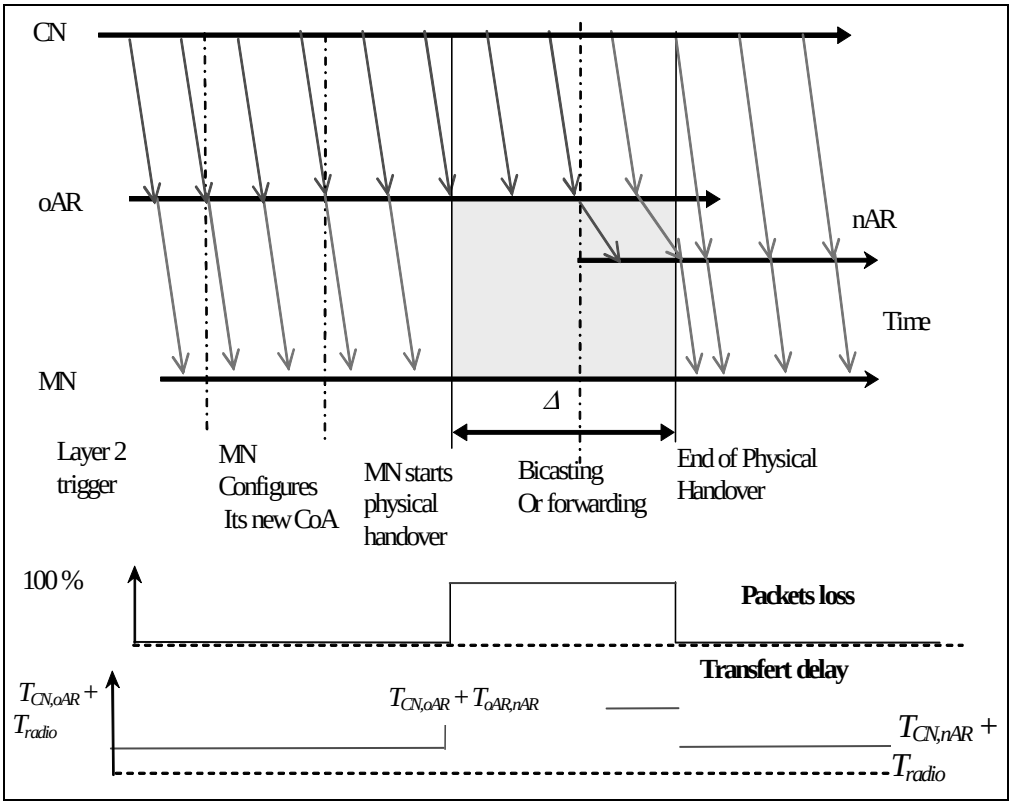


Figure III-10 Fast handover data flows

7. Handover Comparison Summary

We propose in this paragraph to summarize the results of our analysis and to give a brief comparison of described propositions that manage handover in IP layer. The table 2 summarizes the different notations used in this chapter and Table 3 represents performances summary and comparison of these approaches. Mobile IPv4 is the first solution to introduce simple mobility management mechanisms in IP world. When performing the handover, the MN disconnection is relatively important, which imply an important packet loss ratio. In addition the triangular touting of IP packets from CN to MN introduce additional end-to-end transmission delays in the core of the network.

Mobile IPv6 is the straight evolution of mobile IPv4 in IP6 protocol. It exploits the IPv6 protocols features and improvement, such address autoconfiguration mechanisms that suppress the need of foreign agents. As results, the use of Mobile IPv6 protocol simply the process to get a new care of address and lightly reduce the overall MN disconnection delay during a handover. Thus, reduces the number of lost packets proportionally. The implementation in Mobile IPv6 of a native registration mechanism between MN and CNs, fix the triangular routing problem and reduce the end-to-end delay. Unfortunately, they still no specific handover management mechanism in Mobile IPv6, which cause important packet loss and transmission Jitters quit similar to Mobile IPv4.

The network re-structuration, proposed in *Hierarchical Mobile IP*, improves handover performance in the special case of local MN mobility (micro-mobility). In the case of local MN movement within a micro mobility domain, the registration is within local MA and the signaling load needed to register the handover in IP layer is reduced in the core of the network. The local registration means also requires a shorter signaling delay (Round Trip Time “RTT” between MN and MA).The global MN disconnection during a handover is then shorter, and the number of lost packets is reduced. On the other hand, the successive tunneling (encapsulation and decapsulation) of packets between Mobility agents, increases end-to-end transmission delay. In the case of global handover (macro – mobility), the handover process is similar to basic mobile IP, and in this case this solution does not improves handover performances.

The introduction of access routers Buffering mechanisms in s*mooth-handover approaches* reduces sensibly packets loss risks. The packets buffering and recovering after handover have another negatives effects, it increases sensibly end-to-end jitters within the handover. That makes this solution not suitable for application with high level real time constraints.

The fast handover and fast handover bicasting mechanisms reduce sensibly local MN disconnection delay in handover. This can be done using an interaction between link and network layers. If such us interaction can be provided, this solution reduces the disconnection delay and proportionally packet loss. Note that fast handover can increase lightly the jitters, because the additional delays introduced by packets tunneling between the old and new location of the MN after the handover. Some works done in [56][57][58] shows that a fast and hierarchical handover can be deployed and is efficient to improve overall handover performances.

T	End-to-End packet transmission delay
N	Sum of lost packet in handover
Th	Transmission throughput between the CN and the MN
D	MN disconnection global delay
Δ	Delay of physical handover
Ω	Delay of IP registration in handover
Φ	Configuration of CoA delay
$T_{x,y}$	Propagation delay from node X to node y
T_{radio}	Radio propagation delay
B	Buffer size
$cwnd$	Congestion window size (TCP)
RTO	Retransmission Time Out (TCP)
RTT	Round Trip Time (TCP)
J	Handover Jitters

Table 2 General notation.

	Handover performance	Comparison
Mobile IP4	- $D_{MIP4} = \Delta + \Phi_{MIP4} + \Omega_{MIP4}$ - $N_{MIP4} = Th.D_{MIP4}$ - $T_{MIP\ 4} = T_{CN,HA} + T_{HA.nAR} + T_{radio}$ - $J_{MIP4} = \lvert T_{CN,oAR} - T_{CN,nAR} \rvert + J_{radio}$	
Mobile IP6	- $D_{MIP6} = \Delta + \Phi_{MIP6} + \Omega_{MIP6}$ - $N_{MIP6} = Th.D_{MIP6}$ - $T_{MIP\ 6} = T_{CN,nAR} + T_{radio}$ - $J_{MIP6} = \lvert T_{CN,oAR} - T_{CN,nAR} \rvert + J_{rafio}$	- $\Phi_{MIP4} > \Phi_{MIP6}$ - $T_{MIP\ 6} < T_{MIP\ 4}$ - $J_{MIP6} = J_{MIP4}$
Hierarchical Mobile IP	- $D_{HMIP} = \Delta + \Phi_{MIP6} + \Omega_{HMIP}$ - $N_{HMIP} = Th.D_{HMIP}$ - $T_{HMIP} = T_{CN,MA1} + \sum T_{MAi.MAi+1} + T_{MAn.nAR} + T_{radio}$ - $J_{HMIP} = \lvert T_{MAn,oAR} - T_{MAn,nAR} \rvert + J_{radio}$	- $N_{HMIP} < N_{MIP6}$ - $T_{HMIP} > T_{MIP6}$ - $J_{HMIP} \approx J_{MIP6} \approx J_{HMIP4}$
Smooth Handover	- $N_{Smth} = \max(0, B - Th.D_{MIP6})$ - $T_{Smth} = T_{CN,OAR} + x.D_{MIP6} + T_{OAR,NAR} + T_{radio}$ - $J_{Smth} = D_{MIP6} + T_{oAR,nAR} + J_{radio}$	- $N_{Smth} < N_{HMIP}$ - $T_{Smth} > T_{MIP6}$ - $J_{Smth} > J_{MIP6}$
Fast Handover	- $N_{Fast} = Th.\Delta$ - $T_{Fast} = T_{CN,oAR} + T_{oAR,nAR} + T_{radio}$ - $J_{Fast} = T_{oAR,nAR} + J_{radio}$	- $N_{Fast} < N_{MIP6}$ - $T_{Fast} \geq T_{MIP6}$ - $J_{smth} > J_{Fast} \geq J_{MIP6}$

Table 3 Classification & comparison of IP-Based handover propositions

8. Special Case studies, Handover Effects on TCP

After the reviewing and the analysis of IP-handovers approaches using a simple transport protocol such UDP. We investigates now, the effects of these handover mechanisms on a more sophisticated transport protocol namely TCP.
TCP (Transmission control protocol) [60][61] and UDP are the most used transport protocol in the Internet. TCP provides applications with a reliable byte-oriented delivery of data on the top of IP protocol. This complex protocol was designed and turned to perform well in wireline network, where the key functionality is to optimize the use of available bandwidth and avoid overloading of network.

8.1. TCP Response to Lost Packets

TCP is a connection oriented transport protocol, which identifies each connection by a sender and receiver. It performs packets transmission, control and network state evaluation in the same time. TCP responses to lost packet are turned to work well for the detection of the congestion in wired network, and the adaptation of the emission throughput to reduce this congestion. The problem is that in the presence of high bit-errors rates in wireless environments and mobile node disconnection during handovers, packets loss is not caused always by congestion, but TCP thinks so, which causes the sub-optimum performance [62].
TCP considers that a sent packet is lost if no acknowledgement (*ACK*) is received within the retransmission timeout (*RTO*) period. The *RTO* value is based on measurements of the required round-trip delay time (*RTT*) for sent packets to travel over the link. These RTT measurements are collected and the *RTO* is set to the average *3* RTT*. A reasonable *RTO* is crucial to effective utilization of resources. If the *RTO* is excessive, retransmission will be unnecessarily delayed. If the *RTO* is too short, unnecessary retransmissions will occur and effective throughput will be decreased. When a lost packet is determined by expiration of the *RTO*, TCP initiates an exponential backoff of the *RTO* and enters the slow start and congestion avoidance mode. The exponential backoff of the *RTO* involves doubling its value with every expiration, after packets retransmission. Then measures are taken to reduce the packet transmission rate so that congestion can be avoided. Slow start involves setting the congestion window, which indicates the number of packets that can be sent without causing congestion, to one packet. With each *ACK* of a received packet, the congestion window is exponentially increased.
When the congestion window reaches a threshold value corresponding to half its value when the loss was determined, congestion avoidance takes over. In this phase, the congestion window is increased only linearly. When considering transmission over a wireless link, it is important to note here that multiple lost packets will cause the slow start threshold to be repeatedly initiated, and thus the congestion avoidance mode will dominate and the packet transmission rate will grow very slowly. This can lead to degradations in throughput.

8.2. TCP Versions & Packet Loss

In the first version of TCP, if packet is not acknowledged within specific time interval RTO, the slow start procedure is entered, thus, there is throughput degradation. In *TCP Tahoe*, after receiving a small number of duplicate acknowledgments for the same TCP packet (DACK), the data sender infers that a packet has been lost and retransmits the packet without waiting for a *RTO* to expire, that is called fast retransmit mechanism.
Fast recovering mechanism introduced in *TCP Reno*, enhance fast retransmit to avoid slow start algorithm. The idea is that DACK also indicates that packets are leaving the network. Thus DACK can be used to clock sending of data and instead of entering slow start, Congestion window is set to half its previous value in the presence of DACK, and grows with additive increase rather than slow start. However this mechanism still only addresses single packet losses. To solve Reno TCP's performance problems when multiple packets are dropped, *TCP-SACK* uses selective acknowledgements option to enable the receiver to inform the sender about TCP packets that have been successfully received. Thus by making use of selective acknowledgements option SACK in Duplicate ACK packets, the sender can estimate which packets have been lost and retransmit them immediately with, of course, slow start algorithm avoidance [63].

8.3. Mobile IPv4 & Mobile IPv6 Handovers

As stated earlier, the handover delay in Mobile IPv4 is given by $D_{MIP} = \Delta + \tau$, with Δ is movement detection delay and $\tau = \Omega._{MIP4+}\Phi_{MIP4}$ is the protocol delay overhead caused by MN new IP address configuration and registration. Note that $\Omega._{MIP}$ is almost RTT between CN and MN. During this period all sent packets are lost, and if D_{MIP} is too Long ACK from MN will not reach the CN. This one considers these unacknowledged packets to be lost and such thing has two direct negative effects on TCP performance.
First, each TCP packet has to be acknowledged before the end of RTO=3*RTT, if not they are retransmitted. To prevent network congestion, during this lapse of time, D_{MIP}, the RTO is doubled for each unsuccessful transmission. This algorithm called exponential backoff increases so much the delay of retransmission RTO beyond D_{MIP}, that at the end of registration process, there can be period of no activity in which TCP communication remain halted even after the completion of handover [65][68].

Secondary, TCP will assume that packet losses during D_{MIP} is due to congestion, so mechanisms for congestion prevent as Slow Start algorithm will be used. As a result of long handover delay, TCP will repeatedly reduce its transmission-window size, and this lead to unjustified degradation in TCP throughput at the MN new AR. Figure III-11 show us Mobile IP handover effects on TCP connection with, $\Delta + \tau = 11 * RTO$.

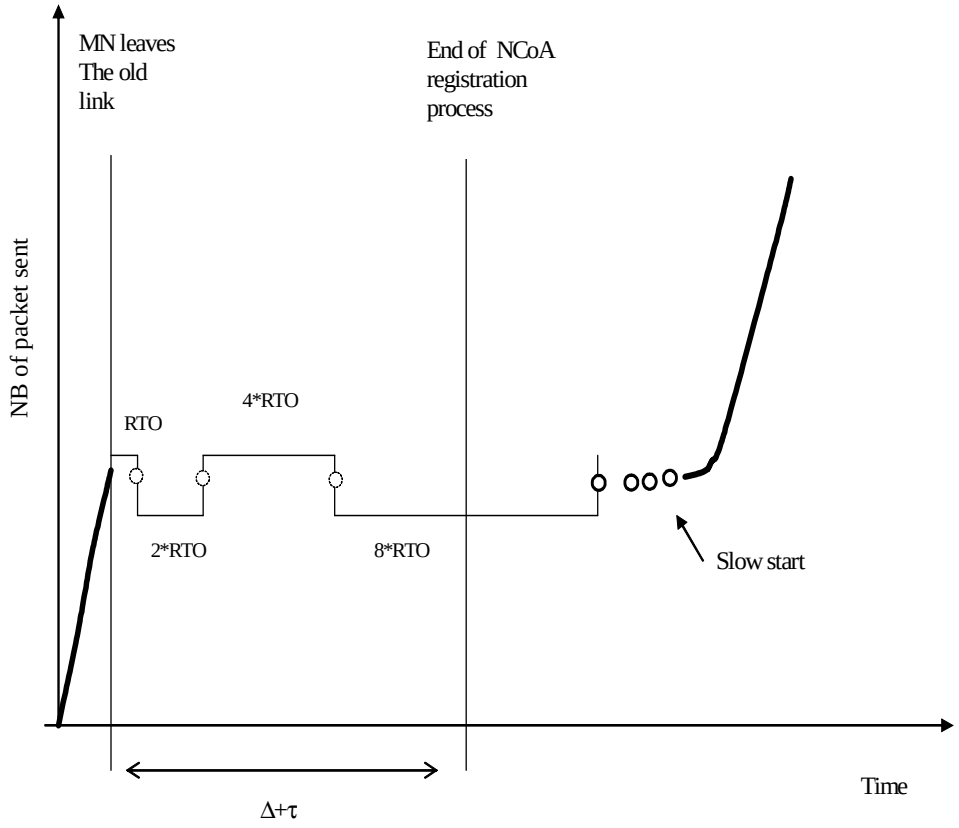


Figure III-11 TCP connection during handover

8.4. Fast Handover

As described bellows, both of fast handover and bicasting approaches, reduces sensibly the period of time between disconnecting from the oAR and the point in time where MN and HA are again appropriately configured to Δ.
We will base on the simulation work done in [64], to show the benefice of shorter handover delay (fast handover or hierarchical), on performance of modern TCP implementation employing selective acknowledgements (SACK).
In long MN disconnection due of basic Mobile IP handover process, TCP sending window will fill up, which block transmission until an *RTO* occurs. In contrast with faster handover process:

- The sending window does not fill up during disconnection delay caused by MN handover.
- the sending window is large enough such that sender can continue send packets after the handoff is complete

- Duplicate packets indicates that packet loss occurred and require instant retransmission
- the SACK options signal which packets to be retransmit
- The sender will retransmit these packets
- The slow start process can be avoided.

Let *Thp* stands for CN data rate and *S* for the size of TCP sending windows. The handover disconnection delay D_{fast}, for which the slow start algorithm will be avoid is determined via

$$Thp * \left(RTT + D_{fast}\right) < S$$

Thus,

$$D_{fast} < \frac{\left(S - Thp * RTT\right)}{Thp}$$

8.5. Smooth Handover

Smooth handover intends to reduce or suppress the number of packets dropped during MN handover process: $D_{Smth} = \Delta + \Phi_{MIP6} + \Omega_{MIP6}$. This can be done, as we shown in III.5 by the introduction of buffering mechanisms to recover lost packets. In follows, we will investigate TCP performances considering packet buffering-mechanisms when effecting MN handover.
We consider the case where CN sends packets to the MN through an established TCP connection. First, If we let $\boldsymbol{S}$ the size of TCP sending windows, $\boldsymbol{D_{smth}}$ The MN disconnection delay, when performing handover,

$$D_{smth} = \Delta + \Phi_{MIP} + \Omega_{MIP}\,.$$

The requirement in Smooth handover buffer size $\boldsymbol{B_{size}}$ to recover all TCP packets dropped during this disconnection, can be determine by

$$B_{size} = \min\left(\frac{S}{RTT} * \mathrm{D}_{\mathrm{smth}}, S\right)$$

If the buffer size is smaller than $\boldsymbol{B_{size}}$, it might overflow and some TCP packets dropped early in MN handover process can not be recovered, until new *RTO* occurrence. Secondary, basic Buffering mechanisms in smooth handover can not always improve TCP performance while handover, even when the size of buffer is larger then number of lost packets. In this case, if the old AR tunnels some buffered packets, and if these packets have been already received by MN successfully through oAR, towards the new AR after performing handover. These packets, will triggers duplicate ACKs at the MN, which direct consequence is immediate activation of Fast retransmit process in CN, and the finale impact is the reduction of TCP connection rate.

Third, as in fast handover, the number of non-acknowledged packets is limited by the TCP window size and MN disconnection. If D_{smth} is too much bigger then *RTO* value, there will be TCP packet retransmission, and if TCP sender achieves its maximum widow size, slow start algorithms will be trigged.
Worst, when MN achieves its handover process, buffered packets and retransmitted packets will trigger duplicate ACK at TCP receiver.

9. Conclusion

Mobile IPv4 is the oldest and simplest solution to manage mobility in IP networks, its simplicity makes it easy to deploy. In the other hand, the poor performance of its handover makes it not suitable for real time applications. Moreover, the analyses the performances of a sophisticated protocol such TCP, shows that Mobile IP handover causes a mobile node long delay disconnection which introduces several successive timeouts. The consequence is that after a handover, the TCP connection remains halted even after MN reconnection and moreover, it can trigger slow start algorithm, which reduces TCP throughput. Mobile IPv6 improves mobile IPv4 mechanisms using IPv6 features. It fixes the triangular routing anomaly in mobile IPv4 and allows the mobile node to auto-configure its IPv6 address, which avoid foreign agents deployment in the network. The hierarchical mobile IP (4/6) proposes to localize the mobility management signaling. The main goal is to reduce the handover registration delay. Thus, reduce the overall mobile node IP disconnection during a handover. Smooth handover introduces buffering mechanisms in access routers to recover lost packet during MN disconnection in handover. UDP analysis shows that this solution combined with optimized buffer size is efficient to recover lost packets. However, buffering introduces additional jitters and transmission delays during the handover. TCP analysis shows that in major cases, the introduction of IP-buffering mechanisms when performing handover cannot prevent timeouts from occurring and triggering slow start algorithm. Moreover TCP performance can be further degraded than the case of Mobile IP because of duplicate acknowledgement. Fast handover “bicasting” is a solution more adapted to real time traffic. It exploits an interaction between the MAC layer and IP layer to anticipate the handover. Thus, reduce the overall handover delay to the physical roaming latency. TCP performance can benefit from the combination of fast handover reduced handover delay and TCP selective acknowledgement to avoid the triggering of TCP slow start process.

CHAPTER 4

IV. Proposed Mechanisms to Introduce IPv6 Soft Handover in Mobile IPv6

1. Problem Overview

To achieve efficient mobile node mobility among different IP access points and sub networks, several solutions have been proposed in both IPv4 and IPv6. In order to prevent and reduce data loss, some solutions are based on additional buffering mechanism in access routers, to recover lost packets after the IP handover, such as “Smooth Handover”. But the efficiency of this family of solution depends essentially on the buffers size, if too small, it may overload and packets can be lost. If too large, the MN can receive same packets twice at its two locations, and duplicate reception of packets can perturb TCP throughput. Other mechanisms as “Hierarchical Mobile IP” reorganize the Mobile IP basic network architecture; they introduce an intermediate home agent in the network to reduce mobile node IP registration delay after the physical handover, thus reduce global handover delay and packet loss, but just for local handover. Another mechanism has been defined in prior document “Fast Handovers for Mobile IPv6”, in this system , before the handover occurrence, the mobile node is able to obtain its new CoA on its new location using an interaction between Mac layer and network layer. When the handover occurs, the access router forwards all packets to the new attachment. The handover delays and packets loss are significantly reduced, but the loss of packets cannot be avoided, it can happen when the mobile node has physical disconnection from the network.

In addition to packet loss, and transmission delays problems of IP-based handover, which still remains unresolved as explained in chapter II, there is still the general problem of the quality of service of the data communication based on radio transmission. More generally, in border wireless coverage areas, the radio waves from both old and new access routers are usually weak, this degradation of radio signal increases the bit-error rates which introduce an important non negligible jitters and packet loss ratio and can enable mobile node ping-pong effect when performing handover between these access routers. Even when no handover is involved, there is still a need for improving data communication from wireless packet-loss, between a mobile node and an IPv6 internet network. Fast handover bicasting enables data duplication through old and new access router, but the mobile node can not receive more than one IP data flow at a time. Sending the same packets flow through different access routers, in this case, is inefficient. Only one copy of duplicated packet can be received by the mobile node.

Soft handover is process during which the mobile nodes are able to have two or more simultaneous connections through different access routers. Multiple identical copies of each packet are simultaneously transmitted to the mobile nodes through these access routers.

In third generation networks, which are predominantly based on WCDMA technology, a more sophisticated soft handover concept is introduced [20][92]. The mobile node can send, receive and combine multiples signals simultaneously on a bit-by-bit basis. Compared with the conventional hard handover, soft handover has the advantages of lossless handover and reduced ping-pong effects. As well as leading to continuity of the wireless services, it has been proved that the soft handover improve the overall wireless link quality [92]. The integration of this approach in WCDMA network requires that,

- The MN combines the information received from different access points on physical layer
- All involved access routers have to be tightly synchronized and a scheduling scheme ensure that that they will transmit the same packet in the same moment, so it can be combined at the reception.

Today and for the purpose of next generation of mobile communication systems, mobile users are facing the fact that many heterogeneous radio access technologies coexist, ranging from wireless LANs to cellular systems. No technology has emerged as common and universal solution which makes the current trends toward the design of All-IP wireless and wireline networks, where radio cells are under the control of IP access routers for signaling and data transmission. That will allow a ubiquitous IP-based access to the mobile users, regardless the heterogeneity of the radio access technology. The design of an All-IP wireless network requires an efficient and flexible handover management, independent of used radio access technologies, to fit the IP-based application quality of services requirements.

Tao-Zhang & co try to propose general IP layer principles and mechanisms to integrate soft handoff in IPv4-based networks [70].They identify some key-elements in the conception of efficient soft handover system.

- First, IP-stream data packets have to be duplicated somewhere in the core network to create multiple copies of the IP stream.
- Second, these duplicated packets have to be distributed via different access routers to a Mobile Node.

The drawback of theirs proposition is the requirement of strong interaction with the link layer. Moreover IP access routers need strong synchronization mechanisms to synchronize duplicated packets sending and combination at reception. Actually they do not present any idea about duplication mechanisms, but they proposed a Mac address based mechanisms to distribute and sends mobile node packets to the right access routers (routers where the mobile node is attached on simultaneously).

For the purpose of soft handover in 4G networks, the MN can be connected simultaneously to two heterogeneous APs. Any soft handover proposition should to be independent of synchronization mechanisms, because it is really difficult to synchronize wireless transmission over heterogeneous wireless access technologies. Our solution, Mobile IPv6 soft handover [71][72][73][74][75] is a complete and pure IPv6 end-to-end solution, which extends and coexists with mobile IPv6 protocol without major modification. It allows mobile IPv6 multihoming management and enables mobile node data reception and emission through multiples access routers simultaneously at IP layer. Such as feature allows,

- The mobile node's session to progress without interruption when it moves from one wireless cell to another regardless of theirs radio access technologies (a lossless and transparent heterogeneous handover).
- It allows also an improvement of wireless part of communication in overlapping regions with poor radio coverage. If the mobile node receive in border area duplicated copies of flows simultaneously through different access router, accept the first received packet and ignore the rest. The objective is to reduce packets end-to-end delays, jitters and packets loss as consequence of radio signal degradation.
- This solution introduces a new IPv6-router concept, "Duplication & Merging Agent" (D&M) agent. It is a conventional IPv6 router located within the IPv6 Network, and is used for
  1) The management of mobile node IPv6 multihoming locally, to make it completely transparent to home agent and other correspondents.
  2) The duplication and the merging of IPv6 packets going to and arriving from the communication links.
  3) Resources call admission and quality of services management.

The IP soft handover approach is based on four main processes: multihoming and registration process, flows duplication process, flows merging process and handover process. They allow duplication and merging of IP flows without the need to synchronize duplicated IP-flows and access router in wireless transmission. The Figure IV-1 shows a MN within overlapping coverage areas. The soft handover can occurs in such as zone.

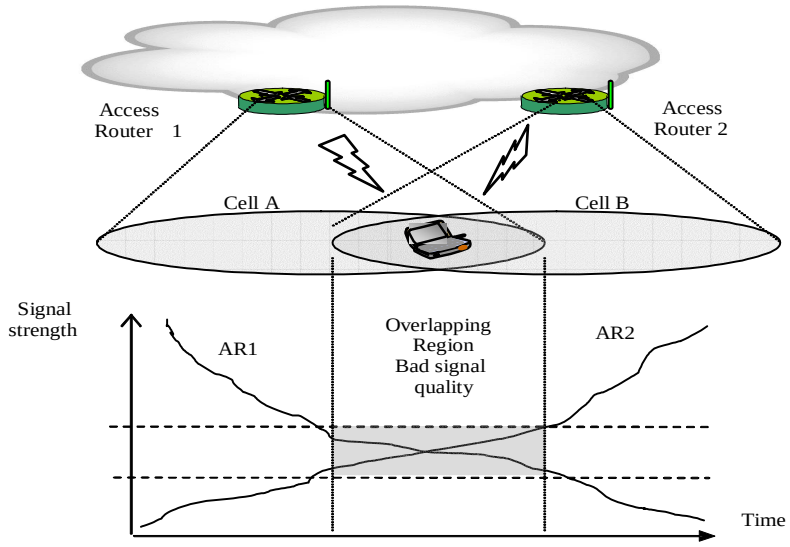


Figure IV-1 Overlapping coverage areas

2. Multihoming and Mobile Registration

The multihoming is the MN ability to have multiple network addresses to identify its multiples and simultaneous connections to the network. At this time, the study of multihoming problem is at a very early stage and it is one of the most critical problems in the current specification of mobile IPv6 protocol. Mobile Pv6 is designed to allow a mobile node to maintain its sessions while roaming between IPv6 sub networks. However, the current specification does not give hints or requirements to deal with mobile nodes with multiple points of attachment to the network, i.e. a multihomed mobile node. We are thus proposing the current mobile IPv6 based mechanisms to fill this gap. Mobile node multihoming management in IPv6 enables several features such as ubiquitous access, redundancy/fault recovery, load sharing, load balancing, bicasting and preferences settings. In this chapter we will propose general mechanisms that can be used to achieve all these goals. But, the main objective of multihoming process design in this dissertation is to propose a signaling protocol to achieve a transparent and hierarchical bidirectional soft handover at the same end point on mobile IPv6.

2.1. Multihoming in Mobile IPv6

To understand the need to extend mobile IPv6 with multihoming mechanisms, we use an “always on” scenario, as described in Figure IV-2, where the mobile node have a basic connection to the core of the network through a wireless 3G interface to global coverage This mobile can also simultaneously access the

network, when it is possible, through a high efficient or lower cost technologies as WLAN IEEE802.11. The user can choose to redirect some applications flows to the 802.11 interface, and to use 3G interface for the rest of flows.

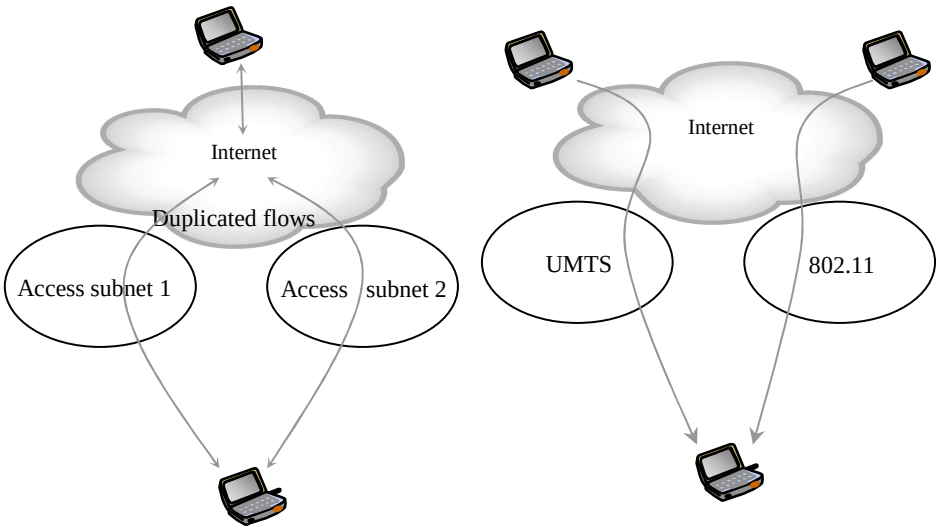


Figure IV-2 Multihoming scenarios

Another scenario consists on a user which is able to have multiple interfaces within one or more technologies. For application with heavy QoS and real time constraints, the user can exploit this interfaces diversity to achieve a seamless handover and perform flows redundancy over different access routers to reduce packets loss and jitters in a bad coverage area. The attractiveness of using multihoming management in Internet protocol layer and mobile IPv6 is that these mechanisms will be independent from radio access technologies. It can therefore be used in heterogeneous radio access technologies without major consideration of the type of the interface. Unfortunately, at this time mobile IPv6 is not able to offer such kind of service. Mobile IPv6 identifies the mobile node as a single and unique entity with a unique connection to the network, this connection is defined by a reference address (Home address), and temporary address (care of address) to identify its new location when it moves away from its home network. This CoA identifies the whole mobile node, and not a specific connection through a specific interface. No more than one CoA can be registered in the home agent in the current mobile IPv6. This feature implies that the MN can receive IPv6 data flows using only one interface at a certain time. In Figure IV-3 the mobile IPv6 MN gets a connection through first interface to the network, it gets a valid CoA1 and registers it within the HA. The MN has another interface, and at certain moment it decides to connect this interface to another access router, and start sending or receiving data flows through the two interfaces simultaneously. The MN sends a binding update to the HA and correspondent nodes with the new CoA2 assigned to the second interface. Considering the current mobile IPv6 specification, the HA and correspondent

nodes refresh the entry related to the MN and create a new correspondence between the home address and CoA2, erasing the old correspondence between the home address and CoA1. That implies the MN can not continue to use the first interface with the mobile IPv6 protocol.

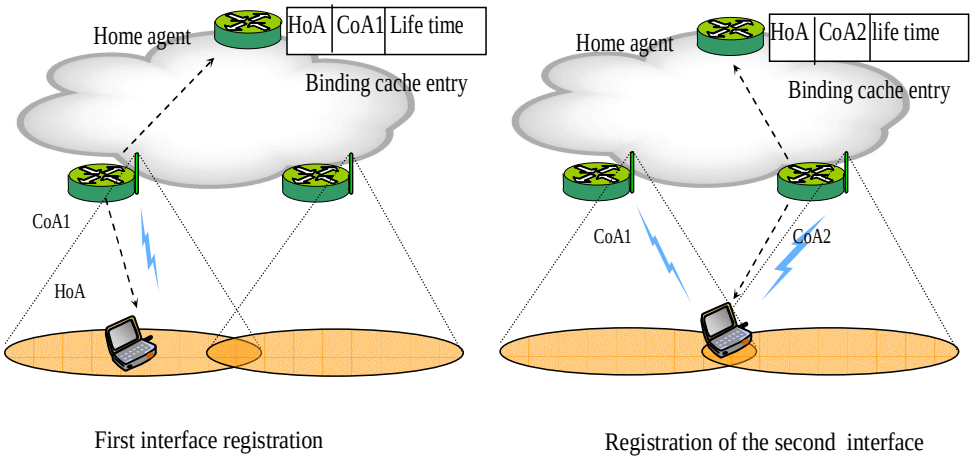


Figure IV-3 Consequences of multi interface use in MIPv6

2.2. Existing Design Possibilities

Recently, some mechanisms were proposed [88][89][90] to introduce multi-homing mechanisms in mobile IPv6. These mechanisms require some modifications to the mobile IPv6 and/or application layer. Two possible approaches can be used as described in Figure IV-4

- Multiple CoA and single HoA.
- Multiple HoA and multiples CoA.

In the first approach, the management of multi-homing is based on the basic mobile IPv6 mechanisms to assign for each mobile node a reference " home address" in his home network, this HoA will be used to identify the MN by its correspondents. A mobile node with multiples interfaces can connect its interfaces to any foreign networks and getting multiple CoAs using IPv6 address autoconfiguration mechanisms. This approach requires the mobile IPv6 to extend home agent binding cache in order to support multiple bindings between the unique MN HoA and its different CoAs that identify the specific MN connections. The CoA registration process has also to be extended to properly register and deregister the different CoAs of the MN.
The principal drawback of such idea is that the HA is the only router in the network which is aware of a MN CoAs binding with HoA, it implies the realization within the home agent of all the functionalities concerning the mobile nodes filtering rules to properly handles IPv6 flows which are: 1) for download flows, filtering and forwarding each packets to the proper interface of the MN,

duplicate IPv6 packets for bicasting to the different interfaces 2) for uplink flows, merge duplicated packets sent by the MN in the case of bidirectional soft handover.
In the second approach, the multi-homing is no more based only on the standard mobile IPv6, the concept is deeply modified. Each MN can have more that one HoA, each HoA identifies one MN interface, and no more the entire mobile. According to this approach, each interface can be seen as an independent MN and a multihomed MN is a union of different simple MN. In this case, the multi-homed MN can require more than one home network and one home agent, and each one keeps a binding entry between one of MN HoAs and its corresponding CoA. According to this solution, the home agent needs no modification to its binding cache, but no single element in the network can be completely aware of the different interfaces of the MN. The specific multi-homing filtering, forwarding and duplication of flows to suitable interface must be defined at application or session layer.

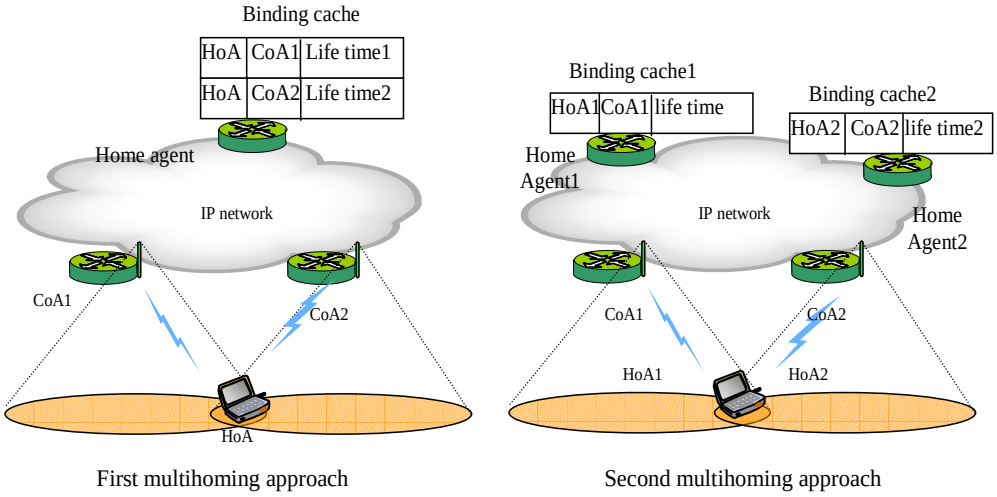


Figure IV-4 Multihoming design possibilities

2.3. Soft Handover Multihoming Design Requirement

In order to perform soft handover over heterogeneous radio access technologies in IPv6 layer, we need to manage MN multihoming in mobile IPv6, and considering that basic mobile IPv6 is not adapted to such as process. We need to design a solution to manage mobile IPv6 multihoming, which enables bidirectional mobile IPv6 flows duplication and merging from and through different MN interfaces.
Contrarily with existing solution described above, this solution should take into account the following basic requirements,

- The MN has to be able to register simultaneously different CoAs associated to its different physical interfaces;
- No major modification has to be done with existing mobile IPv6 protocol and home agent binding cache structure.
- The use of one or multiple interfaces simultaneously by the MN and their registration/deregistration should be transparent to existing home agent and correspondent nodes.
- Contrarily with second multihoming approach, IPv6 flow duplication, merging and redirection to appropriate interface have to be transparent to application and session layers.
- Contrarily with first multihoming approach, it is not realistic to perform mobile IPv6 binding update management and bidirectional flows duplication and merging for multiples MN in the same HA.

2.4. D&M Router for MIPv6 Multihoming and Soft-Handover Management

The key point of our multi-homing and soft handover signaling propositions is the use of existing basic mobile IPv6 mechanisms and structure. Moreover, we introduce one or more special routers named Duplication and merging agent (D&M) in the network. These routers interact with home agent and are responsible of mobile node multi-homing management and bidirectional IPv6 flow duplication, merging, redirection and resources management.

In our approach the MN is identified by a unique HoA in its home link, and multiples CoA are registered within the D&M agent. A binding entry is created between the home agent and D&M agent.

The D&M agent can be seen as special IPv6 router which acts as an intermediate home agent with special binding cache structure, and is responsible for duplicating and merging MN flow in soft handover. The access routers in the network are aware of the presence or not of any D&M agents in the network and theirs IPv6 addresses. When the MN moves to a foreign network, it will not be initially aware of the presence and the IPv6 addresses of D&M agents, so ARs will advertise using router advertisement mechanisms in addition to their IPv6 subnets, the IPv6 addresses for their corresponding D&M agents. When the MN with multiples interfaces receives a router advertisement as movement detection mechanisms, it can create its new CoAs for corresponding interfaces and register them within D&M agent. In case of multi-homing, the MN has three levels of IPv6 addresses:

- **Home Address (HoA):** the IPv6 reference address of the MN.
- **Primary Care of Address (PCoA):** the address given by D&M agent to identify the whole MN in case of multi-homing and soft handover, this address is used to hide the multi-homing to home agent, its considered as MN new The key point of our multi-homing and soft handover signaling propositions is the use of existing basic mobile IPv6 mechanisms and structure. Moreover, we introduce one or more special routers named Duplication and merging agent (D&M) in the network.

These routers will interact with home agent and are responsible of mobile node multi-homing management and bidirectional IPv6 flow duplication, merging, redirection and resources management.

- **Local care of addresses (LCoA):** the IPv6 care of addresses of each MN interfaces; they are registered only locally within D&M agent**.**

The figure IV-5 shows addresses management and hierarchy for multihomed mobile using mobile IPv6 with D&M agent extension.

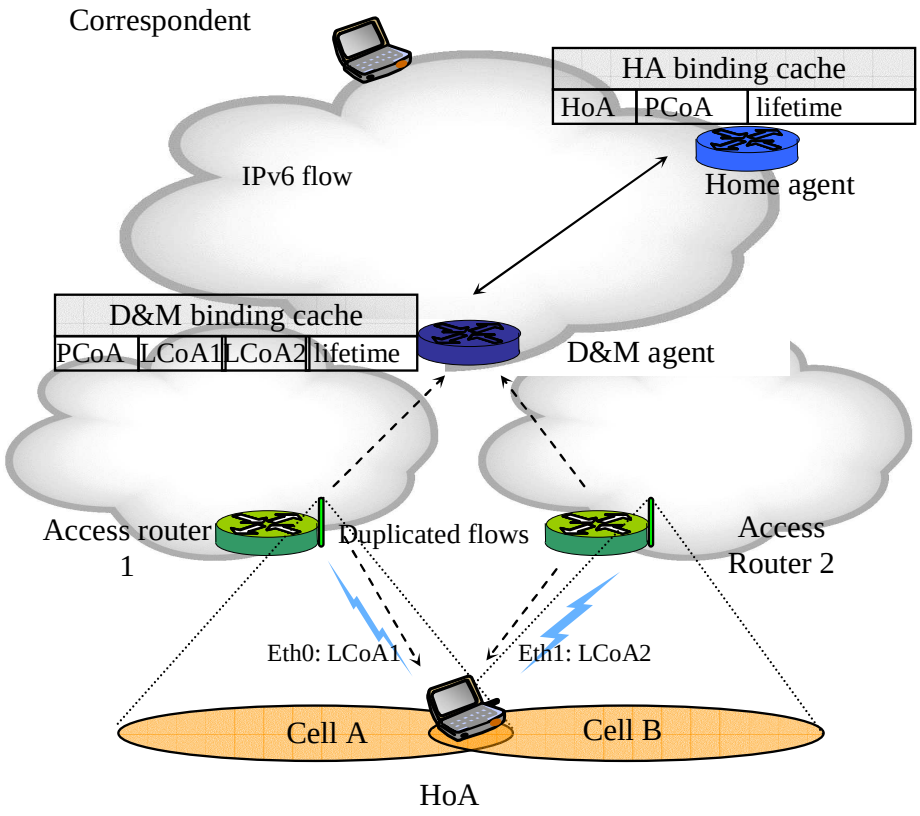


Figure IV-5 Multihomed-MN addresses management

2.5. Description of Registration and Signaling Procedure

Considering the described architecture, no modifications to the basic mobileIPv6 Home registration procedure are required; the only changes are in case of soft handover with multiples interfaces, it requires a MN specific multiples interface local registration request within D&M agent. In the following, we describe general signaling mechanisms in case of multiples interface registration for soft handover.

Basic mobile IPv6 signaling

- It is assumed at the beginning, the mobile node is connected to one access router through one interface with IPv6 HoA as reference address.
- We extend the movement detection to all MN physical interfaces. It can also obtain for each interface a distinct valid IPv6 CoA address using IPv6 stateless address autoconfiguration mechanism [31].
- When the MN is in foreign sub network using its first interface, it performs IPv6 basic handover procedure: it detects the movement, configures its new CoA namely Locale care of address (LCoA1) and sends a Binding Update message to the HA. The HA creates a binding entry in its binding cache, in this entry it registers the HA of the MN, the CoA and binding lifetime.

Soft handover multihoming registration

- When the MN decides to initiate a soft handover and establish simultaneously a second interface physical connection to start bidirectional bicasting, it extracts from the access routers advertisement the IPv6 addresses of the D&M agent.
- The MN then initiates its local registration within D&M agent; it gets a secondary CoA for this first interface from AR1. This is the *local Care of address* 2 (LCoA2), this address will be hidden to home agent.
- The MN generates a new message named *merging solicitation message*, its is a kind of local binding update with D&M agent, the format of this message will be described in next paragraph.
- The merging solicitation message is in the same time a local binding update and resource allocation request, the MN sends its LCoA1 and LCoA2 to the D&M agent address, in order to request a local registration, and necessary resources for bicasting, for a certain delay T.
- When the D&M agent receives this message, it decides whether it accepts or not the requests transmitted by MN. If the D&M agent accepts the request and it processes a merging acknowledgement message to the MN.
- It can be seen that the merging acknowledgment message defines, in addition to a period of validation of the binding entry, the particular *Primary care of address*. This address is an IPv6 address that defines the mobile in the D&M agent virtual network.
- First time, the MN receives the merging acknowledgement form D&M, it send a binding update to home agent and correspondent node with the PCoA as its new LCoA.
- The home agent updates MN binding entry in binding cache and the new MN binding will be (HoA → PCoA), as results all MN nodes destined packets will be sent to the D&M agent.
- The D&M agent incorporates a set of tables for flows management and addressing. The duplication control table handles multiple care of address association within a PCoA. This table define for each MN entry the primary care of address given by D&M, and the following information

- T: it defines the default time during which the entry should be kept within the duplication control table.
- X: being an integer used as current sequence number for the fast handover bicasting process.
- Local care-Of address1: it corresponds to the first mobile node interface ipv6 address
- Local care-Of address2: it corresponds to the second mobile node interface ipv6 address
- Local care-Of address3……

Figure **IV-6** is an example of duplication control table and home agent binding cache structures. The example illustrates two MNs, MN1 has two simultaneous connections and MN2 has three simultaneous connections to the core network.

Binding	*Home address*	*CoA*	*lifetime*
MN1	HoA1	PCoA1	Lf1
MN2	HoA2	PCoA2	Lf2

Home agent binding cache

Binding	*PCoA*	*LCoA*	*LCoA*	*LCoA*	*T*	*X*
MN1	PCoA1	LCoA1	LCoA2		Lifetime1	2356
MN2	PCoA2	LCoA4	LCoA5	LCoA6	Lifetime2	56

D&M agent duplication control table

Figure IV-6 Binding cache and DCT structures

- It should be noticed that the MN can establish one or more physical connections in the same time, by means of the same merging solicitation message; the mobile node can register one or more local Care-Of addresses using a single registration message.
- The MN can at any moment release a duplicated link by sending a merging solicitation message to the D&M agent with the desired LCoA of the link and with default life time set to (T=0). Thus, The D&M agent will delete the corresponding LCoA from the DCT.

- After performing first time MN registration within D&M agent and getting the PCoA, the MN will not more, perform binding update with home agent. To perform handover to a new access router with any interface, the MN detects the movement, creates its new IPv6 address using the unique interface IID and the new subnet address, finally it sends only MES with this new LCoA to the D&M agent.
- The MN has at any moment the possibility to stop using soft handover process, D&M agent services and back to basic mobileIPv6. To perform such a thing, the MN sends a binding update with the LCoA of its desired interface directly to both of home agent and CN to update their Binding cache entries and allow direct packets reception.

The Figure IV-7 depicts a mobile node multi-homing registration process for soft handover.

2.6. Signaling Messages for Mobile IPv6 Soft Handover

Basic mobile IPv6

For the purpose of mobile IPv6, and as described in the previous chapter, new destination option messages are defined. They carry The MN data, registration and signaling information to the correspondent nodes and the home agent. They are encoded in Type-Length-Value (TLV) format.
Home Address Option: this option carried by destination option, is used in packets sent by the MN while from home, to inform the correspondent of the mobile node home address.

Option Type "0xc9"	Opt Length "16"	Home Address "Unicast"

Binding Update (BU): this message is used by the MN to register its new care of address within the HA and CNs. The MN refers to the CoA as source address of the IPv6 packet, and uses the home address option to indicate its home address.
The MN can ask or not the correspondent to act as home agent or acknowledge the BU message.
Binding Acknowledgement (Back): This message is the answer of CNs or HA to the BU messages sent by the MN. In this message they can accept or reject the MN registration request. When accepted, they answer with the granted lifetime, for which they retain the entry of the MN in their binding caches.
Binding Request (BR): this destination option is issued by a fixed node to request the MN to issue a BU, in order to update its entry in the fixed node binding cache.

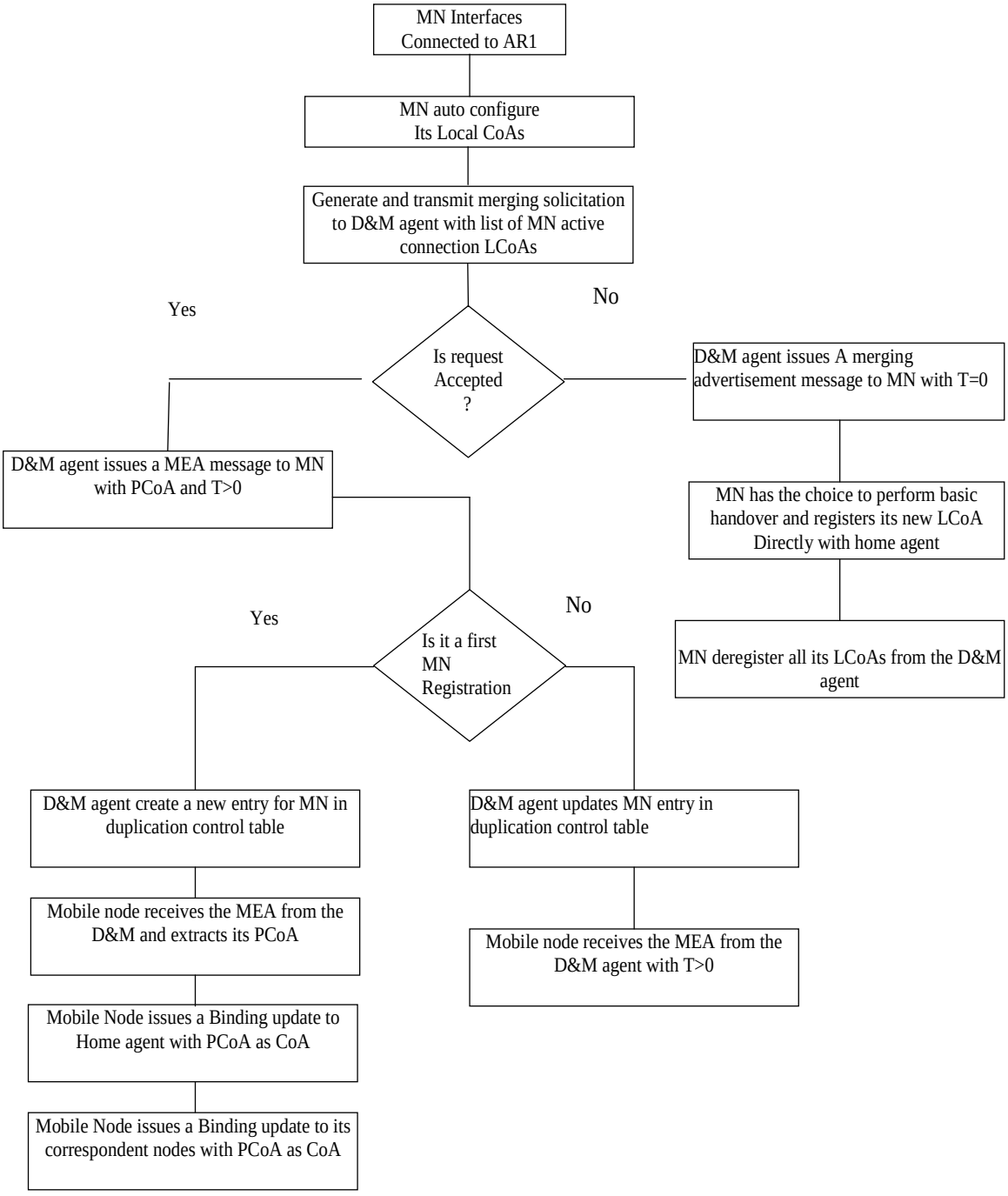


Figure IV-7 Soft handover registration process

Additional soft handover messages

For the registration with D&M agent while performing soft handover within its covered domain, a merging solicitation and merging advertisement messages are issued by the MN, as discussed in the previous chapter. To perform this registration process, we define new message option namely merging option as described in Figure V-8. Two types of merging option will be used:

- Merging solicitation: generated by the MN to request the registration or deregistration of one or more interfaces
- Merging advertisement: issued by the D&M agent to acknowledge or denied the MN merging request.

Merging option generic fields

- option type (8 bits) (to be defined)
- option length (8 bits)
- P (1 bit): number of primary CoA field
- I (1 bit): if set, the Initial Identification field is relevant
- Local CoA Length (6 bits): number of Local CoA fields
- Initial Identification (24 bits): initial identification number for the data merging mechanism
- lifetime (32 bits): number of seconds before a merging link must be considered expired
- Primary CoA (128 bits): defined by the merging agent
- Local CoA (128 bits): defined by the mobile node
- Sub options ($n \times 32$ bits where $n \geq 0$): QoS specification, traffic profile specification, etc...

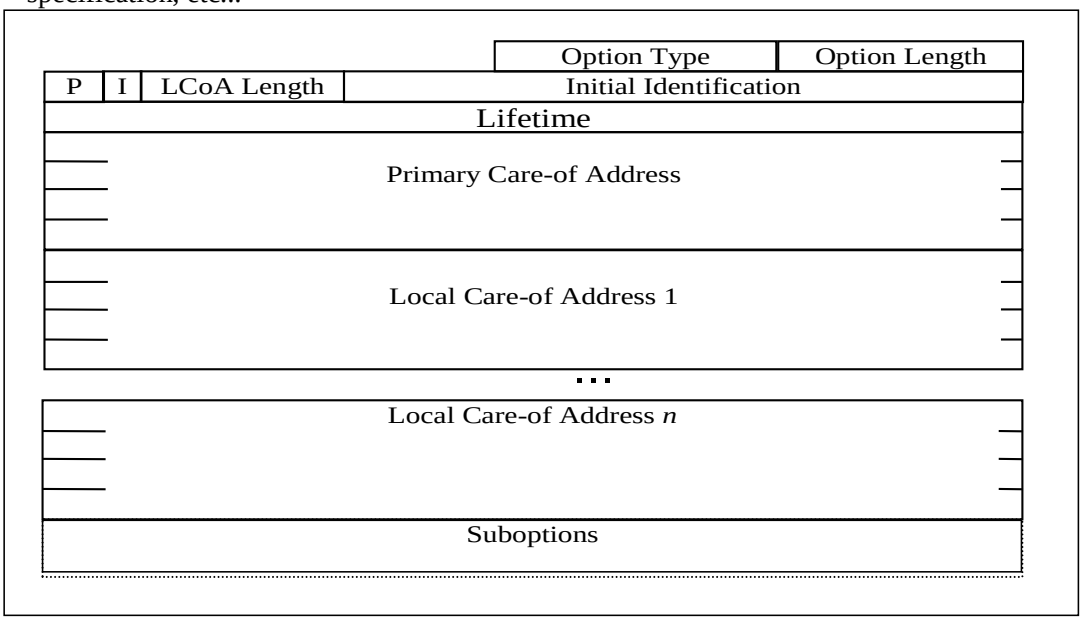


Figure IV-8 Multihoming registration message: Merging option signaling message

3. IPv6 Flows Duplication Process

When the mobile node is in overlapping region, and if both radio links, from the old and new access router, have weak signal strength. The MN can use its interfaces diversity and became multi-homed using the registration process depicted in the previous chapter. When the wireless part of communication between the CNs and the MN involved more than one access point, the bicasting and duplication of the same data through different access points to MN different interfaces can offer soft handover and improve the overall quality of radio communication between the MN and the core network. The registration process allows the MN to use mobile IPv6 and gets multiples care of address for its different interfaces and registers them within the D&M agent.

3.1. Downlink Duplication Process

When the MN exploits soft handover registration process with mobile IPv6 basic process, a new CN that communicates with the MN uses the MN HoA as destination address to send packets. The packets routing scheme depends on the MN position, situation and the number of its simultaneous connection to the network. The main cases are MN in home and MN running outside

MN is in its Home network: In this case the MN has not to perform any registration process within the home agent. Hence, there is no MN corresponding in binding cache, the home agent will route packet normally to MN HoA.

MN is in foreign network using only one active interface: When the MN is in the foreign network using a single interface, its gets as described above, a CoA, and the MN can decide to register this address, either within the D&M agent and home agent or only with the home agent.

- Registration directly within the HA. The home agent intercepts all packets sent to the MN HoA, looks of the corresponding entry in its binding cache, the HA then, tunnels the packets [34] to the MN current network.
- Local registration with the D&M agent. In this situation, the MN has two binding entries. The first one located in the HA binds the MN HoA with its PCoA. The second entry located in the D&M agent duplication control table binds the PCoA with the MN local CoAs. Therefore all MN destined packets are routed form the correspondent node to the home agent, which intercepts them and forwards them in an IPv6 tunnel to the PCoA. The D&M agent intercepts these tunneled packets, decapsulates them and extracts the MN LCoA from its duplication and merging table. The D&M agent encapsulate the packets in another IPv6 tunnel, to the LCoA.

MN is in foreign sub network in soft handover mode: The first step of IPv6 data packets routing scheme, between MN and D&M agent, is similar to the one described previously for a single active interface. However, as soon as the D&M intercepts the packets sent to the MN PCoA. The process changes and D&M agent applies the duplication process to all packets sent to the multi-homed MN. In following the process is summarized, the HA intercepts all packets sent to the MN HoA and forwards them the PCoA located in the D&M network, if the MN is in soft handover state, the D&M agent intercepts all packets sent by the CN

and stores them in its internal memory, extracts the destination address (PCoA) from each packet and looks for its corresponding LCoAs in the DCT table. Using these LCoAs, the D&M agent creates a new IPv6 packet with same payload information, but with substitute LCoA as new destination address. Additional sequence number (X) is inserted in a Destination Identifier Option (DIO) field and added to each IPv6 packets header before duplication. This field is used to stamp all duplicated packets sent tunneled in direction to MN. The same duplicated packets will be identified by the same sender, the same receiver and the same sequence number. The new option header namely data Identification Option (DIO) used to carry the identification information has followed structure:

- option type (8 bits) (to be defined)
- option length (8 bits)
- identification (32 bits):
    - Sequence number for packet Identification
    - Incremented by one for each new packet sent
    - Two or more duplicated packet have the same sequence number

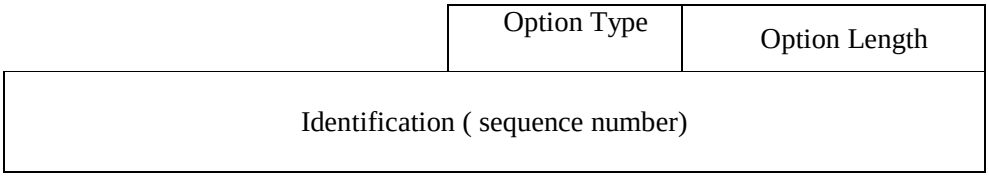


Figure IV-9 Data identification option

The Figure IV-10 shows an IPv6 packet structure format after the insertion of the DIO and IPv6 tunnel header.

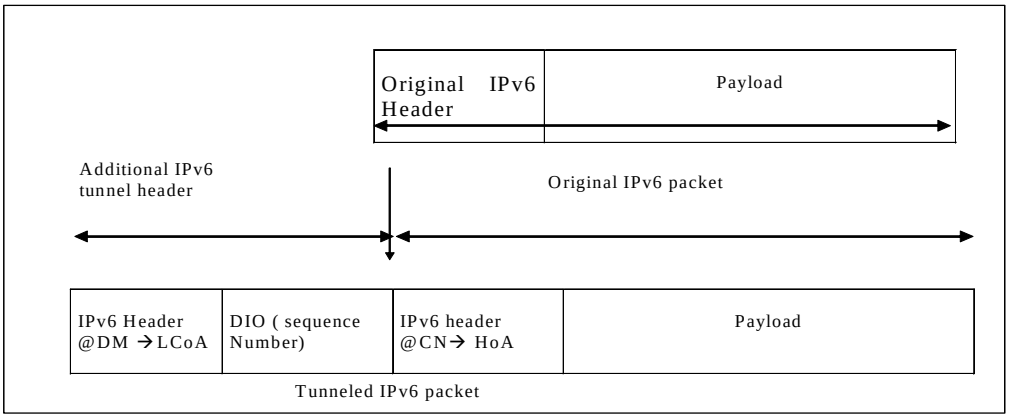


Figure IV-10 Packet format in the tunnel between D&M agent and the MN

The duplication process and the insertion of an identifier in IPv6 packets allows detecting duplicated packets at the reception and the introducing of a path diversity of packet reception to income the handover process and signals degradation in the overlapping regions. This path diversity allows to:

- Have two chances or more to receive a packet correctly at IP layer.
- Reduce jitters and end-to-end transmission delays as 1st duplicated received packet will be accepted and 2nd packet will be destroyed. The packet choice is independent of path the reception interface.
- Reduce the probability to loose a packet. If "P1" is the probability of packet loss through the first path and P2 in the second path the new probability will be P = P1*P2. (P<p1 and P<P2)

In the next chapter we will depict the way to exploit the DIO by the merging process to filter duplicated packets to upper layers. The Figure IV-11 shows the downlink IPv6 packet format and binding entries in case of MN soft handover duplication process based in D&M agent.

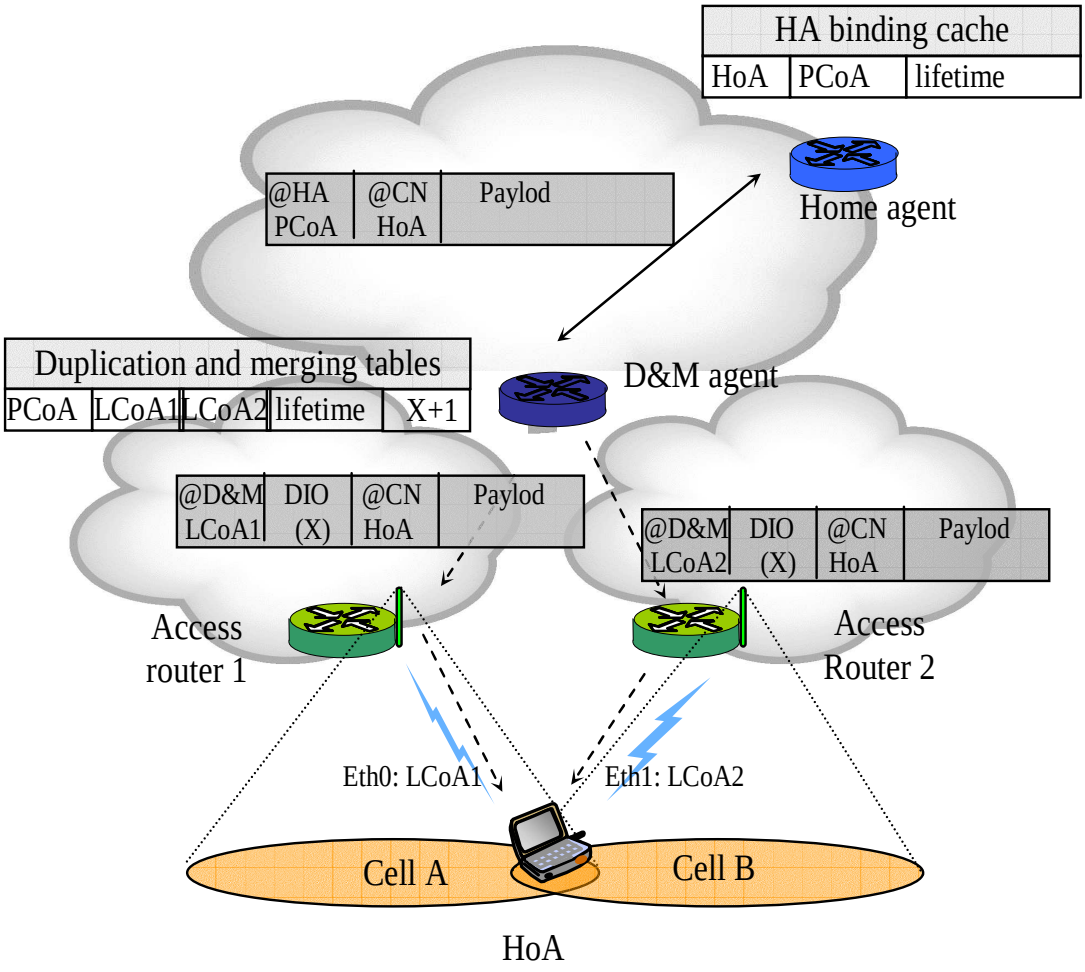


Figure IV-11 Soft handover data structures in the network

In following, we describe the complete downlink duplication process algorithm.

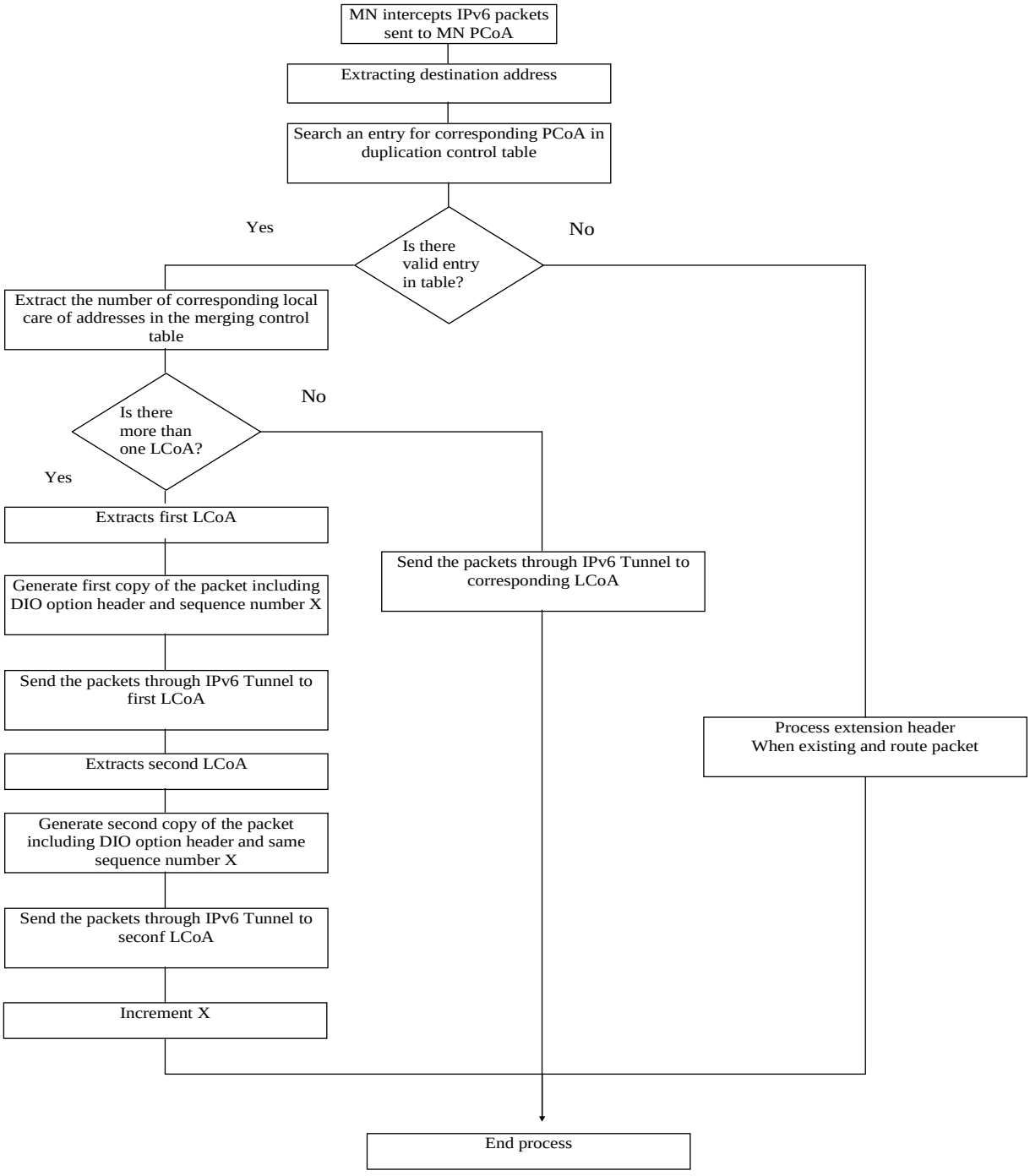


Figure IV-12 Downlink duplication process in D&M agent

3.2. Uplink Duplication Process

In order to improve the quality of service in bidirectional flows, the MN exploits the packets path diversity in the uplink flows. The duplication process is quite similar and is described in following:

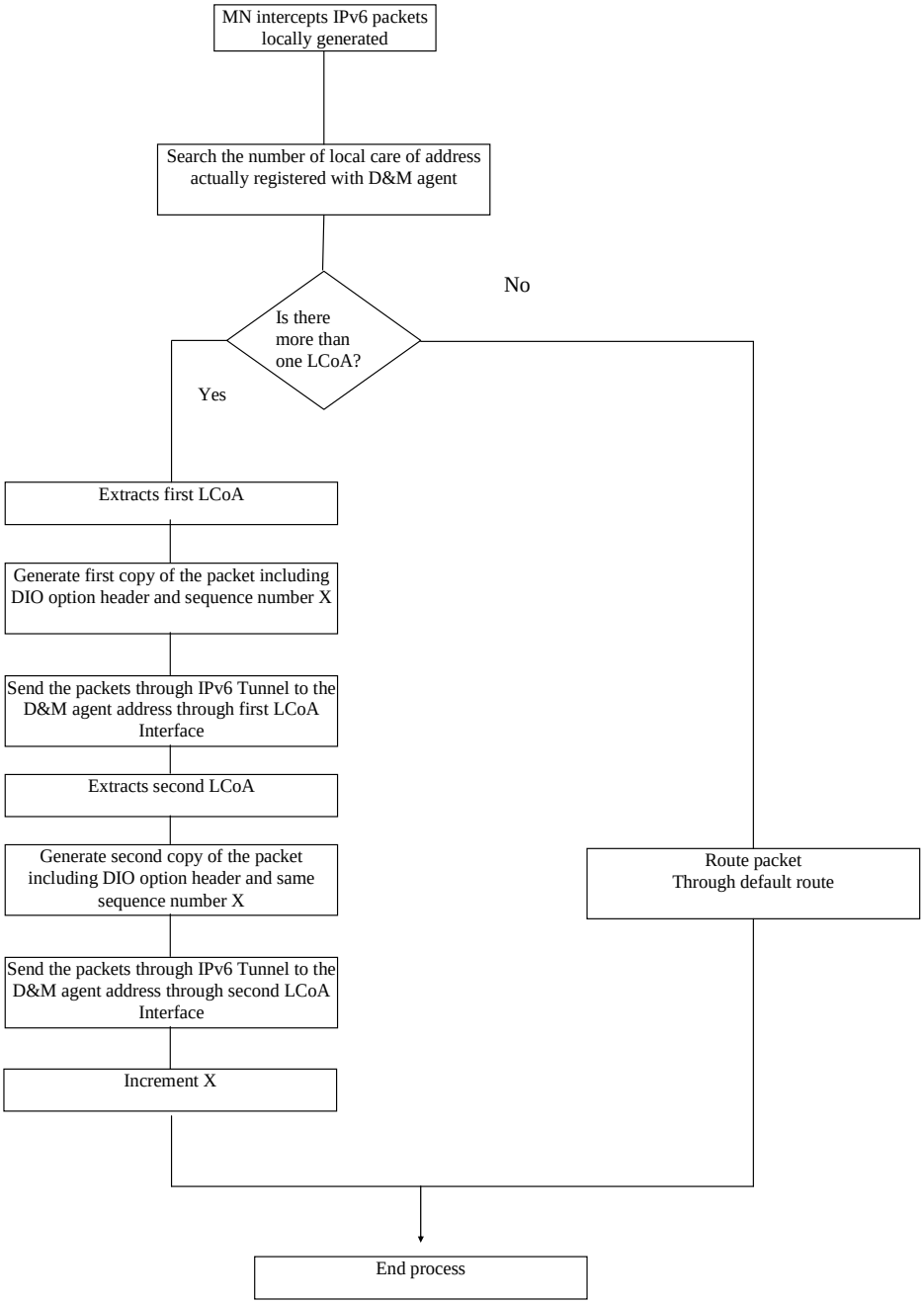


Figure IV-13 Uplink duplication process in mobile node

The main differences between downlink and uplink duplication process are:

1. For downloading, the D&M has no to duplicate downlink packets, which are not generated locally but only intercepted packets. For downlink the MN detects the soft handover state and duplicates packet generated locally before applying routing mechanisms
2. In order to ensure the path diversity, the D&M agent can forward duplicated packet throw unique interface but with different IP access routers as intermediate destinations. The MN tunnels duplicated packets to the same destination address which is the D&M agent address, but the forwarding mechanism ensures that the packets are forwarded through different interfaces to guarantee the uplink radio transmission diversity.

4. IPv6 Flows Merging Process

In order to exploit the MN multi-homing and IPv6 packets duplication and redundancy, with guarantee of transparency regarding the transport and application layer; we need to imagine flexible IPv6 packets merging mechanisms at reception. This mechanism is implemented on the MN to merge downlink duplicated flows, and in D&M agent to filter uplink duplicated packets. The use of D&M agent (respectively MN) duplication process to send separate copies of the same data via multiple ARs to the MN (respectively D&M agent), introduces the need to filter out the duplicated packets. To efficiently perform such process, the MN or D&M agent needs to match these multiple streams in IP layer upon reception.

In case of downlink flows, the MN receives duplicated packets through IPv6 interfaces, for each packet it applies the same process:

- The MN check the extension header of the received packets
- It Checks, than, if the special option header “DIO” is included in the IP packet.
- If there is no option header or no DIO information in the packet header, that is mean that the IP packet was not duplicated. The IPv6 routing mechanisms will process the packet normally and will route the carried payload information to the upper layer.
- The D&M agent and MN incorporate special tables to store the necessary information to merge packet namely merging control table (MCT). The D&M agent and MN table are not similar:
- The MN MCT table defines, for each associated D&M agent:
    - “e” corresponding to the expected value being awaited. It is the integer which is immediately superior to the higher value of the sequence number “X” of received packet.
    - List of sequence number “Xi” corresponding to packets which are been transmitted by the correspondent bode, but which are not yet received yet. This table therefore registers the list of value of sequence number “Xi” which correspond the packets which are still missing

The Figure IV-14 depicts structures of “Merging Control Tables” located in the MN and D&M agent

Address Of D&M agent	*e*	*Expected Value x1*	*Expected Value x2*	*Expected Value x3 Expected Value x4*	*….*

Downlink merging control table in the MN

List of MN LCoAs	*E*	*Expected Value x1*	*Expected Value x2*	*Expected Value x3 Expected Value x4*	*…*

Uplink merging control table in the D&M agent

Figure IV-14 Merging Control Table structures

- If an entry corresponds to the source address and the DIO exist, the parameter X within the DIO is read, and a test is performed to determine whether this value is inferior to the expected value “e” of the merging table.
- If the value X is superior to the expected value “e”, the packet is routed to upper layer. Intermediate values between the expected number and the value of X are inserted within the merging table as corresponding to the new missing packets. The value of “e” is set to “X +1” and stroked as the next expected IPv6 packet identifier.
- Otherwise, if the value “X” is included within the “Xi” value in corresponding MCT entry, this means that the received packet corresponds to one packet which is still missing. The packet is processed normally and the current value of “X” is suppressed from the MCT entry.
- If DIO is included in the received packet, the source-address has an entry in the MCT table and the value Xi is not expected. This IP packet will be simply discarded.

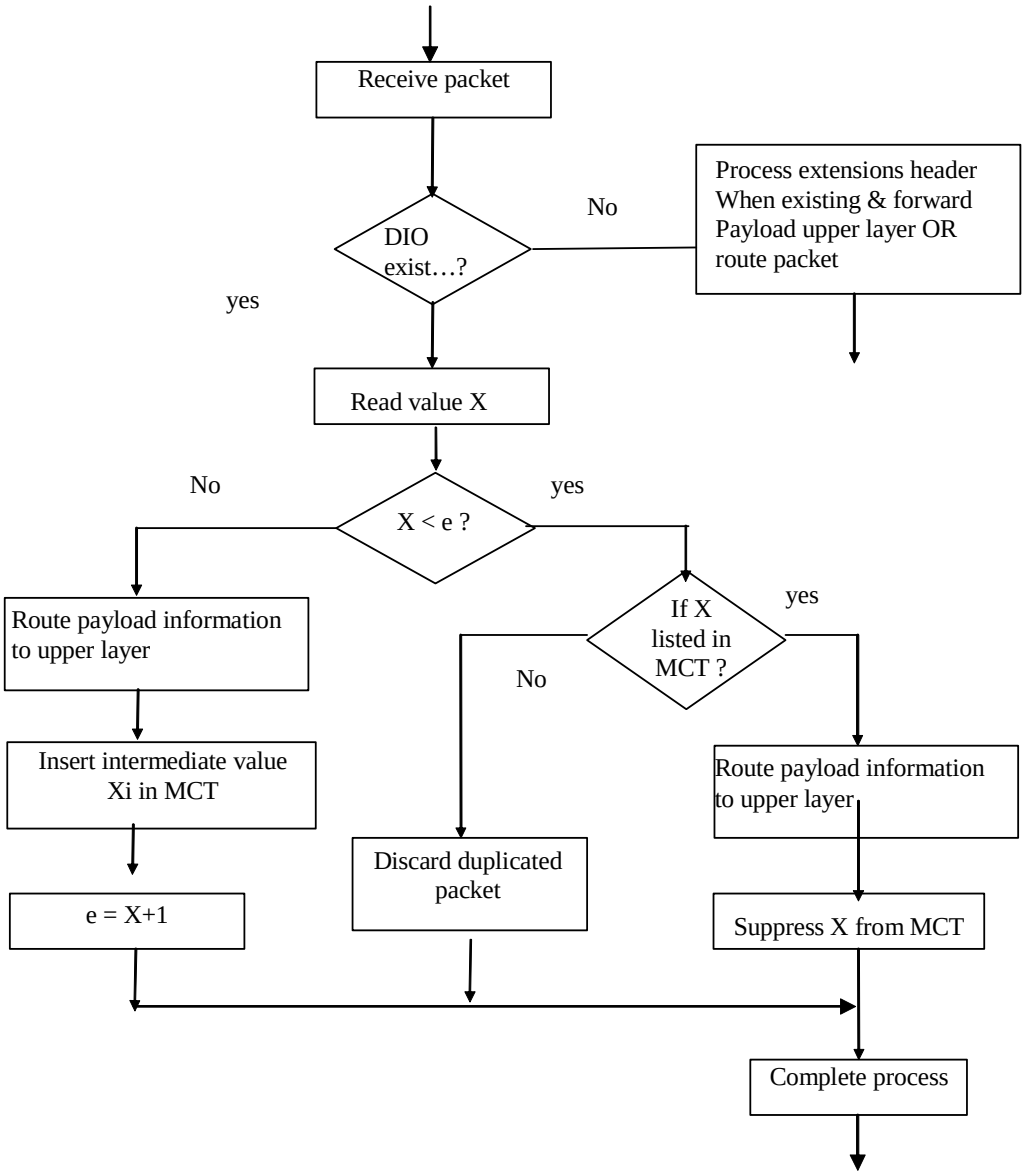


Figure IV-15 IPv6 flow merging algorithm

5. Handover Process

We consider a MN with two interfaces primary and secondary. The interface priority choice is dynamic; we assume that primary interface is always the interface with the best connection quality. The MN must be kept connected to the network through its primary interface. The secondary interface is used to allow multihoming, seamless soft handover and allow path diversity to avoid severe signal strength degradation. The aim of this handover initiation and management strategy is to efficiently exploit all available resources in order to improve the QoS, avoid packets loss and the introduction of additional end-to-end delay during MN roaming from an AR to another one. Two signal strength thresholds are defined. Handover threshold (H_SH), is the basic threshold used in mobile IPv6 to initiate the handover. Primary threshold (P_SH) is used in soft handover to initiate the secondary interface connection process, as shown in Figure IV-16.

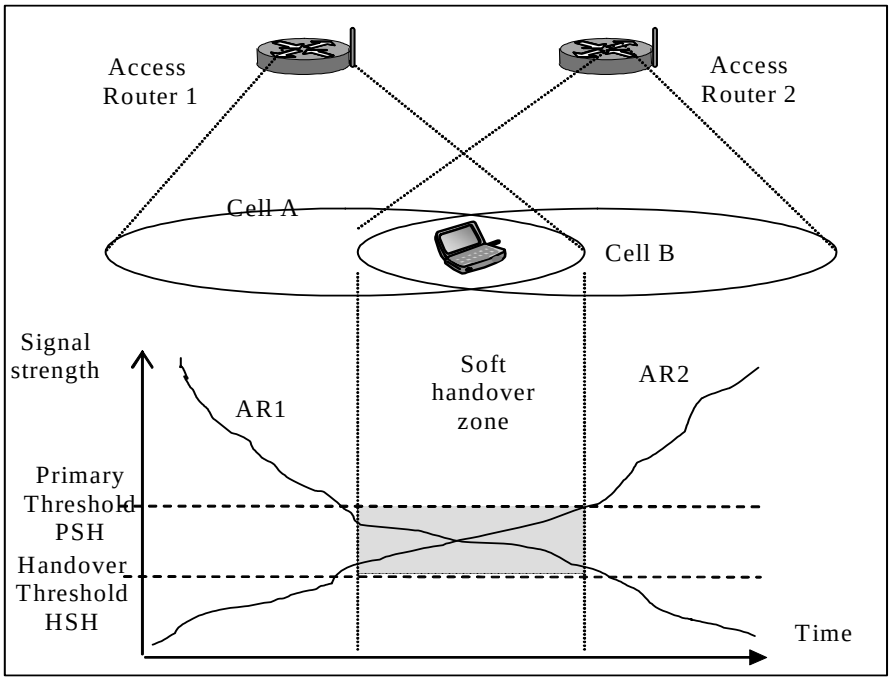


Figure IV-16 Soft handover thresholds

We assume that a MN is connected on its primary interface with AR1, it has its PCoA and LCoA1, and both of them are registered within the D&M agent. When MN discovers AR2, and if the quality of the primary connection is less then P_SH, the secondary interface connection is established with AR2, LCoA2 is registered within D&M, and duplication and merging process will be UP. In this case:

- The interface with better connection quality will be assigned dynamically to be the primary one.

- If the signal strength of the secondary connection becomes worse than H_SH, the secondary connection is closed and active scanning is initiated to connect it to a new AR.
- When the Signal strength quality became better than H_SH (very good connection quality), the MN closes the secondary connection, shut down duplication and merging processes. The Complete handover algorithm is described in Figure IV-17.

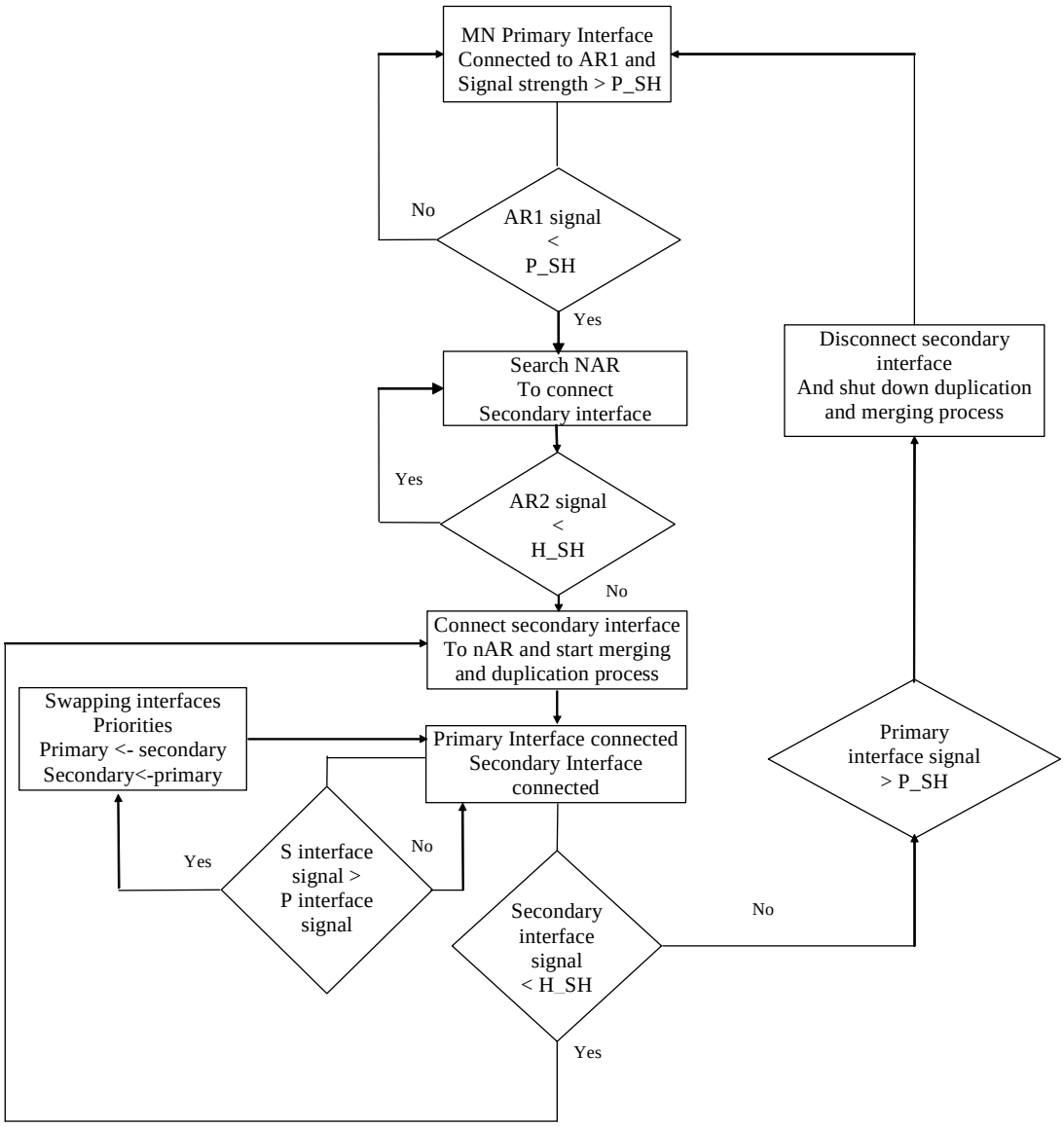


Figure IV-17 Handover process

6. Soft Handover Analysis

From Figure IV-18 showing the temporal diagram of soft handover process, we distinguish three main steps of handover. In the first step the MN has only one physical connection to the network through its old access router (oAR). The second step starts when the MN establishes a second connection to the network through the new access router (nAR). During this soft handover period the MN receive duplicated data-flow through to the two ARs simultaneously. Finally, the third step begins as soon as the MN releases its connection with the oAR.

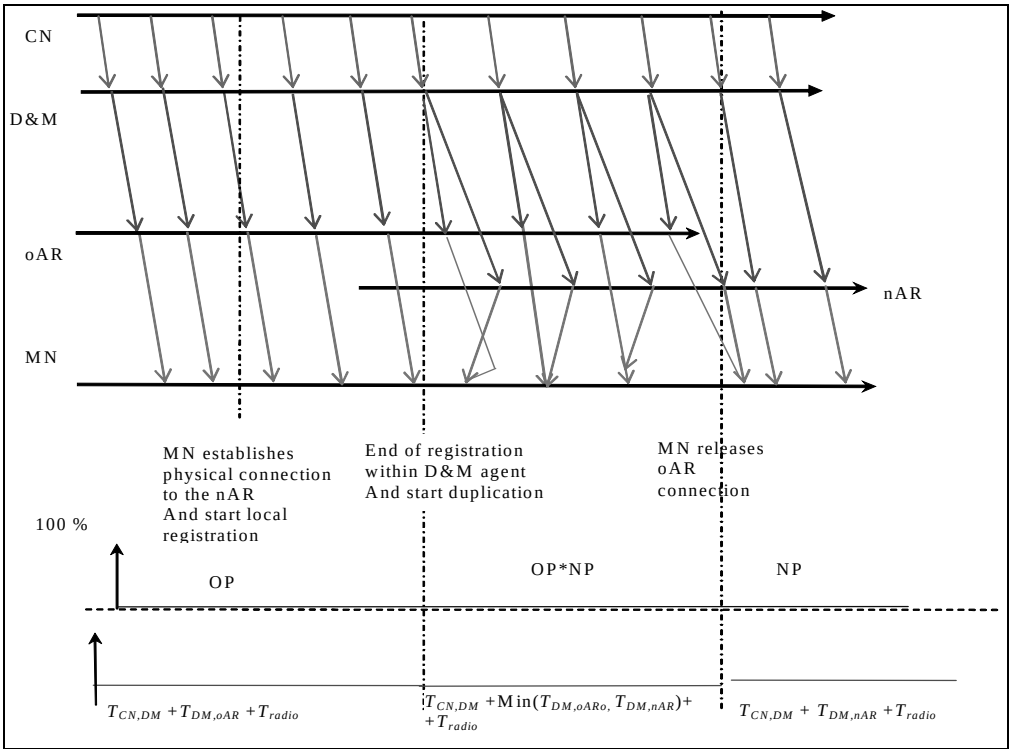


Figure IV-18 Soft handover temporal diagram

During the first step, the end to end transmission delay can be given by,

$$T_{soft} = T_{CN,DM} + T_{DM,oAR} + T_{radio}$$

In the second step, it becomes

$$T_{soft} = \min(T_{DM,oAR} + T_{DM,nAR}) + T_{CN,DM} + T_{radio}$$

Finally, in the third step

$$T_{soft} = T_{CN,DM} + T_{DM,nAR} + T_{radio}$$

Note that during the second step of handover process, the end to end transmission delay is optimal. It is the minimum delay between the end to end transmission delays of duplicated packets through the two paths. If the wireline transmission error rate between the MN and ARs is considered as negligible the overall packet erroneous transmission probability can be given by

$$P_{soft} = oP.nP$$

With "oP" is the probability of erroneous transmission through the oAR, and "nP" is the erroneous transmission probability through nAR. The path diversity and flow redundancy allows to considerably decreasing the overall probability of packet transmission errors. Not that using soft handover, the MN is always connected to the network, so the number of packet loss as direct consequence of handover is

$$N_{soft} = 0$$

Finally the following data loss comparison between soft handover and others IP-based handover approaches can be given,

$$0 = N_{soft} \leq N_{smth} < N_{fast} < N_{HMIP} < N_{MIP6}$$

7. Conclusion

In this chapter, we introduced a set of control and data management mechanisms to extend mobile IPv6 with multihoming and soft handover support. The future deployment of an all-IP wireless and wireline networks, will push the mobile users towards more access to various IP based multimedia traffic. Regarding the IP based multimedia traffic quality of services requirements compared to voice traffic, new service and communication continuity parameters might be expressed in terms of no data loss, minimal, stable and uniform information transmission delays.

For the purpose of such environment, we presented a set of new mechanisms in IPv6 layer that interoperate with mobile IPv6. The aim of this work is to integrate universal soft handover management in IP-based networks, which provides a better Quality of services (QoS) support of data communication regardless of the heterogeneity of wireless access technologies. This solution enables the reception and the emission of duplicated IPv6 flows by the MN from two or more access routers (AR) simultaneously. By merging these flows in IP layer at reception, the MN can simultaneously

- Avoid connection disruption, packets loss and transmission jitters introduced by wireless radio signal degradation.
- Allows MN's session to progress without interruption when it moves from one radio cell to another regardless of its radio technology.

To realize such promising approach in mobile IPv6 protocol, a set of challenges, in both control plane and data plane, have been identified and appropriate solutions were proposed. According to this idea, mobile IPv6 soft handover new mechanisms are split into two main parts regarding their locations, the IPv6 core network components and MN components.

The "Duplication & Merging Agent" (D&M) concept is introduced in the IPv6 network. It is a conventional IPv6 router located at the core network. The control plane in D&M agent manages MN multihoming and soft handover signaling. The data plane duplicates and merges IPv6 flows to-and-from the MN. The main goal of this component is to hide the MN multihoming addressing management and data duplication and merging to the basic mobile IPv6 protocol. The soft handover mechanisms located in MN manage multi-interfaces Dynamic priorities, simultaneous connection, default routes and handover signaling. The data plane is in charge of bidirectional IPv6 flow duplication and merging to and from the network.

The soft handover in IPv6 as proposed in this chapter is constructed using a set of different and elementary mechanisms. These mechanism are not exclusively designed for the purpose of soft handover, they can be used within other approaches to propose solutions to a set of mobile IPv6 basic open issues such as flow redirection and multihoming management, other end-to-end QoS mechanisms…etc.

In the same way, the soft handover approach stills a general and open proposition. It can be combined with other IPv6 based handover approaches as Hierarchical and fast handover. In the Chapter 6, hierarchical D&M agent architecture in the core of the network is proposed. The aim of this solution is to reduce to overall duplicated packets and signaling overhead in the network. In the next chapter, we will study the performance of mobile IPv6 soft handover in a packet level simulator. We aim to provide a first and full implementation of described mechanisms to evaluate soft handover performances under different movement and traffic scenarios. We than compare its performance to other IPv6-based handover mechanisms.

CHAPTER 5

V. Simulation Results and Performances Analysis

In previous chapter, we have introduced our propositions: Mobile IPv6 transparent multihoming management by the means of the D&M agent and the extension of mobile IPv6 with universal soft handover mechanisms. In this chapter we evaluate the performance of soft handover through detailed packet level simulation under a home made network simulator "Gemini2" to have a closer observation on this approach. This simulation work on mobile IPv6 soft handover over IEEE802.11b radio access technology contains two goals, testing the feasibility and the interoperability of the different proposed mechanisms with basic mobile IPv6: the introduction of D&M agent, the management of mobile node with multiples 802.11 interfaces at IP layer and the simultaneous reception and emission of IP packets by then MN. The second goal of our simulations is to examine the soft handover end-to-end performances on UDP sessions and to compare them with called mobile IPv6 basic handover and another IETF Bicasting approach which is Fast handover Bicasting. In particular, this simulation process investigates the packet loss ratio, end-to–end transmissions delays, UDP reception throughput disruption and layer 3 control load information as a direct result of:

- The Signal degradation when the MN moves towards the borders of access routers coverage areas.
- The MN handover through our simulation network topology.

The rest of this chapter is organized as follow. Section 1 introduces simulation environment and Gemini2 simulator followed by section 2 in which we present the handover performance metrics that will be used in the simulation. In section 3 we present the simulation scenarios. Section 4 evaluates the performance of soft handover and section 5 evaluates and compares the performance of Fast handover bicasting, soft handover and mobile IPv6 basic handover. Finally, section 6 concludes this chapter.

1. Simulation environment

Gemini2 as NS-2 network simulator [93] or Opnet [94], is an open-source GNU simulation tool that runs on Solaris [95] and Linux [79]. It is a discreet event simulator developed in Eurecom. Gemini2 provides support for simple, open and efficient conception of a network topology to simulate complete wireless and wireline networks architecture and protocols validation and evaluation. The goal of our simulator is to simulate an IPv6 network with its different entities: IP routers Fixed nodes, special servers, access routers with ethernet and wireless interfaces, mobile nodes with one or multiples interfaces and with movement capabilities. Using all these components and connection medium we aim to simulate mobile IPv6 protocol (signaling and data transmission), with support of soft and fast handover bicasting. Finally, in order to evaluate the gain of the duplication and merging mechanisms in the wireless connection in overlapped border areas, we implement an accurate "IEEE802.11b" propagation model for the wireless interfaces.

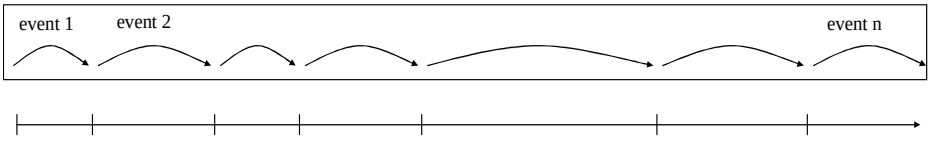
Gemini2 is a simple and efficient tool to simulate:

- Network topology: (with nodes: station, router, bridge, etc…and links: Ethernet bus, point-to-point link, radio, etc...)
- Node architecture:(logical layer: IP, UDP, etc…and hardware card : Ethernet, IEEE802.11b)
- Message structure: ("physical" message: UDP segment, IP datagram, Mac frame, etc…)
- Signal: irq, primitives.

To perform such things, our simulator is based on set of basic components, schedule, message, box and probe.

Scheduler

The modeled scheme in Gemini2 changes its state at discrete points in simulation time, as described in following figure:



The scheme state, which can be for example a network stat with mobile movement and packet load, can only be modified upon reception of an event by the scheduler. An event is identified by a time stamp indicating when that event occurs and its nature (e.g., reception of a packet, expiration of a timer, mobile movement…etc).

When an event occurs, the scheme state may be modified, and this introduce new events, these events will be store in an ordered event list namely scheduler. The basic actions of scheduler algorithm are

- Extract the event with the corresponding smallest timestamp
- Process the event
  - modify the scheme state
  - or insert new elements in the scheduler

    - or extract some elements of the scheduler
    - or do nothing
- If the scheduler is not empty, return to the begin

Box

The box is the basic and "atomic" structure of Gemini2 simulator, any station, mobile, router, access medium or protocol layer is constructed using boxes. Each box can inherit from other boxes and has a number of input and output to be connected and communicate with other boxes in order to construct a complex structure. For each box there are three primitives and important methods:

- *Receive* (Messages *msg, IO inp), which is a method processed by the scheduler when the box receive a message msg from the input number port inp (if defined).
- *Send Messaged* (msg, opn, t), this method send the message msg to the box output port number opn, and the receiver will receive the message after the period "t". Concretely, insert a new event in the scheduler.
- *Attach_o* (Box *b,"IO" onp), this method allows any box to attach itself to the box "b" o. The link will be unidirectional and its entry will be in the output point identified by "onp".

Messages

Information that any box can send to another attached box through the link, this information can be a physical message (IP datagram or Mac frame) or it can be a signal (irq, primitives).

Probe

Probes are information that we can insert in packets or nodes, they allows us to follows these components and get back simulations results.

Gemini2 main Classes

In following figure we describe the hierarchy of major Gemini2 classes useful to create network node, protocols and mobile using different medium technologies and handovers approaches.

- Medium class: in this class we describe necessary methods and elements necessary to models Ethernet and wireless medium. The wireless mediums we simulate IEEE802.11b (11Mb/s) (radio interface 802.11 DSSS at 2.4 GHz lucent Orinoco).[36]
- Mac class : this class describe Ethernet and 802.11 Mac layer
- IPv6 class : Internet protocol Version 6, protocol routing and tunneling mechanisms are described in this class
- ICMP6 class: ICMP6 messages, mechanisms ,router advertisement, and ping6 use the primitives defined in this class
- Transport Class: UDP protocol mechanisms
- Application class: in this class we define the Sink (reception) and process (emission) applications than can be used on the Top of each IPv6 node to send and receive data packets with fixed size and throughput. The emission process can be exponential or constant bit rate
- Script Class: methods defined in this class are used to parse simulation script files, create the simulator components, initiate the process and define MN movement. Script files are used to define probe in order to collect performances information.

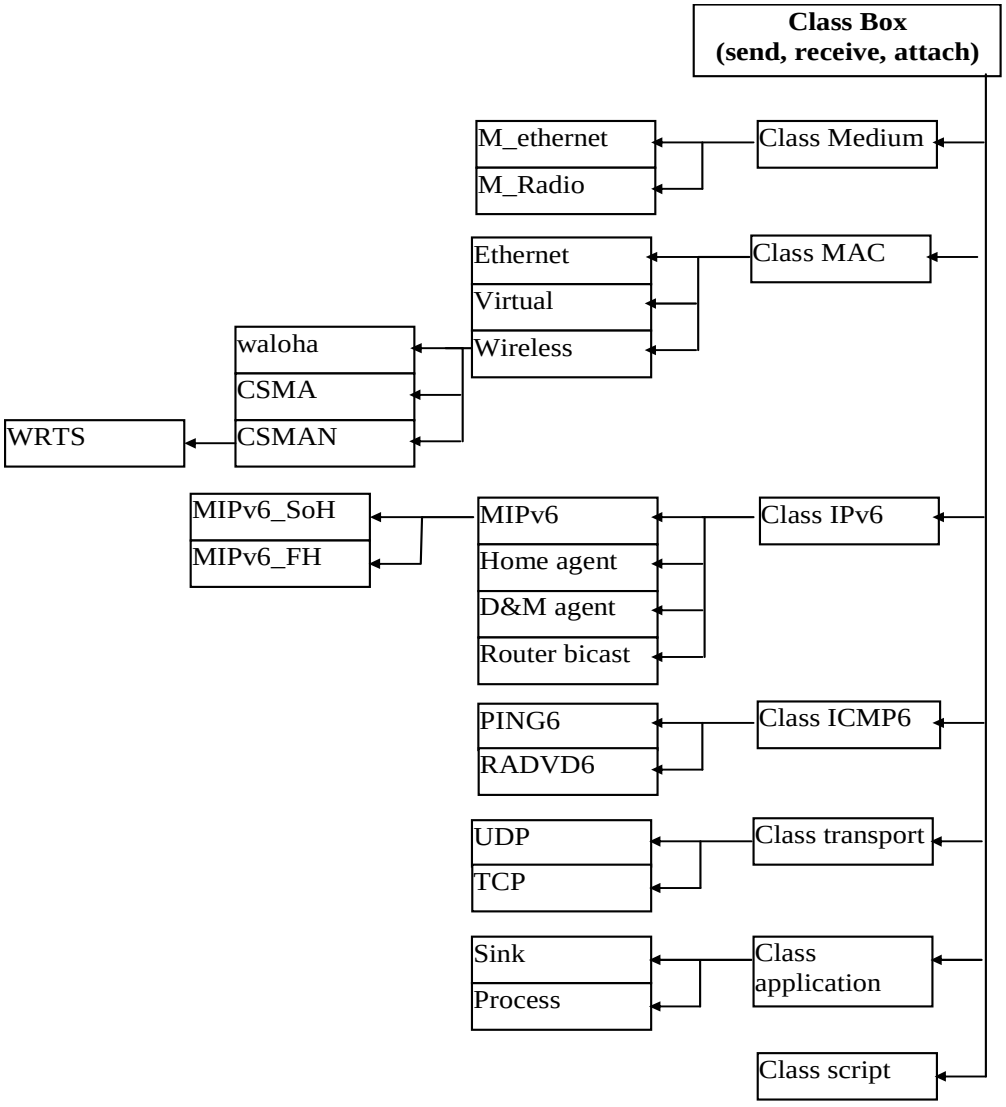
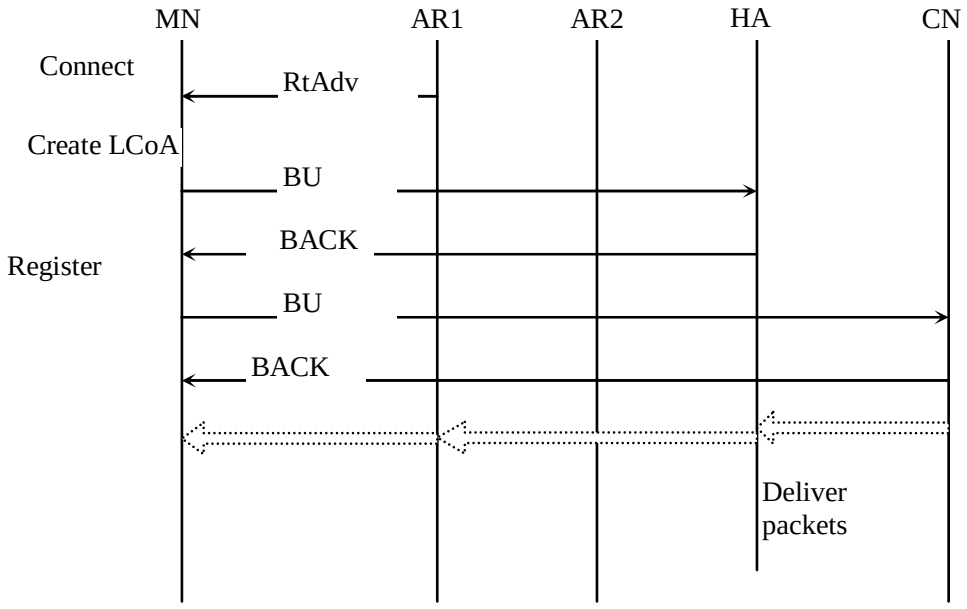


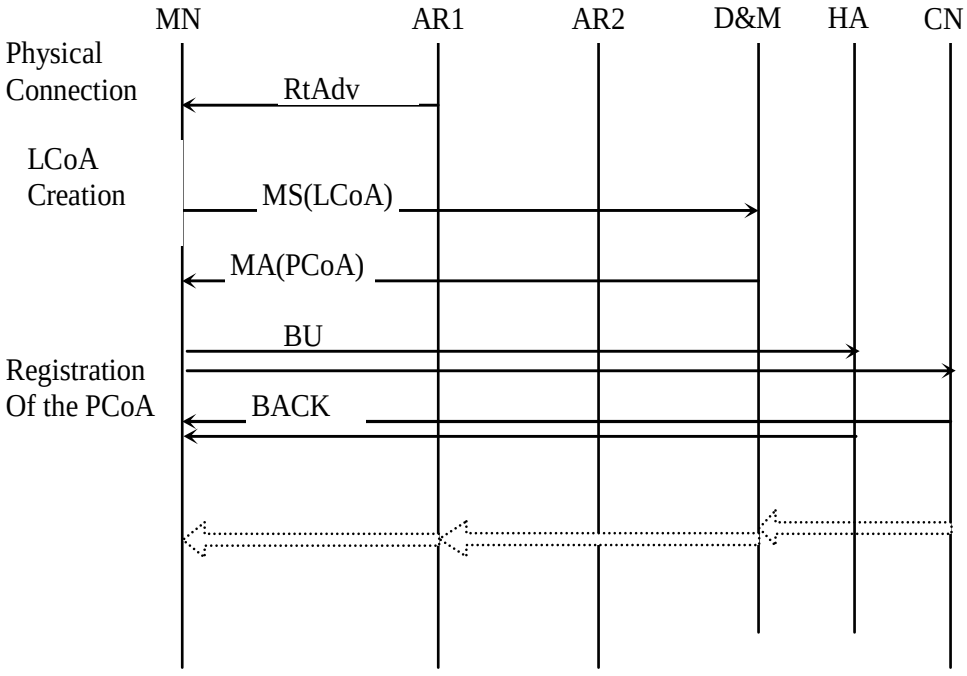
Figure V-1 Main classes used in gemini2

Finally, for the purpose of this dissertation, in gemini2, we implement process to create a MN in specific space coordinate. Each mobile support basic mobile IPv6, and can have one or more interfaces (IEEE802.11b). The box mobile IPv6 box provides all mobile IP signaling mechanisms. To this box we can attach soft handover mechanisms that exploit the multiples interface to provide soft handover support to our mobile. As consequences of MN movement with fixed speed described in simulation script, and the degradation of signal strength, the MN performs handover to keep itself attach to the network. The signaling process of mobile IPv6 and soft handover approaches as modeled in Gemini2 simulator are depicted in following figures. The Figure V-2 depicts the signaling mechanisms to establish and register a first connection to the network

through AR1. The Figure V-3 shows the signaling process to perform a basic and soft handover from AR1 to AR2 as done in Gemini2.

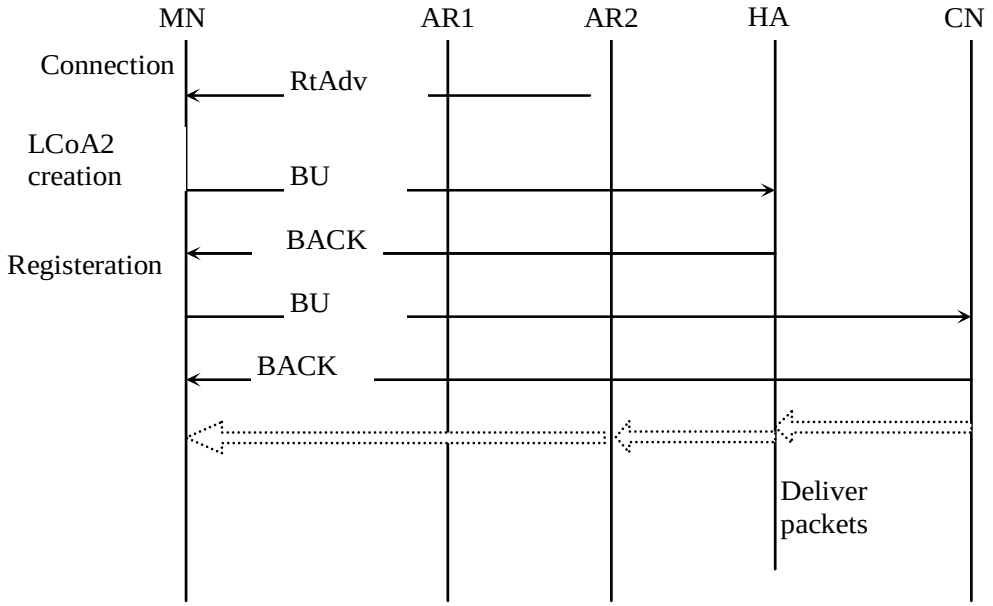


Basic mobile IPv6 signaling

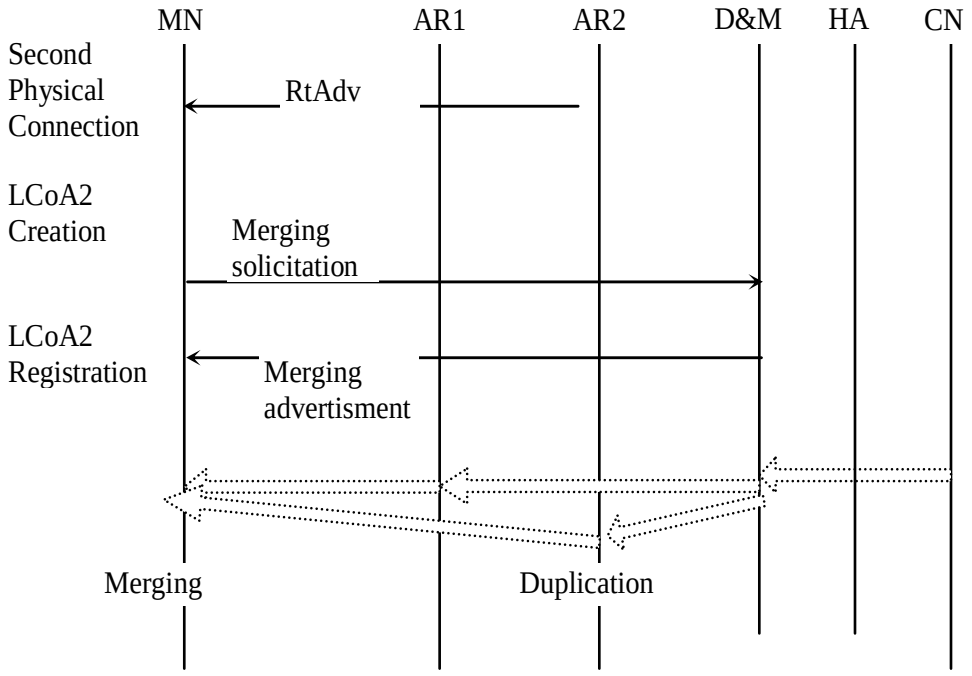


Mobile IPv6 soft handover signaling

Figure V-2 first connection to AR1 in Gemini2



(a) Mobile IPv6 signaling



(a) soft handover signaling

Figure V-3 Mobile IPv6 and soft handover from AR1 to AR2 in Gemini2

2. Performances Metrics

The purpose of our simulation is to examine the effect of mobile IPv6 handover, fast handover bicasting and soft handover on the performance of an end-to-end UDP communication sessions. In particular we want to examine the packet loss, end-to–end additional delays and IP signal load information as a direct result of mobile handover across IP- based access routers. In following we define the metrics that will be used across this chapter to analyze and evaluate handovers performances.

- *End-to-end transmission delays*: the delay needed by UDP packet sent by CN to correctly reach the application layer in the top of MN. Additional transmission delay can be introduced either in the core of the network or by the wireless retransmission in link layer of corrupted packets.
- *End-to-end jitters:* Inter-packet Jitter is a measure of the variation in the end-to-end delay of packets receiving by the MN. It is very important metric for real-time applications such as video conferencing, which require packets to arrive at a steady rate.
- *Packet loss* and *Packet delivery ratio*: The ratio of the number of unicast UDP data packets generated by the CN and correctly delivered to the MN through the core network and radio communication versus the number of packets supposed to be received. There are two main causes of packet loss, the radio transmissions degradation and MN disconnection when performing handover.
- *Signaling load*: the load of signaling and control messages on the air generated by the MN and the network as a direct consequence of MN handover from an AR to a new one.
- *UDP Throughput*: in this study, CN transmits packets to the MN in movement at fixed throughput. The throughput measure is essential to evaluate the MN reception rate data. The throughput can be perturbed by packet loss and retransmission caused by handover and signal degradation.

3. Simulation Scenarios

The simulated network topology is shown in Figure V-5. The wireless access network consists of ten access routers (ARs). Each AR has two interfaces, an Ethernet interface for the connection with the core of the IPv6 network, and IEEE802.11b wireless interface. ARs are located at the limit of each others coverage with sufficient overlapping of the coverage area to allow both of mobile IPv6 handover and soft handover (the distance between ARs is set to 150m). Each wireless interface has 4 channel frequencies to avoid signals interferences. The two-ray model, also known as the plain earth loss model, is used as the path loss model. The simulated card is Lucent Orinoco DSSS 2.4 GHZ (11 Mb/s)[103], with the range (packets reception/packet detection) of (50m/422m). If the distance between MN and AR is lower than 50m, sent packets are received, if the distance is between 50 and 422 m, packets are detected and received with certain probability of correct reception. Probability depends on the distance between MN and AR, as described in Figure V-4.

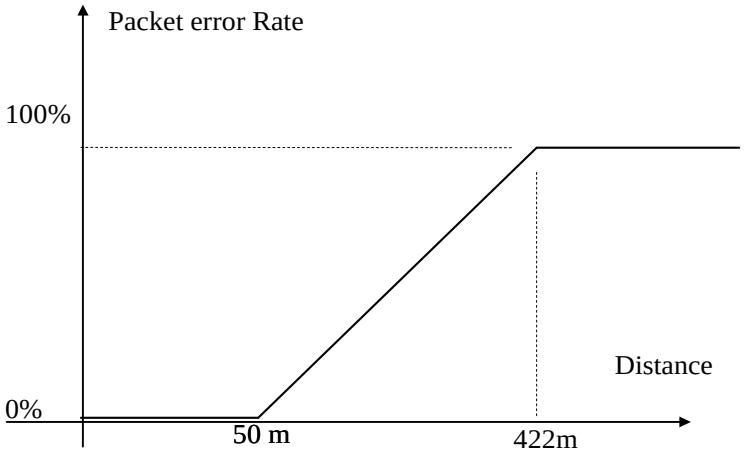


Figure V-4 IEEE802.11 propagation model in Gemini2

The core of the network consists of an IPv6 switch, to which we connect three IPv6 specific nodes: home agent, D&M agent and correspondent node.

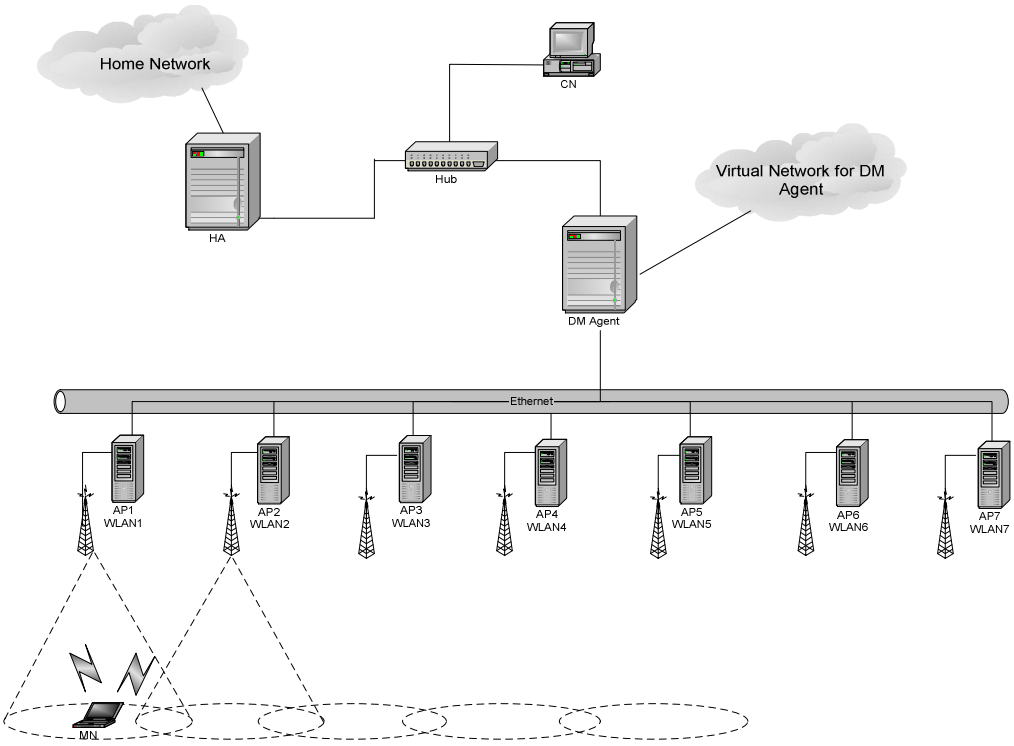


Figure V-5 Simulation network topology.

The CN is a simple IPv6 terminal with one Ethernet interface, its role is to generate packets to the MN home address, it has a fixed IPv6 address and a binding cache to store MN care of addresses, as described in mobile IPv6 RFC. The home agent is an IPv6 router with two Ethernet interfaces; one of them is used to define the virtual IPv6 home network of MN. The HA is responsible of the binding cache management. The D&M agent is an IPv6 router used to manage MN multihoming and IPv6 flow duplication and merging during the soft handover. We define two MNs: the first has only one wireless interface and the second one have two wireless interfaces and soft handover capabilities.

User Datagram Protocol (UDP) [35] is the most used transport protocol for real time applications such as audio and video traffic for internet telephony and video conference applications. For this reason, we will use UDP as transport layer in our simulations. The simulation principle consists of a process application running on top of CN sending UDP packets at 500kb/s to the MN home address. This address is an IPv6 address which define the MN in the virtual home network of the HA. A sink application running on the top of MN is responsible of receiving UDP packet and probe registration.

Each AR has a wireless interface defined by an ESSID and represents an IPv6 subnetwork. An ICMP6 router advertisement daemon attached to each AR, broadcasts periodically (period of 1500 ms) a router advertisement message which contains the IPv6 address of AR subnetwork. At this stage of simulation, RtAdv message is the principal available mechanism for MNs to detect a handover in network layer. At the beginning of the simulation, the MN establishes a wireless connection with the first AR. A set of MN movement's scenarios are used as inputs to the simulation. Each movement scenario determines MN movement at different speeds across coverage areas. When the signal quality from a current AR became worst than a certain threshold, the MN initiates an active scanning in 802.11 layer. The goal of this operation is to locate another AR with better quality of the signal. If found the MN initiates physical handover from old AR to the new one. Using RtAdv the MN1 detects and changes its AR by the way of basic mobile IPv6 handover and the MN2 is performing soft handover to change its point of attachment.

4. Basic Mobile IPv6 and Soft Handover Performances

First simulation set aims to examine basic mobile IPv6 handover and soft handover performance to confirm the feasibility of proposed IP6 soft handover mechanisms and our theoretical analysis. The Figure V-6 shows handover delays of a MN performing basic mobile IPv6 handover generated by different simulation runs. The registered average handover latency is 1453ms. This handover latency is caused by for major handover steps: IEEE802.11 roaming, movement detection in IPv6 layer and the new address configuration and registration within the HA. The 802.11 roaming delay values (Δ) are between 200 and 300 ms. This delay is generated by the scanning phase and re-association procedure. During the scan, the MN 802.11 interface listens for beacon messages (sent out periodically by ARs) on assigned channels. Thus the station can create a list of ARs prioritized by the received signal strength. After

choosing the best AR to roam-on using the scan results, the re-association step delay is the latency occurred during the exchange of the re-association frames between the MN and the AR. the MN sends a re-association request frame to the new AR and receives a re-association response frame which completes the physical roaming process.

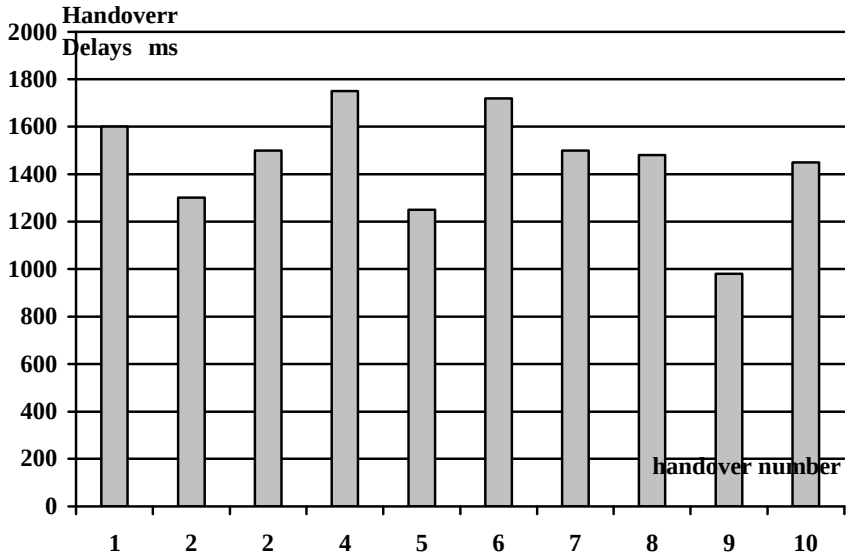


Figure V-6 Mobile IPv6 handovers latency

The delay caused by the movement detection in IP layer noted by Φ_{MIP6} can be expressed by the following equation:

$$Delay_{Movemnt\_detection} = \Phi_{MIP6} \in [0,1500ms]$$

Note that in case of high data load on the wireless medium coupled with the fact that there is no priority for signaling message compare to data message; the MN may not receive the first router advertisement. This results a longer handover delay. In our simulation there is no long distance between ARs and (HA,CN) and the Ethernet propagation delay is negligible. That makes the value of Ω_{MIP6}, which denote the new care of address registration delay negligible.

In order to evaluate the soft handover gain compared to basic mobile IPv6, and to improve the overlay wireless connection quality in border coverage areas, the end-to-end packet transmission delays between the CN and the two MNs is analyzed. The comparison simulation scenarios consist of moving the two MNs across ARs coverage areas at different speeds to generate a set of handover. Higher speed introduces higher handover frequency by minute. In first simulation set, the MN uses basic mobile IPv6, and in second set, the MN uses soft handover mechanisms. By looking at the trends in Figure V-7 showing average end-to-end transmission delays in both mobile IPv6 and soft handover, the following consideration can be made. Soft handover allows MN to keep a minimal transmission delay, about 25ms when crossing coverage area. When MN uses mobile IPv6 basic handover, average transmission delay is to much bigger, about 170ms.

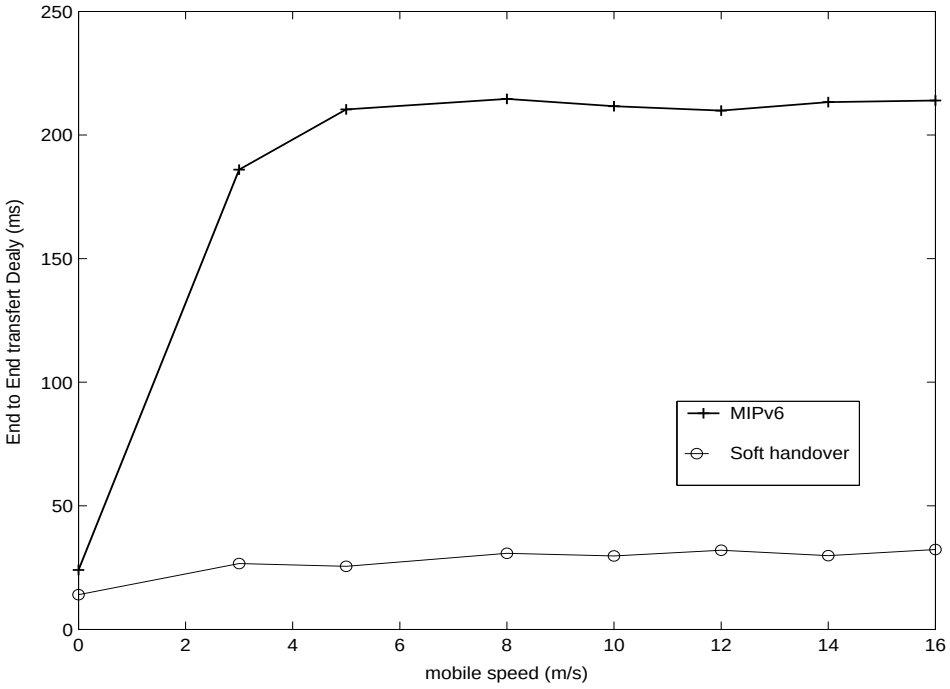


Figure V-7 Average end-to-end transmission delays**.**

To understand the reason of this difference between end to end transmission delays of mobile IPv6 and soft handover, we plot in Figure V-8 and Figure V-9 end-to-end detailed transmission delays for all packets sent by CN to MNs, during one MN movement across the coverage areas at 3m/s speed.

When MN uses basic mobile IPv6, the handover is not initialized before the degradation of old AR signal strength (it became lower than handover threshold). Before each handover, this old AR signal strength degradation generates successive MAC retransmission of packets before the correct reception. These successive retransmissions are responsible of the additional average packet delivery delays in mobile IPv6. After each handover, a better signal strength from nAR allows correct reception of packet at link layer which avoid huge additional retransmission delay. A transmission delay of the MN that uses soft handover remains stable since the soft handover thresholds are more sensible to signal degradation; So as the moment as the MN detects a degradation in its current connection, It establishes a second connection with the new AR and performs local registration with the D&M agent. The Asynchronous transmission on the air of duplicated packets through the two ARs coupled with the use of merging process allows MN to receive the first received among duplicated packets at IP layer. That avoids the introduction of additional end-to- end transmission delays and keeps a stable and minimal transmission delay of 25ms. That validates our propositions and makes soft handover suitable for real time applications.

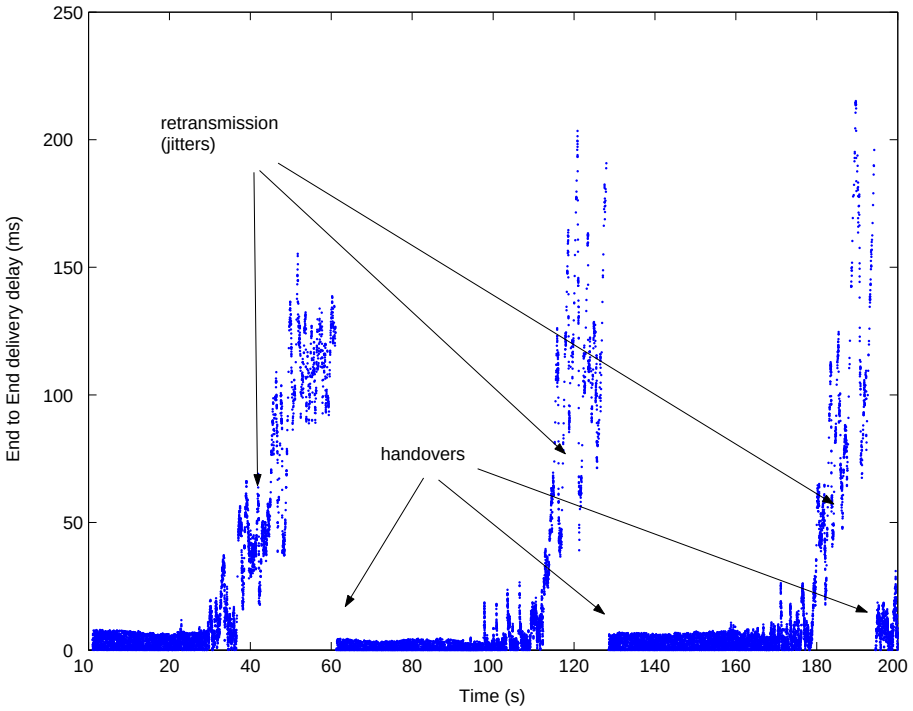


Figure V-8 Detailed mobile IPv6 end-to-end transmission delays.

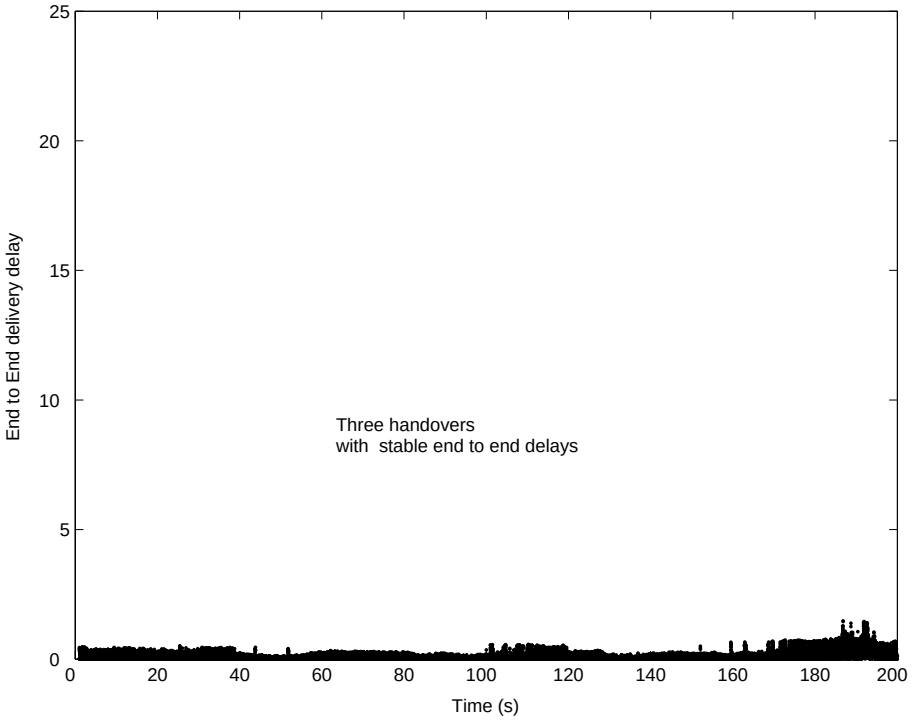


Figure V-9 Detailed soft handover end-to-end transmission delays.

The Figure V-10 present the average end to end jitters variation registered between two MN handovers. These handovers are generated by the same MN movements scenario across coverage areas.

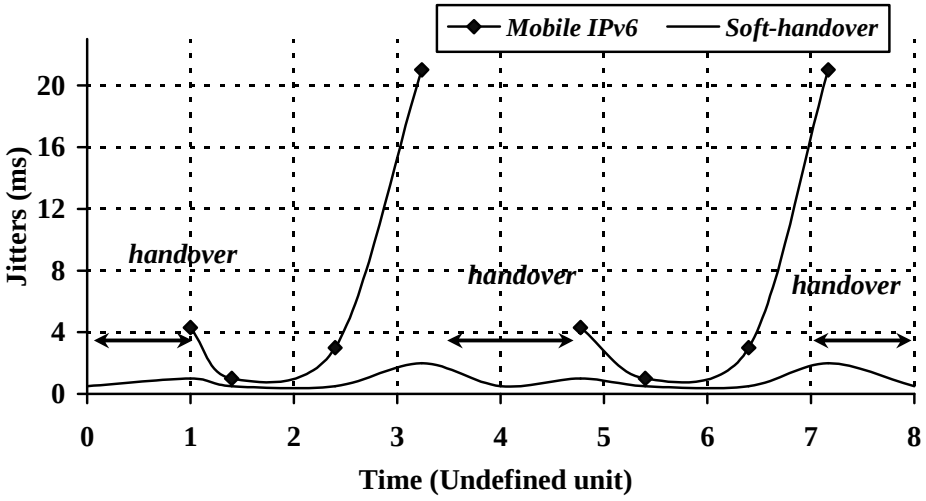


Figure V-10 End-to-end Jitters variation between handovers

For the single-interface-MN which uses mobile IPv6, before each handover, the signal degradation from current AR increases the end-to-end jitters until 21ms. At this moment the MN enables a handover to a new AR with better signal quality. The end-to-end jitters in this connection start with 4.5 ms. jitters decrease with MN movement to the center of coverage area. When the MN moves outside current coverage area, the new signal degradation introduces additional jitters until the next handover. During MN handovers all UDP packets are lost which suppress jitters. For the MN with two interfaces and performing soft-handover, the end to end jitters variation is stable near 2ms. Using two connections with duplication and merging mechanisms in overlapping region reduce transmission delays and stabilize end to end jitters.
The average UDP packet loss is determined using the same scenario. The MN moves across same network topology using mobile IPv6 basic mechanisms and than soft handover. Figure V-11 and Figure V-12 shows two simulation run results. The CN send UDP packet to MNs during 120 s. Each MN moves across coverage areas and performs three handovers. Each figure depicts the sum of UDP packets sent by CN and the sum of the packets received by the MN in movements at each moment. We can see that for mobile IPv6, MN handovers effect in packets reception is clearly visible. Before each handover we distinct two main reason of packet loss:

- The MN movement outside the coverage area causes Signal degradation before handover. This signal degradation causes as seen before, retransmission of corrupted packets, and after a set of failed MAC

retransmission, this packet can be considered as lost. The average delay of this period in this simulation run is 15s.

- When the signal degradation and packet loss reaches the threshold, the MN initiates the handover. As a result, the MN is disconnected for average 1500ms and during this period all UDP packets are lost.

The use of two simultaneous connections in soft handover suppresses packets loss during handover and reduces packets loss introduced by signal degradation. This is depicted in figure V-12, where two-interfaces-MN performs the same previous simulation scenarios using soft handover.

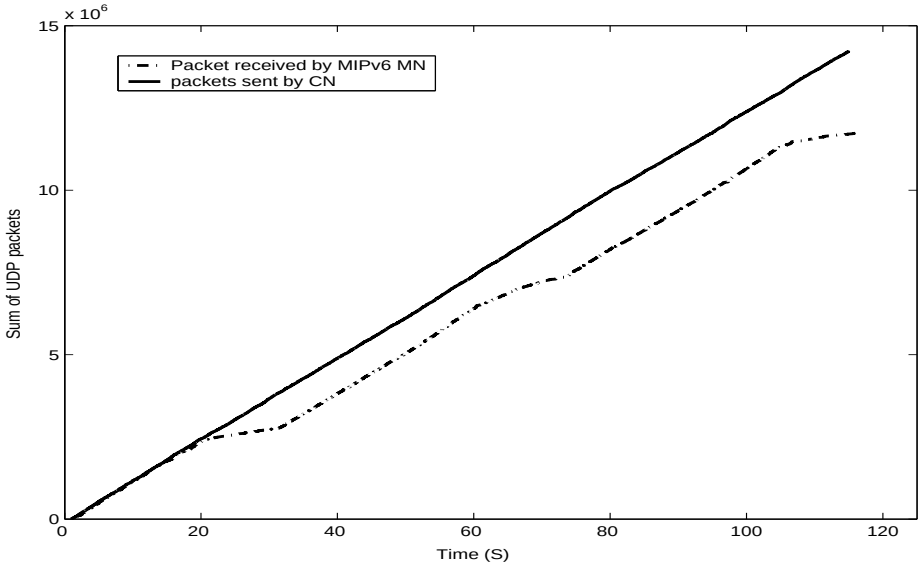


Figure V-11 Sum of received packets in Mobile IPv6**.**

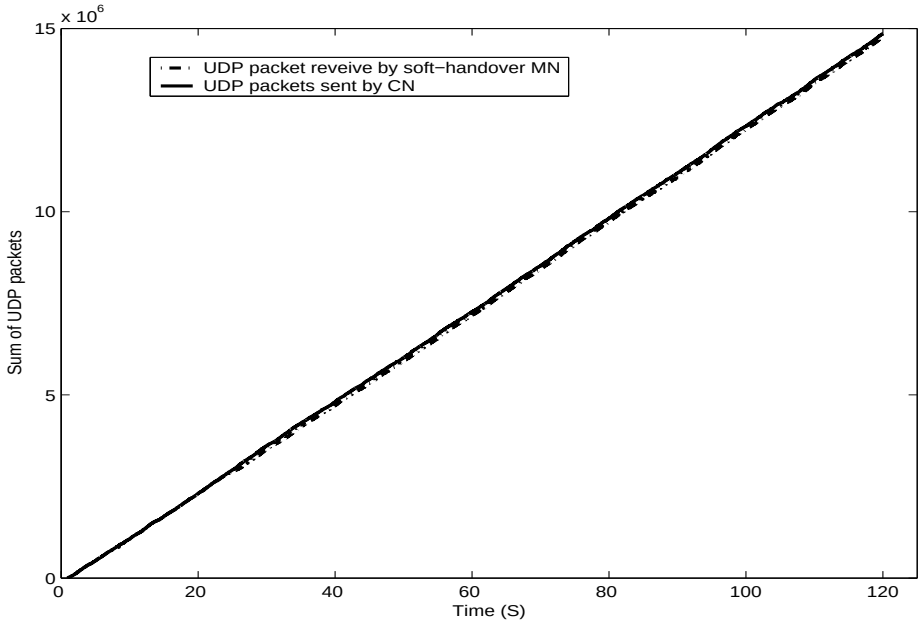


Figure V-12 Sum of UDP received packets in Soft handover**.**

Several simulation runs with different MN speeds allows us to have the Figure V-13. By looking at the trends shown in this diagram, the following consideration can be made. By performing soft handover, the MN registers an average of 98% of UDP packets delivery fraction. This value is stable even MN increase its speed. When MN uses mobile IPv6 basic handover, initial delivery fraction is lowest and the increase of MN speed decreases the delivery ratio. That decreases from 90% in 3m/s speed to 75% in 16 m/s, because of the rising of the number of handovers disconnections.

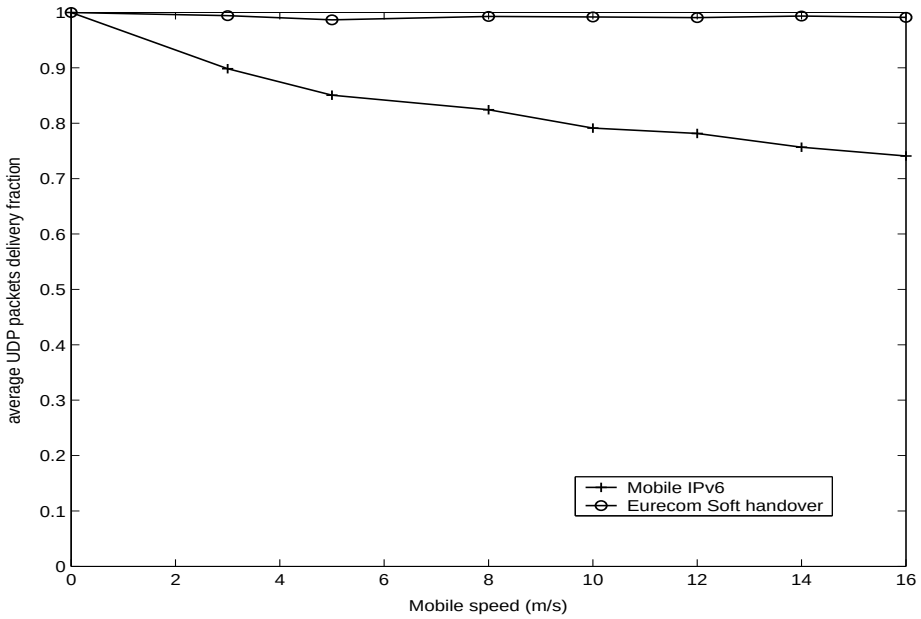


Figure V-13 Average UDP packets loss ratio

5. Protocols Performances Comparison

As shows in chapter III, mobile IPv6 fast handover bicasting is one of the most promising solutions to improve basic mobile IPv6 handover mechanisms. It anticipates the configuration and the registration of future MN address using Layer2/Layer3 interaction. ARs exploit this anticipation to simultaneously duplicate data to the old and new CoAs of MN. That allows MN to receive data immediately after performing layer 2 handover and removes layer3 handover latency. To simulate the fast handover bicasting in gemini2, we implement special function to allow an interaction between IEEE802.11 MAC layer and IPv6 layer. When the MN is about to perform a physical handover and after the 802.11 ARs scanning, it sends a trigger to IPv6 layer of the old AR with the ESSID of the new AR. Fast mobile IPv6 introduces additional Layer 3 messages types [54] for using between AR and MN: RtSol, PrRtAdv, FBU, FBUack, HI, and Hack.

Fast mobile IPv6 signaling and duplication process as modeled in Gemini2 is depicted in figure v-14. We also implement necessary mechanisms in all ARs to intercept MN destined packets, to perform duplication and routing to the MN different care of addresses.

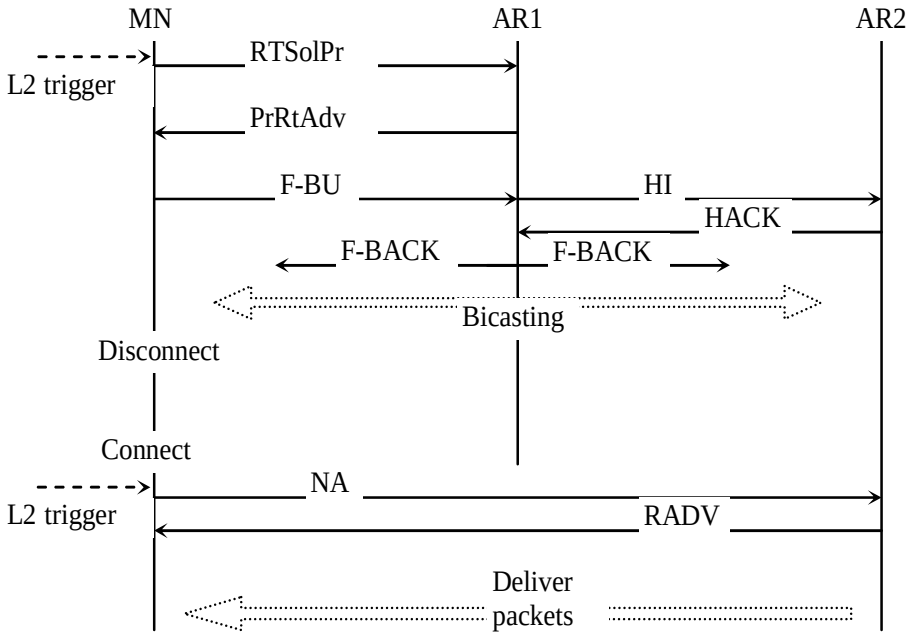


Figure V-14 Fast handover bicasting process

After the general analyses of mobile IPv6 and soft handover done in the past paragraph, the goal of this simulation process is to compare these methods with the other well known IP-based bicasting approach “fast handover bicasting “.

The Figure V-15 describes the network simulation topology that will be used in following. Compared with the previous simulation network topology, we introduce an internet network between the (HA, CN) and the rest of the network (D&M and ARs), the RTT between an AR and the HA is set to 200 ms. The consequence is that the delay of the binding update process becomes not negligible. Each AR run router advertisement Daemon with RtAdv interval set to 500 ms. To reduce the effect of signal degradation on basic mobile IPv6 and fast handover, we reduce the distance between the ARs to get a bigger overlapping region, and we reduce also the value of basic handover threshold.

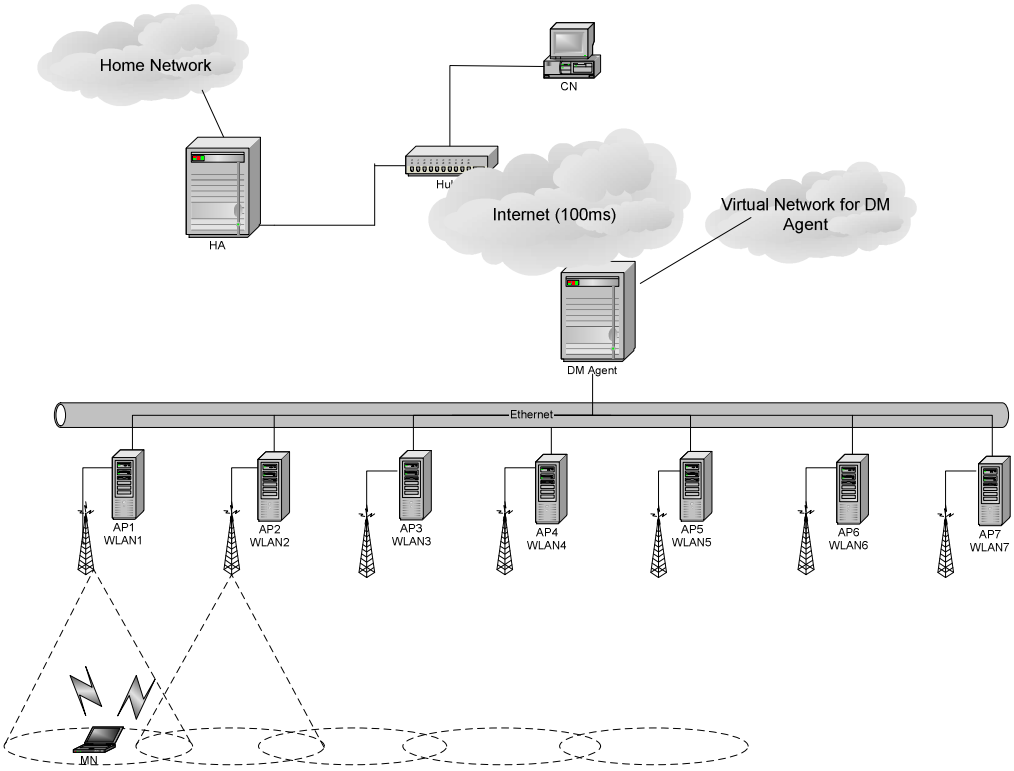


Figure V-15 Simulation network topology 2

We define also the ***mobility rate*** as the number of handovers by seconds that the MN performs when moving across coverage area. The variations of MNs movement speed through the coverage area during a fixed delay give a different mobility rates.

We keep the same simulation scenario, the CN generates UDP packet at 0.5 mb/s to the MN IPv6 home address, with UDP packet size set to 1kb. The MN is first connected to the AR1, and start moving across coverage area with different speed, to generate different mobility rates.

By looking at the trends in Figure V-16 showing average packet loss Vs mobility rate of the three MNs, the following consideration can be made: When the mobility rates increase, the load of packet loss in mobile IPv6 increases from 150kb at 0.02 to 500 kb at 0.08. Fast mobile IPv6 minimizes packet loss about three times compare to mobile IPv6, but the number of lost packets increases also with high values of mobility rate, from 50kb a mobility rate 0.02 to 160kb at 0.08. Using soft handover, there is almost mo packet loss regardless of mobility rate. This phenomenon can be explained by the fact that the MN which performs performing soft handover, still always connected to a network which suppress packet loss. When MN uses Fast mobile IPv6 bicasting handover, packet loss is lowest than mobile IPv6 handover, because global handover latency is equal to the 802.11 physical handover and the disconnection latency is between 200ms~300ms. Whatever the old access router duplicate MN destined

packets through old and new ARS, the MN have only one interface so it have to performs physical handover and can not receive more than one flow at each moment . The highest packet loss rate is for mobile IPv6. The reason is the high global handover latency = the delay of 802.11physicale handover (200 to 300ms) + Router Advertisement messages (500ms)+ Round Trip Time (MN, CN) (200ms).

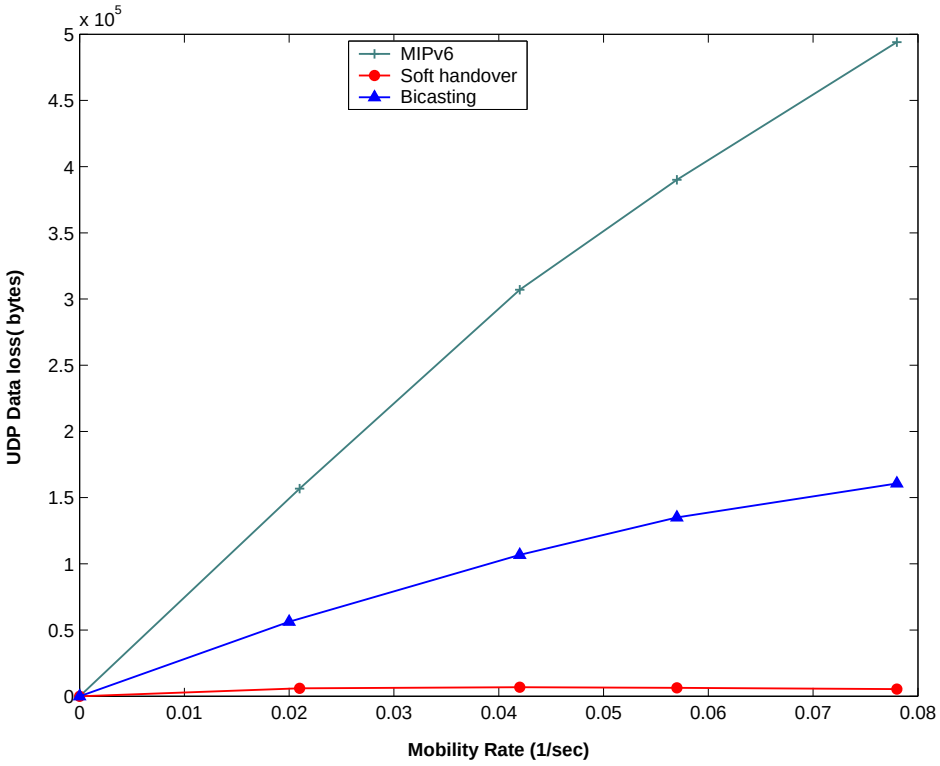


Figure V-16 Average UDP packet loss

Real time applications are sensitive to packet delay and can not typically tolerate additional transmission delays and jitters. By looking at the trends in Figure V-17 showing average end-to-end transmission delays from CN to MN with different mobility rate, we can see that soft handover allows MN to keep a minimal transmission delay, about 102 ms when crossing coverage area. When MN uses mobile IPv6 basic handover, or fast handover average end-to-end transmission delay is similar, about 106ms. Knowing that the wireline transmission of packet is about 100ms, we focus now on the effect of MN handover in wireless transmission delays. Soft handover allows the MN to keep a minimal and stable average wireless transmission delay, about 1ms at different mobility rate. When MN uses mobile IPv6 basic handover, or fast handover, the average wireless transmission delay is about 6ms.

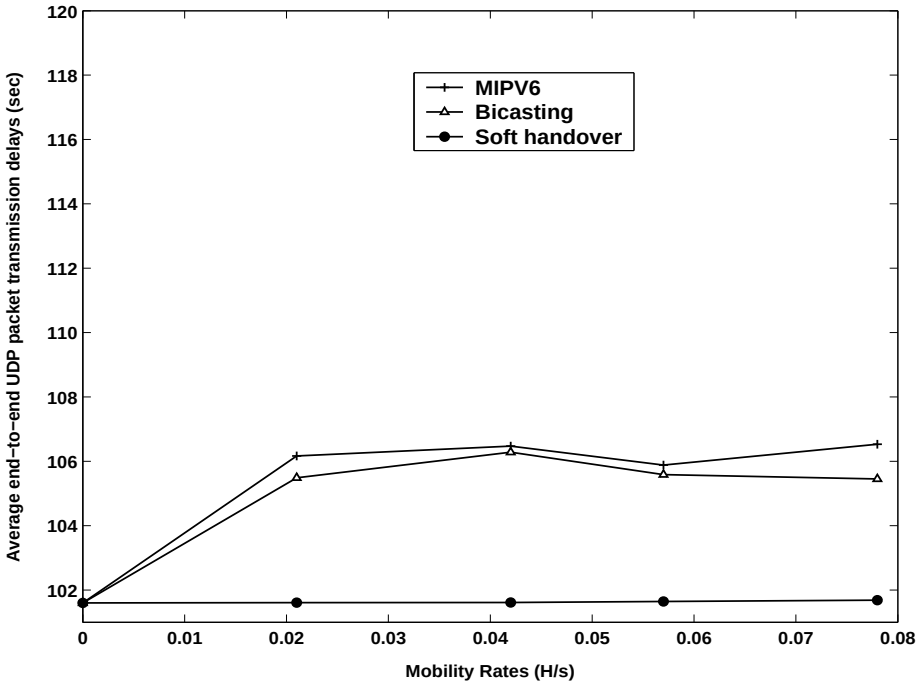


Figure V-17 Average UDP transmission delays

To understand the reason for this additional end-to end delivery, in Figure V-18, Figure V-19, Figure V-20, we plot end-to end transmission delays of all UDP packets sent by CN and received by the MN, in a single MN run over the coverage areas at mobility rate set to 0.07. The MN performs a handover each 10 seconds, this handover is triggered by current signal degradation when the MN move away the coverage area of an AR and enter the zone of new AR with better signal quality.

We can see that using basic mobile IPv6 or fast handover bicasting, an additional end-to end transmission delays is introduced by signal strength degradation of MN connection when it moves away from its old AR. It generates successive 802.11 MAC retransmission [6] of packets before their correct reception. These successive retransmissions are responsible of the additional average packet delivery delays in mobile IPv6 and fast mobile IPv6 bicasting. Transmission delays of the MN that uses soft handover remains stable, because the MN establishes a second connection with new AR before severe degradation of old AR signal strength. Asynchronous emission of duplicated packet through the two ARs allows MN to receive the first among duplicated received packets at IP layer. The maximum registered jitters are similar between mobile IPv6 and Fast handovers (about 70 ms) and for soft handover is about (5ms).

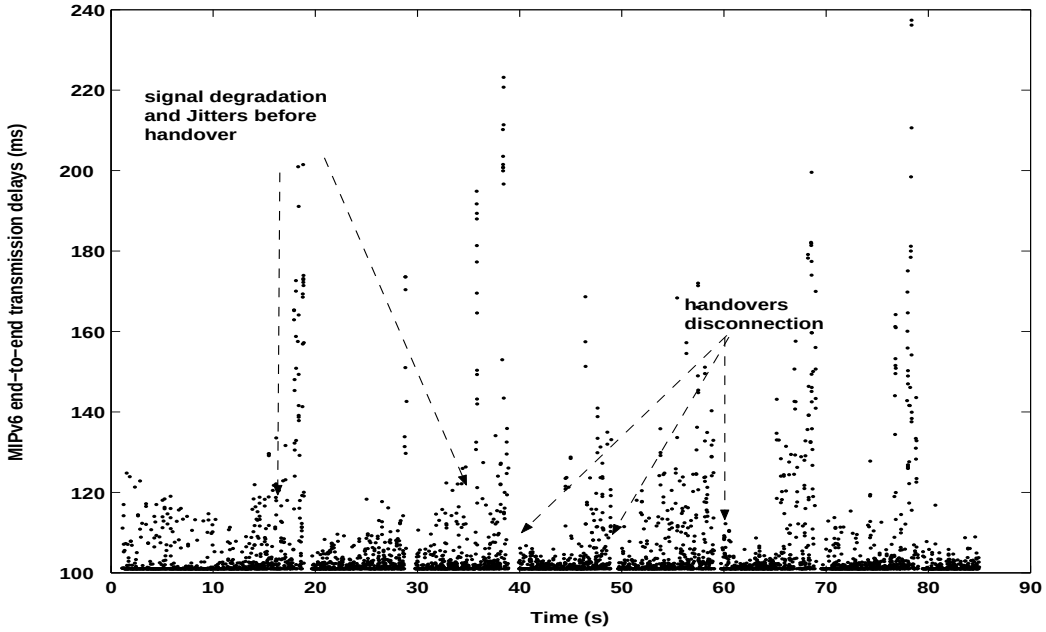


Figure V-18 Detailed end-to-end transmission delays (Mobile IPv6)

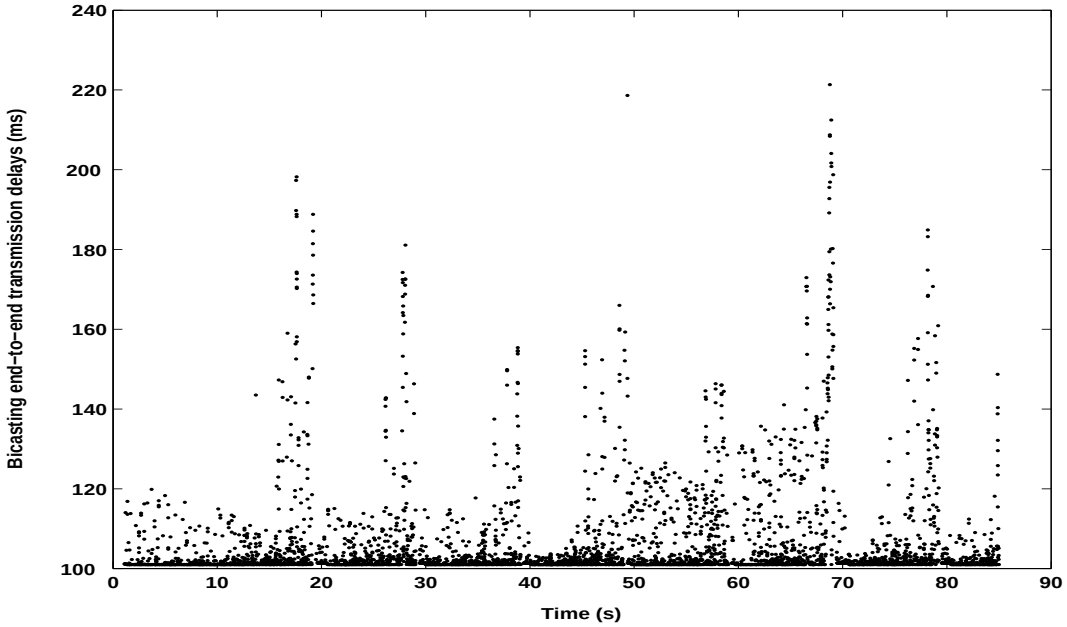


Figure V-19 Detailed end-to-end transmission delays (Bicasting)

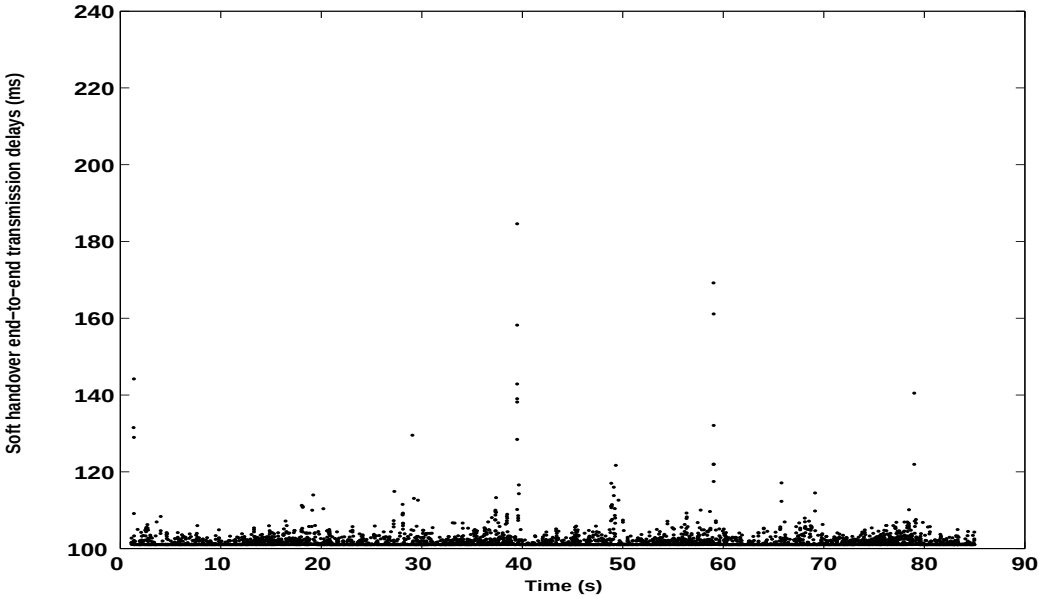


Figure V-20 Detailed end-to-end transmission delays (soft handover)

This simulation set is used to provide analysis and comparison of the amount of IP signaling -related messages load over the air generated by mobileIPv6, fast mobile IPv6 bicasting and mobile IPv6 soft handover.

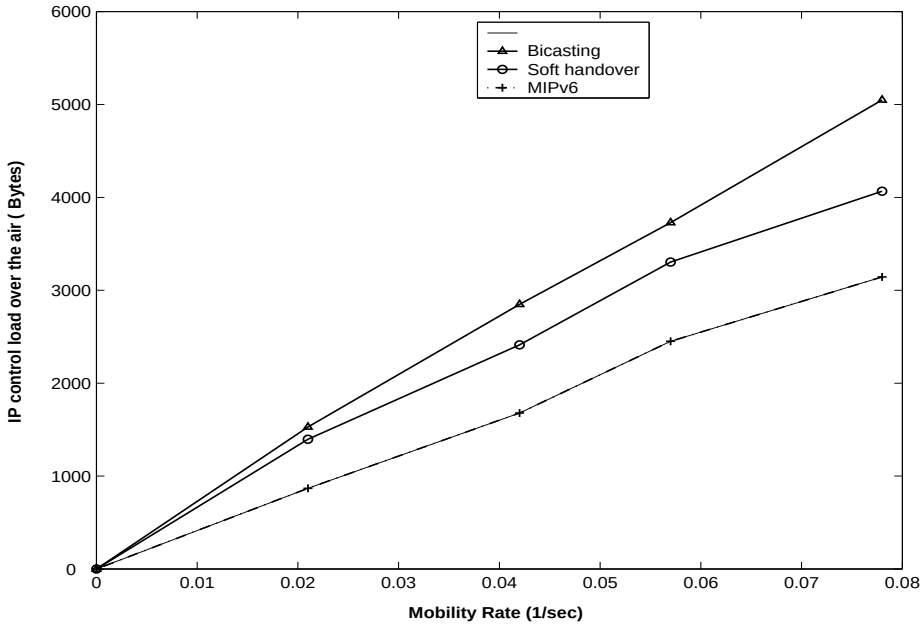


Figure V-21 Handovers Signalling load

The result of the analysis is shown in Figure V-21. Both soft handover and fast mobile IPv6 introduce additional control information load compared to mobile IPv6. Even thought, soft handover manages the handover process using two interfaces, its signaling load over the air as direct result of complete handover process is less than Fast mobile IPv6 bicasting handover signal load.

From Figure V-21, we can see also that mobile IPv6 bicasting and soft handover improve mobile IPv6 handover performances but on the other hand they introduce additional Layer 3 messages types for using between AR and MN: RtSolPr, PrRtAdv, FBU, FBUack, for Fast mobile IPv6 and Merging Advertisement and Merging Acknowledgement, to initiate and close duplication and merging process for soft handover. These additional messages introduce additional signaling load in the wireless network compared to mobile IPv6.

By looking at the trends in Figure V-22, Figure V-23, Figure V-24, showing UDP reception throughput of MNs moving across network topology. We can see that each MN handover using basic mobile IPv6 disturbs considerably the MN reception throughput. Each mobile IPv6 handover generate a MN disconnection, each disconnection has a direct effect in throughput disruption.

The use of fast handover reduces the MN overall disconnection delay. The direct impact of this disconnection delay improvement can be seen in Figure V-23 with a reduced throughput distribution for each handover. By performing soft handover we can see that there is no distribution of throughput, because the use of flows duplications and merging in overlapping region, which make the handover transparent.

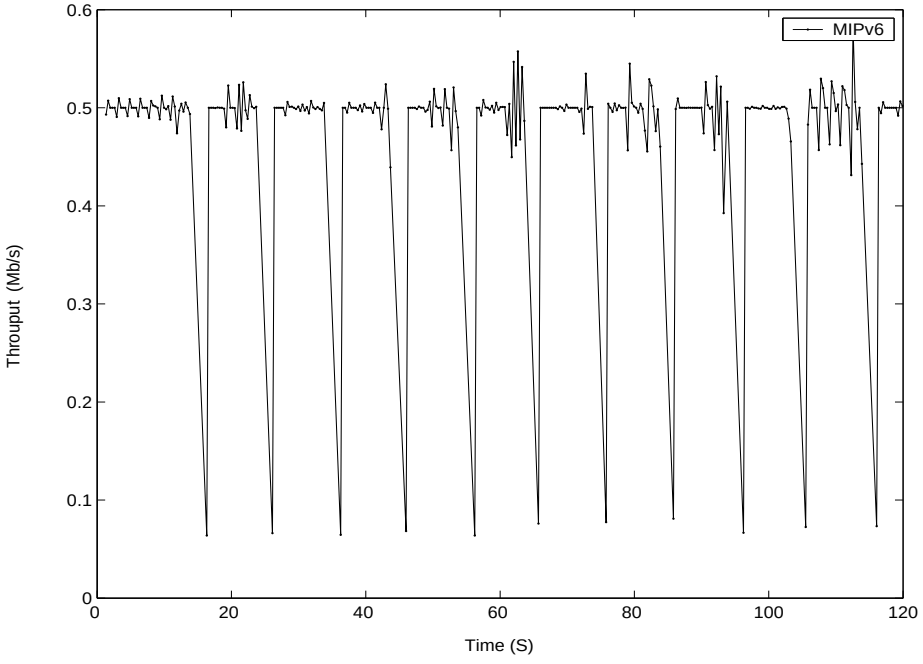


Figure V-22 Mobile IPv6 throughput

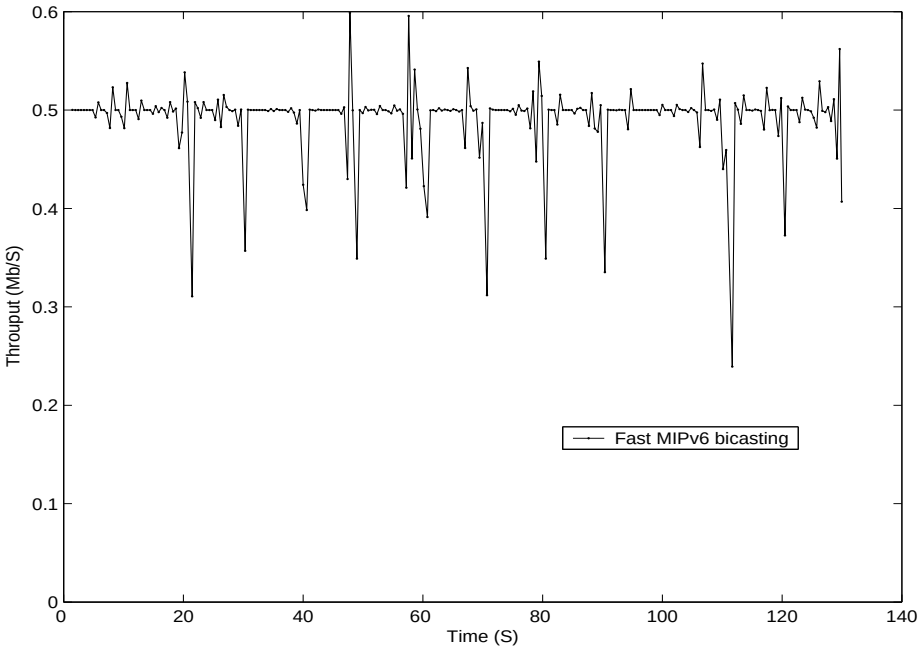


Figure V-23 Bicasting UDP Throughput

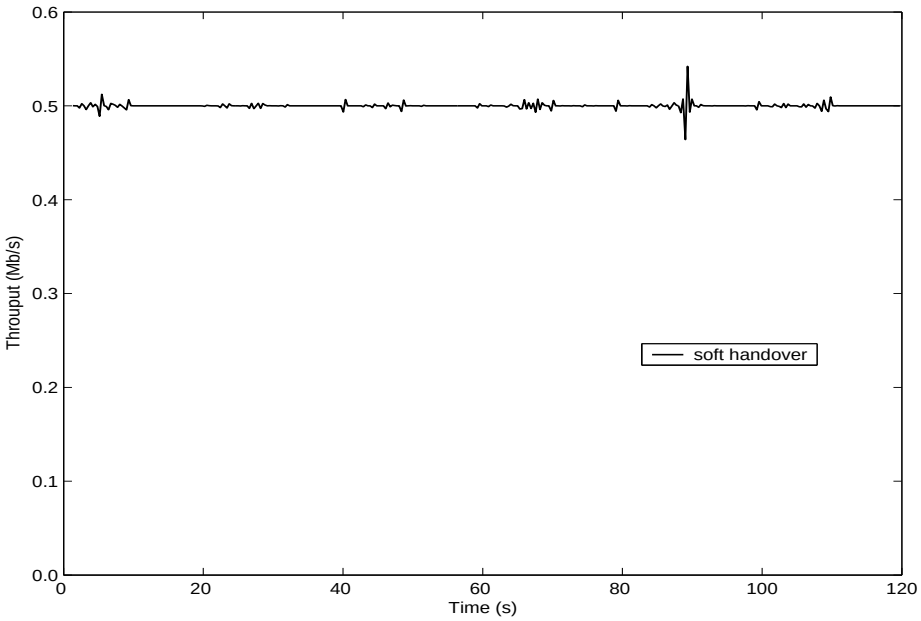


Figure V-24 Soft handover UDP throughput

6. Conclusion

In this chapter, we studied the performance of mobile IPv6 bidirectional soft handover in Gemini2 simulator over Wireless LAN IEEE 802.11b. Two MNs were used for the simulation First MN has a single interface and performs basic mobile IPv6. The second one has two wireless interfaces and roams between access routers using soft handover. The core mobile IPv6 network is composed of access routers, D&M agent, CN and home agent.

First simulation set aims to only examine basic mobile IPv6 handover, soft handover brut performance. The goal is confirm our analysis on mobile IPv6 handover performances and the feasibility of proposed IP6 soft handover mechanisms. The performance evaluation of mobile IPv6 and soft handover, based on UDP data traffic generated by a CN to MNs in movements, identifies two main raisons of UDP session perturbation. The MN movement causes Signal strength degradation, which generates MAC packets retransmission of corrupted packets. Thus introduce additional end-to–end UDP delays, additional jitters and packet loss. Moreover, the MN disconnection in basic mobile IPv6 handover introduces most of packet loss. Simulation shows that soft handover overcomes the two problems and allows the MNs to keep a minimal jitters and no packet loss when performing handover. The MN double connection before sever signal degradation in soft handover combined with IP merging process allows MN to reduce sensibly this additional delays.

In the second simulation set, we compare the soft handover with other well known approaches, which is the fast handover bicasting. This approach exploits an interaction between layer2/layer3 and a unidirectional bicasting process to improve mobile IPv6 handover performance. Simulation results show that the fast handover bicasting reduces MN disconnection handover to 200ms. Thus, it reduces sensibly packet loss compared to the standard mobile IPv6. IP soft handover have a better overall performance, because there is no MN disconnection at all when performing handover. Moreover, the soft handover merging mechanism exploits path diversity to improve the quality of connection in border area when fast handover bicasting process does not address this issue at all. On the other hand, both of soft handover and bicasting introduce additional signal load over the air compare to mobile IPv6. Soft handover signal load is less than Fast handover bicasting load, but we have to note for the two approaches, that the data tunneling and duplication introduces additional overhead of about 48 bytes to each duplicated IPv6 packets.

In the next chapter we propose and evaluate the impact of hierarchical architecture of D&M agent in terms of duplicated packet load, and signaling load in the core of a Wide Area Network.

Finally, the best way to validate the performances of our approach is to perform real measurement on real traffic. In the last chapter the propositions are validated using a multi-interfaces MN prototype and core network implementation.

CHAPTER 6

VI. Hierarchical D&M Agents Architecture

1. Hierarchical Architecture Proposal

After the description and the evaluation of mobile IPv6 soft handover approach, we try in this chapter to propose a solution to the D&M agent deployment challenge. Note that the D&M agent is a key element in the multihoming management and soft handover realization. Thus, using a single D&M agent in the network is not a realistic deployment solution.

In following we extend our soft handover solution with additional proposal. It consists of the deployment of multiples D&M agents in the networks, organized in several levels of hierarchy per site. We describe in following, basic principles and necessary signaling mechanisms to manage multiple level of D&M agent located between the MN and the CN. The goal of this extension is to reduce the overall duplicated packet load in the network, and confine the soft handover data duplication and signaling messages on local subnetworks. This can be achieved by performing the duplication and merging process as closer as possible to the ARs used by MNs.

To perform such architecture, we split the global networks in a set of sites. Each site can be split into several levels of hierarchy. A D&M agent is then deployed in each level of hierarchy of the site. The D&M agent that manages duplication and merging for hole the site is in the top of the tree, followed by the D&M of the lower hierarchy level and so on, until the lowest level. We suppose that each AR is aware of the addresses and network hierarchy of its D&M agents. E.g. from the Figure VI-1, the access router (A) and Access router(B) D&M agents lists contain: (D&M2, D&M1). For AR(C) the list contains from the lower to upper level (D&M4, D&M3, D&M1).

Each AR broadcasts to the MN, in addition of the RtAdv basic information (the IPv6 address of the current AR), the D&M agent related information. Using this information collected through its different interfaces, the MN keeps a different D&M agent list of each one of its active interfaces currently connected to the network. When the MN connects its first interface, it registers its first LCoA within lower D&M agent and registers the PCoA getting in this D&M agent with the D&M agent with a higher hierarchy …..Etc.

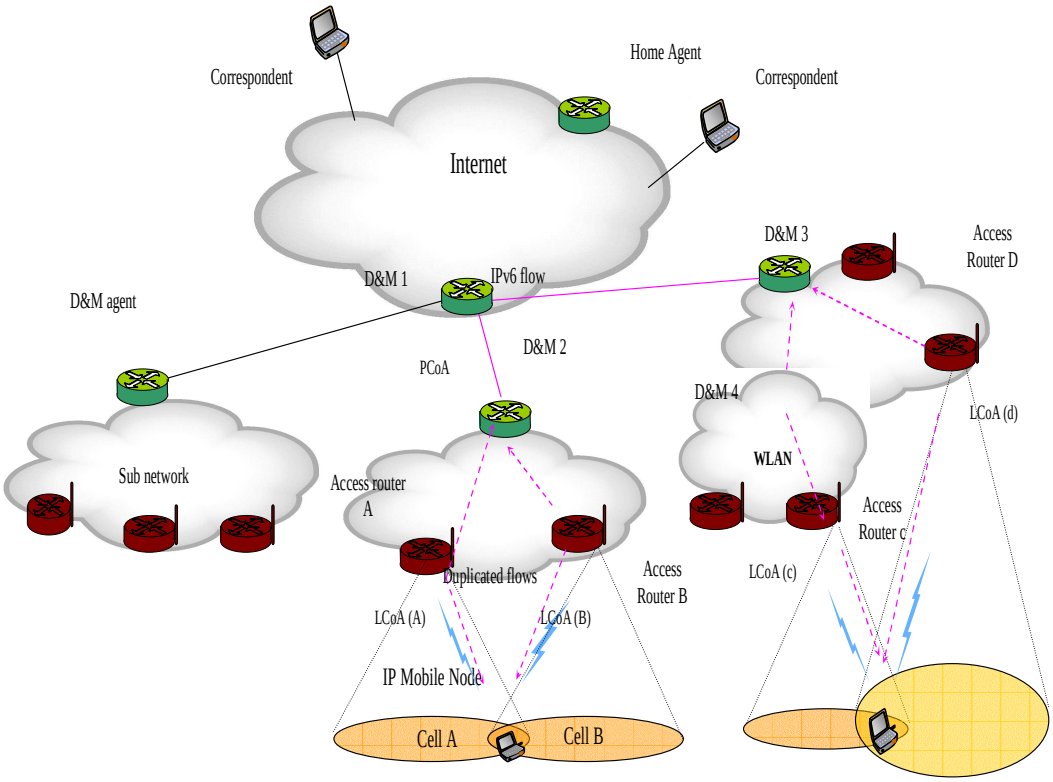


Figure VI-1 Hierarchical D&M agents architecture

When performing a soft handover the MN connect its secondary interface with a new AR. To manage the second connection of the mobile, we separate mobility into micro mobility (within the same lower D&M agent range) and macro mobility (inter-site mobility). In micro mobility, the mobile node has to establish the second connection within the same sub-network with its first connection; in this case, the lowest D&M agent assigned to the MN will be the same in the two interfaces. The MN then performs the same local registration process as described in chapter 3.

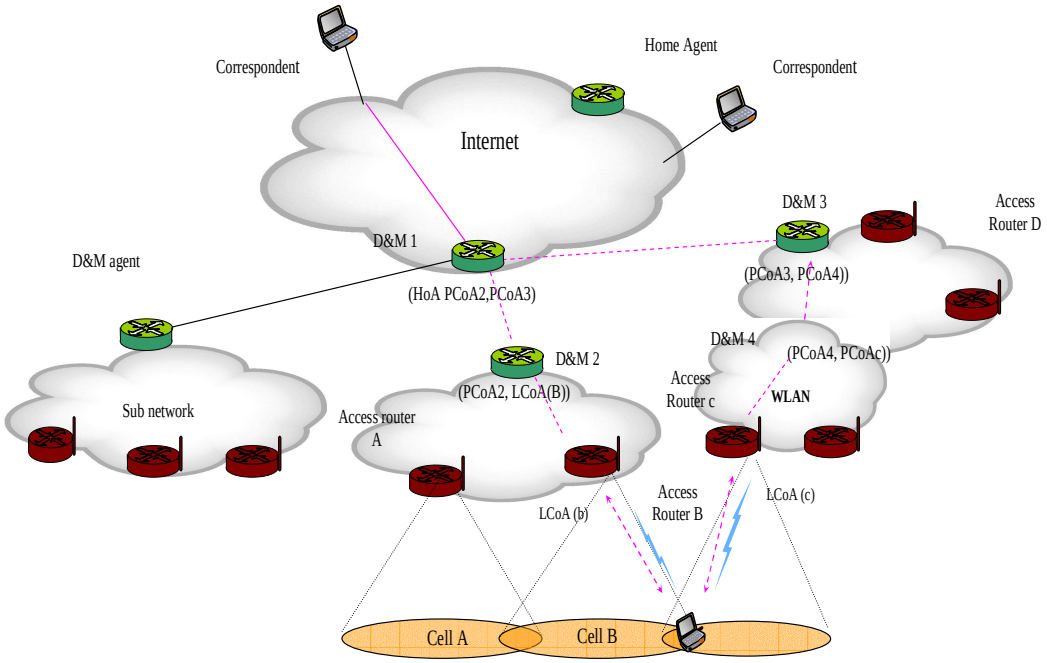
It sends merging request with its new LCoA to the lowest D&M. this D&M will update the MN duplication table entry with this new LCoA. As result, this D&M duplicates packets to the MN, and the MN uses this D&M agent address

as destination address of all its duplicated packets. The MN exploits the D&M agent's hierarchy list sent by each AR to determine the nature of mobility, micro of macro mobility.

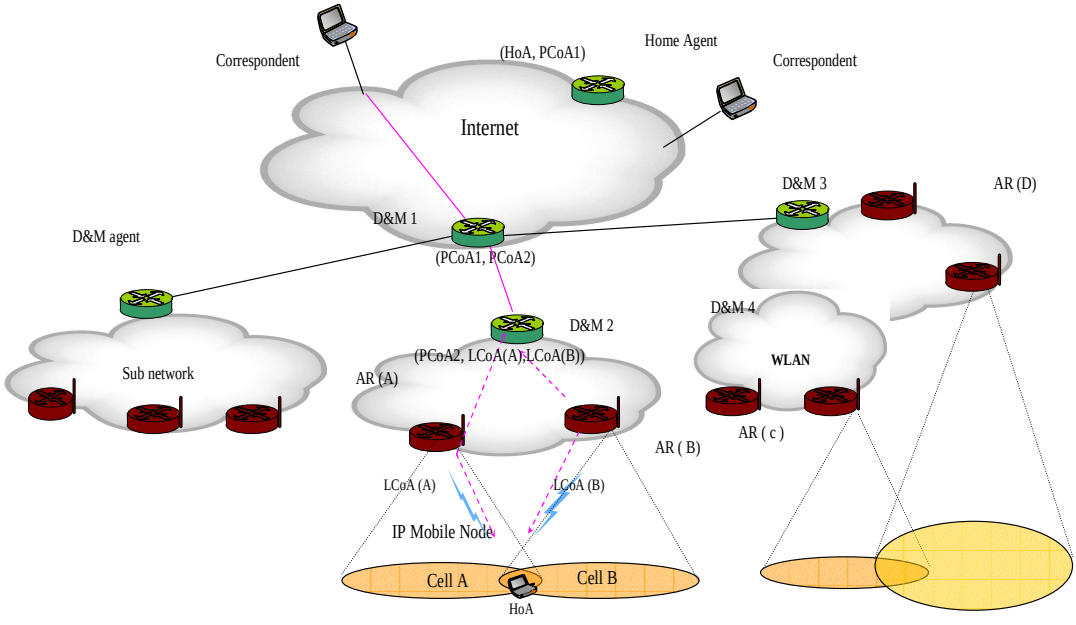
In case of macro mobility the MN performs the following operations:

- It gets a new LCoA from its new AR.
- From the D&M agent's hierarchy lists of its current AR, it extracts the IP addresses from the lowest D&M until the first common D&M between its two interfaces.
- This lowest-common D&M agent noted by D&Mn , will be assigned as the MN D&M agent; its address will be used as the destination of MN uplink duplicated packets during soft handover process.
- The MN gets new PCoA in each D&M agents from D&M1 to D&Mn (we note D&Mi, the D&M of rank "i" in the branch from the MN to the top D&M agents).
- D&Mn is the first common D&M agent between the primary MN connection and the new secondary connection.
- MN creates and updates its binding entry in each of D&M agent duplication and merging tables.
- As results the D&Mn will have in its duplication and merging tables table, a MN corresponding entry with two LCoA.
- The results, is that D&M will duplicate packets to the two MN connections.
- Others intermediate D&M, will have only one LCoA in their duplication table, so they will not reduplicate packet, they have just to decapsulates and encapsulate packets. They act as local HA.
- The result is that the duplication process will be as near as possible to the MN.

Figure **VI-2** shows two examples of signaling within hierarchical D&M agent's architecture for soft handover.



(a)



(b)

Figure VI-2 Hierarchical D&M Binding entries

2. Hierarchical Architecture Performance Evaluation

Gemini2 simulator is used for the evaluation of the benefits of hierarchical D&M architecture in soft handover compare to a single D&M agent. The goal of these simulations is to examine the effect of a hierarchical D&M agent architecture compares to a single and centralized D&M agent on an end-to-end UDP communication session between a CN and MN. The CN is located in the Internet Network, which is connected to three local networks. The MN is moving and connecting to the internet through these local networks. In particular we want to examine the sum of duplicated packets and signaling load in each part of our simulation network: the Internet and each local network.

The same simulation scenario is used; a CN sends UDP packets at 0.5 Mb/s to a MN moving across simulation network topology as described in Figure VI-3 and Figure VI-4. These figures show the network topologies used in simulations. An Internet network connected to three local networks, in each local network we have a set of ARs uniformly distributed. These ARs give MN optimal radio coverage for about 1000m. In first network topology, we use only a single and centralized D&M agent. In the second topology, we introduce two levels of hierarchy. A local D&M agent is used in each local network and global D&M agent in internet is used to manage MN global mobility.

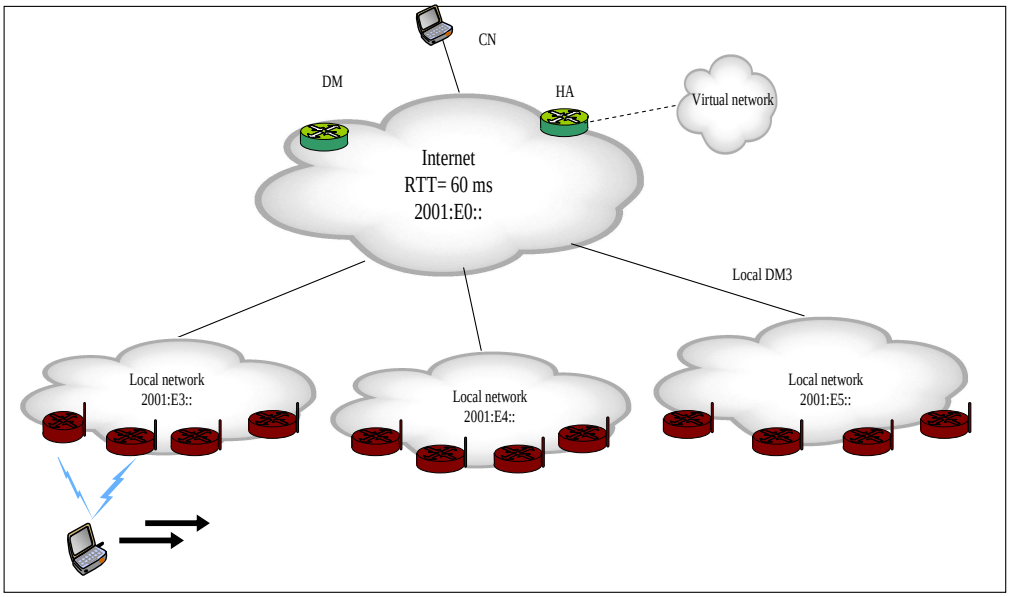


Figure VI-3 network topology with single D&M agent

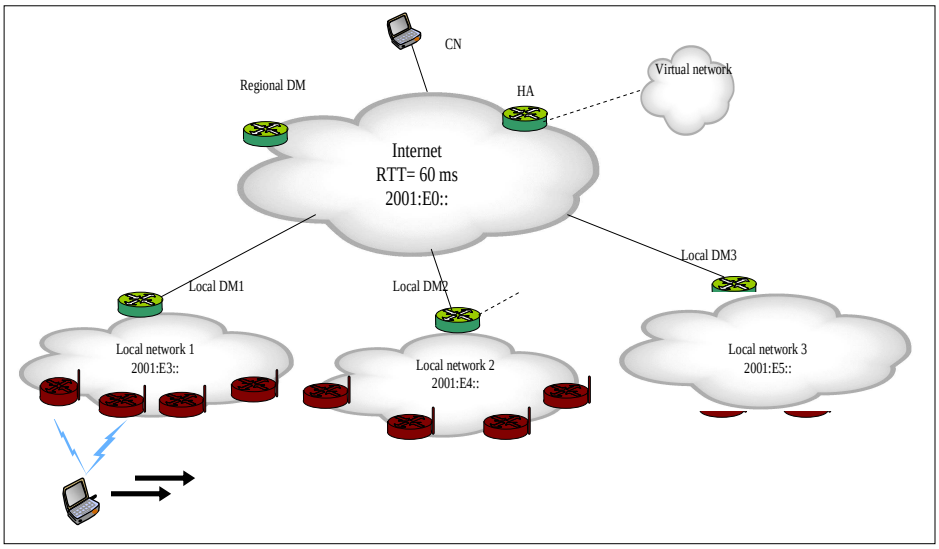


Figure VI-4 Network topology with Hierarchical D&M architecture

*Duplicated packets in the networks***:** One of the most important drawbacks of soft handover is the duplicated data overhead introduced in the core of the network and wireless part of communication. Using a hierarchical architecture of D&M agents as shown in table 4, allows a local duplication of packets when MN performs local handover. The duplicated packets will be routed through Internet only when the MN performs a global handover between sub networks. The table 4 shows the sum of duplicated data packets sent from CN to the MN when the MN moves across network topology 2 with mobility rate =0.05. It performs both local handover and global soft handover between border ARs.

	Internet	LAN1	LAN2	LAN3
Duplicated packets	1358	2974	5021	4473

Table 4 Sum of duplicated packets

Local soft handovers in LAN1 introduce 2974 IPv6 duplicated data packets, in LAN2 they introduce 5021 and in LAN3 4473. Global MN handovers between each sub networks are managed through global D&M agent. They generate 1358 duplicated packets in the Internet. Using the second network topology, we register that the sum of duplicated packets in Internet network is equal to the sum of duplicated packet in LAN1, LAN2. LAN3.

Signaling load in the network: This simulation set tries to determine and compare load control information generated in each sub network as direct results of soft handover. The MN moves across the two networks using soft handover and performs both local handover and global handover. The MN speed is set to 5

m/s and mobility rate is set to 0.05 handover/s. Simulation results are shown in table 5.

	Internet	LAN1	LAN2	LAN3
Hierarchical D&M	1792	1024	1024	1024
Single D&M	3584	-	-	-

Table 5 Signalling load (byte)

Using a single D&M in the network, for each handover, the MN sends merging request/merging advertisement signaling to its current D&M agent and requests for duplication and merging process. Thus, the entire signaling messages have to be routed through the local network and Internet to this D&M. In case of local Mobility in hierarchical D&M architecture, the MN send its binding update only to the local D&M which reduces significantly the signaling load in internet and confines it only to the local level.

3. Conclusion

One of the most important components of the mobile IPv6 soft handover is the duplication and merging agent (D&M). This IPv6 router with special capabilities located in the core of the network is on charge of mobile node multihoming control plane and the duplication and the merging of data between the core of the network and the mobile node when performing soft handover. In chapter 3, we described the soft handover mechanisms; we introduced the D&M agent notion without proposing solution to deploy one or more D&M agents in the core of the network. In this chapter, we identified first, two main constraints of D&M agent deployment in real Wide Area Network,

- In real scenario with many MNs, more than one D&M agent are required, to allow the duplication and merging charge distribution through different routers. It is difficult to imagine that one router can duplicate and merge packet for hundreds of MN without network congestion.
- To reduce the duplication packets and signaling load in the core of the network, it is necessary to duplicate packets as closer as possible to the MN, moreover.

For this reasons, we proposed a combination of hierarchical architecture and soft handover, called hierarchical D&M agents architecture, to disturb the duplication among different D&M agents deployed in the network. This solution allows a local management of data duplication and merging. The simulations results show that the use of local D&M agent in wide area networks reduces the delay needed by the MN to register its secondary LCoA and reduces duplicated packet and signaling load in the core of the WAN. Local MN movements are managed by local D&M agent, the handover signaling and packet duplication are generated only in local networks.

CHAPTER 7

VII. Mobile & Testbed Implementation

For the case studies of multi-homing and mobile IPv6 soft handover mechanisms, a software platform has been implemented termed Eurecom soft handover mechanisms. As will be explained later in this chapter, the software platform is not limited to the case studies investigated in this dissertation and can rather be regarded as an experimental platform to investigate general multi-homing mechanisms, QoS issues and support of soft handover experiences between different radio access technologies. The implementation is based on the mobile IPv6 multihoming and soft handover protocol design presented in the patent [69] and publications described in [71][72][73][75][74].
The implementation is based on Linux Redhat [96] kernel 2.2.18 IPv6 Stack and open-source software MIPL version 0.9.4 [77][78]. Under the GNU General Public License (GPL) and publicly available at[97]. This software extends the basic IPv6 routing mechanisms of the kernel with mobility mechanisms and data structures to support basic mobile IPv6 entities. We use also the Monash patch 0.3 for MIPL 0.9.4, [86] to exploit its features in order to implement the local registration within D&M agent. [84].Our platform [69]has the following features:

- The native support of IP next generation (Version 6) by both of mobile terminal and access networks
- The support of heterogeneous access network technologies, namely IEEE802.11, and UMTS (TDD) and can be extended to other technologies [91].
- The mobile IPv6 basic correspondent node and home agent are not modified. That means that all IPv6 capable hosts can communicate with

the mobile node. Only the mobile node and D&M router require specific mobile IPv6 modifications.

- The support of MAP defined extension to RtAdv daemon. That allows mobile Node dynamic discovering of D&M router and its IPv6 address.
- The SoH provide a generic and a basic solution to soft handover and multihoming management. Therefore it can be easily extended to support other IPv6 handover mechanisms and Quality of Services schemes.

Moreover on the mobile IPv6 soft handover the following functionalities have been implemented

- Advertisements/solicitations to advertise the availability of access routers and allow the MN to detect handover in IPv6 layer.
- Introduction of multi interfaces priorities management in MN.
- Advertisements/solicitations to indicate whether the D&M agent is available or not and allow a dynamic discovery of D&M agent and its IPv6 address.
- Support for different handover types: basic mobile IPv6 handover, vertical handover, soft Handover , which can be intra or inter-technology (vertical) handover,
- Introduction of D&M agent to duplicate and merge packets to and from the MN in the case of soft handover.
- Introduction of new Option field in IPv6 packets to allow identification of duplicated IPv6 packets.

The software platform has been implemented for Linux, a free UNIX-type operating system [76][79]. The main components of soft handover are based on modified version of MIPL 0.9.4. They are implemented as daemon running in user space with root privileges. A router advertisement Daemon version 0.7.2 with MAP options enabled is used in access routers [80]. The platform is comprised of the following main components.

- Mobile Node: The mobile node is responsible of multiple interfaces management, handover detection and registration messages.
- Home Agent: The home agent maintains a MN home address/regional care of address binding entry, it intercept all packets sent to the registered MN and redirects them to its new location.
- Duplication and Merging Agent: It is a conventional IPv6 router located in the core of the network; it maintains a mobile regional address/local care of addresses. It intercepts packets sent to the NN regional address and duplicates them to the actives interfaces. It allows also the merging of duplicated packets issued by the mobile node through its different interfaces.
- Access routers: They have a wireless and wireline interfaces. They broadcast router advertisement RtAdv in wireless interfaces to indicate the address of D&M Agents using MAP options, and allow the mobile node to detect the handover in IP layer.

1. Implementation Environment

1.1. Linux Operation System

The soft handover platform is running in Linux operating system on x86 architecture as Pentium or AMD. The Linux operating system and its kernel are an evolutionary project which has been developed since 1991 by hundreds of developers around the world. As a consequence of this process, no complete design documentation exists that could be used as a basis for further development.
An alternative approach to understand the functionality of the Linux OS and related programs is of course given through the source code itself. Regarding the Linux kernel, analyzing its sources seems to be the only kind of available documentation for many parts of its implementation especially that of the IPv6 network layer. The Linux kernel has the possibility to separate part of its functionality in modules that can be loaded when needed and unloaded when unneeded. This, provides a running operating system with the capability to potentially offer a lot of functionalities and at the same time keep the amount of code and processes currently running in kernel space relatively small. Another advantage of loadable kernel modules emerges when developing new kernel functionalities. By this way, the possibility is given to load, test, unload, and modify some kind of prototype implementation in kernel space even multiple times without the constraint to recompile the whole kernel or reboot the whole system. Once the module is loaded into the kernel, other functionalities can be accessed. Regarding the soft handover implementation, all the new required kernel functionalities as Network Support, IPv6 and mobile IPv6 are provided as a kernel module or applied as an extension to an already existing one[82]. Another important kernel module used in the development of the soft handover and specially IPv6 packets management and modification during Routing Processes is *Netfilter Module.* Netfilter [81][85] is a module for packet mangling, outside the normal Berkeley socket interface. It introduces a series of hooks at five well-defined points while a packet traverses across the IPv6 routing process of an IPv6 node. When an IPv6 packet is processed by IPv6 routing stack and passes any of these hooks points, it is handled to the Netfilter module. An appropriate routine can be written to handle the packets in any of these hook points. The position of the IPv6 related hooks and their names are illustrated in Figure VII-1.
Every incoming IPv6 packet which is delivered from the link-layer to the IPv6 layer first encounters the NF_IP6_PRE_ROUTING hook. Then it enters the first routing part of the IPv6 stack, which decides whether the packet is destined for another node, or a local process. If it is destined for the node itself, it is hooked by NF_IP6_LOCAL_IN before being passed to the next higher layer processing.

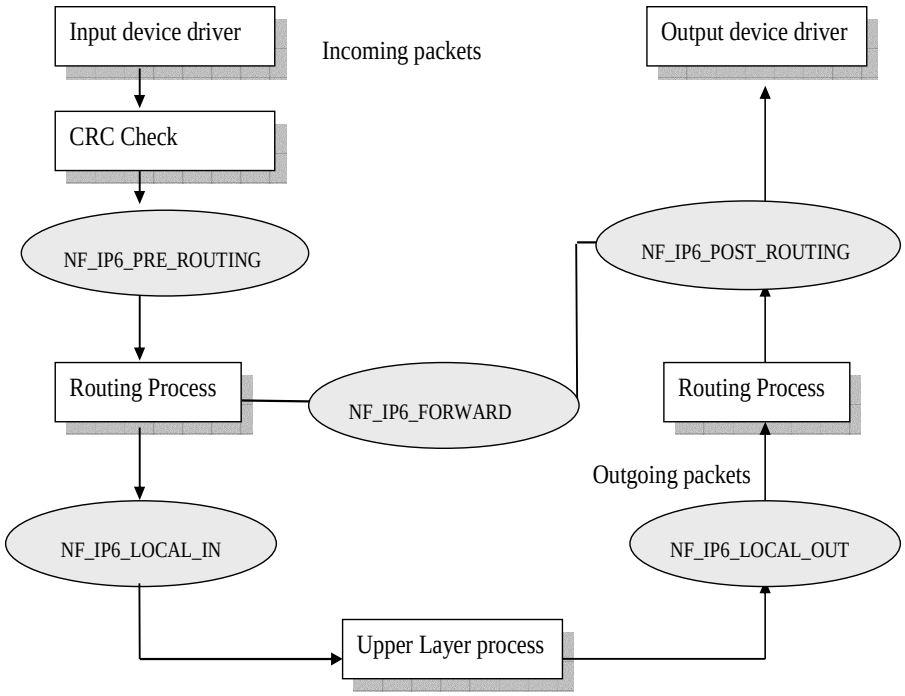


Figure VII-1 Packet filtering architecture in Linux 2.4.x

Otherwise, if it is destined to another node instead, the Netfilter module is called again via the NF_IP6_FORWARD hook. The packet then passes a final hook, the NF_IP6_POST_ROUTING hook, before being passed to the link layer again. The NF_IP6_LOCAL_OUT hook is called for packets that are created locally before being processed by the routing part of the IPv6 stack. Kernel modules can register listener at any of these hooks. A module that registers a function must specify the priority of the function within the hook; then when that netfilter hook is called from the core networking code, each module registered at that point is called in the order of priorities, and is free to manipulate the packet. The module can then perform a specific treatment and notify netfilter to perform one of five treatments with IPv6 packets:

1. NF_ACCEPT: continue traversal as normal.
2. NF_DROP: drop the packet; don't continue traversal.
3. NF_STOLEN: I've taken over the packet; don't continue traversal.
4. NF_QUEUE: queue the packet (usually for user space handling).
5. NF_REPEAT: call this hook again.

The traditional purpose of the Netfilter was to provide a framework for firewalling. With the further developing it proved to be a very flexible basis for various network control functions such as traffic scheduling, network address translation (NAT) or to enforce other advanced packet treatments.
In the SoH implementation, the Netfilter module is utilized for Downlink flow:

- The HA intercepts packets destined to MN Home address and tunnel them to MN Primary care of address.
- The D&M agent intercepts packets destined to MN PCoA, duplicate them, insert a DIO header and tunnel them to MN Local care of addresses.

For uplink flows:

- The MN intercepts packets generated by upper layer; duplicates them, inserts a DIO header and tunnels them thought its different interfaces to the D&M agent.

1.2. Mobile IP for Linux (MIPL) Environment

Because the evident interaction between IPv6 and mobileIPv6 stacks in Linux kernel is believed to be essential, the MIPL developers decided to implement all related mobile IPv6 functionality in kernel space until version 2.0.
Otherwise splitting the code into user and kernel level would require new interfaces and lead to extra complexity and overhead. The system is provided as a single kernel module, which can be dynamically inserted and removed from the kernel. The module provides mobile IPv6 functionalities for HA, CN and MN. Whether a node running the MIPL, daemon serving as HA, CN or MN, is defined via a special script files.
To allow dynamic loading and unloading of the module into the kernel, models for MIPL callable functions were introduced into the IPv6 code. This is provided through the “Mipglue” module. If, during the processing of a mobile IPv6 destination option, the IPv6 stack passes a stub, it checks whether the MIPL module is loaded and if so, the MIPL related function is called. The advantage of this approach is that the module can be unloaded, modified and reloaded into the kernel of a running system.
Figure VII-2 gives a rough overview of the MIPL general architecture. Several hooks were patched to the IPv6 stack allowing the “Mipglue” module to forward certain calls from IPv6 stack to the mobile IPv6 stack.
The way around, once the module is loaded into the kernel, other functionalities from the kernel code (in particular the IPv6 code) can be called directly. This avoids functionalities redundancy between IPv6 stack and MIPL stack which actually already exists in the IPv6 module.

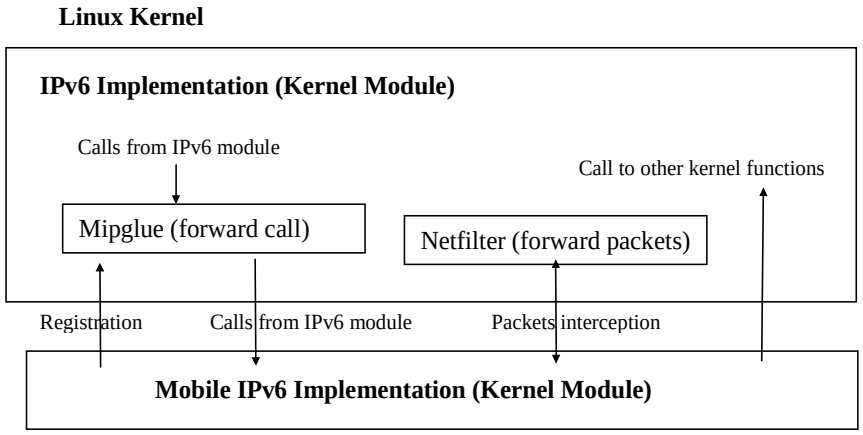


Figure VII-2 MIPL general architecture

2. Implementation Design

2.1. Assumptions and Limitations of the Platform

Our test bed is a prototypal implementation with the purpose to:

- Prove the general feasibility of MN multi interfaces management, soft handover bidirectional duplication and merging mechanisms and D&M agent coexistence with basic mobile IPv6 elements.
- Validate our simulation results obtained by Gemini2 simulator.

In particular, we do not claim to provide a full implementation of any of the aforementioned underlying architectures. We focus our job on the entities and functionalities required to realize the core idea of the proposed scheme and allow a real time video and audio demonstration on soft handover.

- D&M agent detection mechanisms: In order to broadcast the presence and the IPv6 address of the D&M agent, we exploit MAP option in RtAdv messages without modification. The drawback is that our mobile can considers all MAP in the networks as D&M agents.
- Handover initialization procedure: The handover process is initiated by script file which manage also the interfaces priorities to enable soft handover. The script file simulates the handover decision based on signal strength.
- IEEE 802.11b access routers structures. We do not use real 802.11b access points in our platform; we use wireless cards (802.11b Cisco Aironet card in Ad-Hoc mode). Each card has an ESSID and subnet IPv6 address.
- Integration of UMTS access routers. To perform a real heterogeneous test, we are integrating UMTS interface in MN and UMTS BSS in our platform, addition modification are necessary to update IPv6 driver of these cards and introduces IPv6 RtAdv support at UMTS driver.

2.2. D&M Router

The HA MIPL-based implementation can be used for the purpose of a D&M router but additional signaling and data management requirement are extended in the MIPL and IPv6 code. We describe in the following the data and control plane architecture extension used in D&M router implementations.

Duplication data process: In order to duplicate any packet destined to the MN, We have first to intercept it. The starting point of packet interception is the NF_IP6_PRE_ROUTING hook. The Modified MIPL daemon installs this hook in kernel space during loading process. The motivation to choose this hook is the need to check every incoming IPv6 packet before applying routing process. After the interception, we extract from this packet the IPv6 destination address and through Mipglue functions we send request to the DCT (hash table).
If there is a binding entry with PCoA equal to extracted Address and exists more that one LCoAs associated to this PCoA. That is means that the packet is destined to MN. At this moment the process stoles the socket and sends it to duplication process in MIPL space. This one extracts the current Sequence number from the binding entry, cerates a new DIO option header, and increments this sequence number. The process extends the socket that carries the IP packet with the size of the DIO and inserts this new option header.
Finally this process duplicates the resulting socket, encapsulates the packets in anew IPv6 header. Each duplicated packet will have different LCoA as destination address. Finally the resulting socket is rerouted to the final destination.

Merging Data Process: For the purpose of the merging process, we do not need hook or interception mechanisms. The MN carries the duplicated packets through a tunnel to the D&M agent. All packets that need to pass the merging mechanism will have the D&M router address as their destination IPv6 address. We first extend in IPv6 kernel space, the header parsing process, with DIO parsing support. When the IPv6 headers parsing mechanism detects a DIO in a packet, it extracts the sequence number. Through the mipglue, its sends this value and the source address of the packet to the merging mechanisms in MIPL space. The merging mechanism will determine using the MCT information whether the packet has been already received or not.
If the IPv6 packet has been received, the parsing mechanism in kernel space destroys the current socket; otherwise the parsing mechanism ignores this option header and continues the normal routing mechanism.

Signaling and Control plane: the MN sends also a signaling message (Merging solicitation to the D&M agent). The IPv6 parsing headers process is responsible of detecting these packets and sending them to the MIPL signal handling process. This one parses the signaling message, updates the MCT and DCT and generates merging advertisement to acknowledge the MN request. The Figure VII-3 depicts the D&M agent implementation architecture.

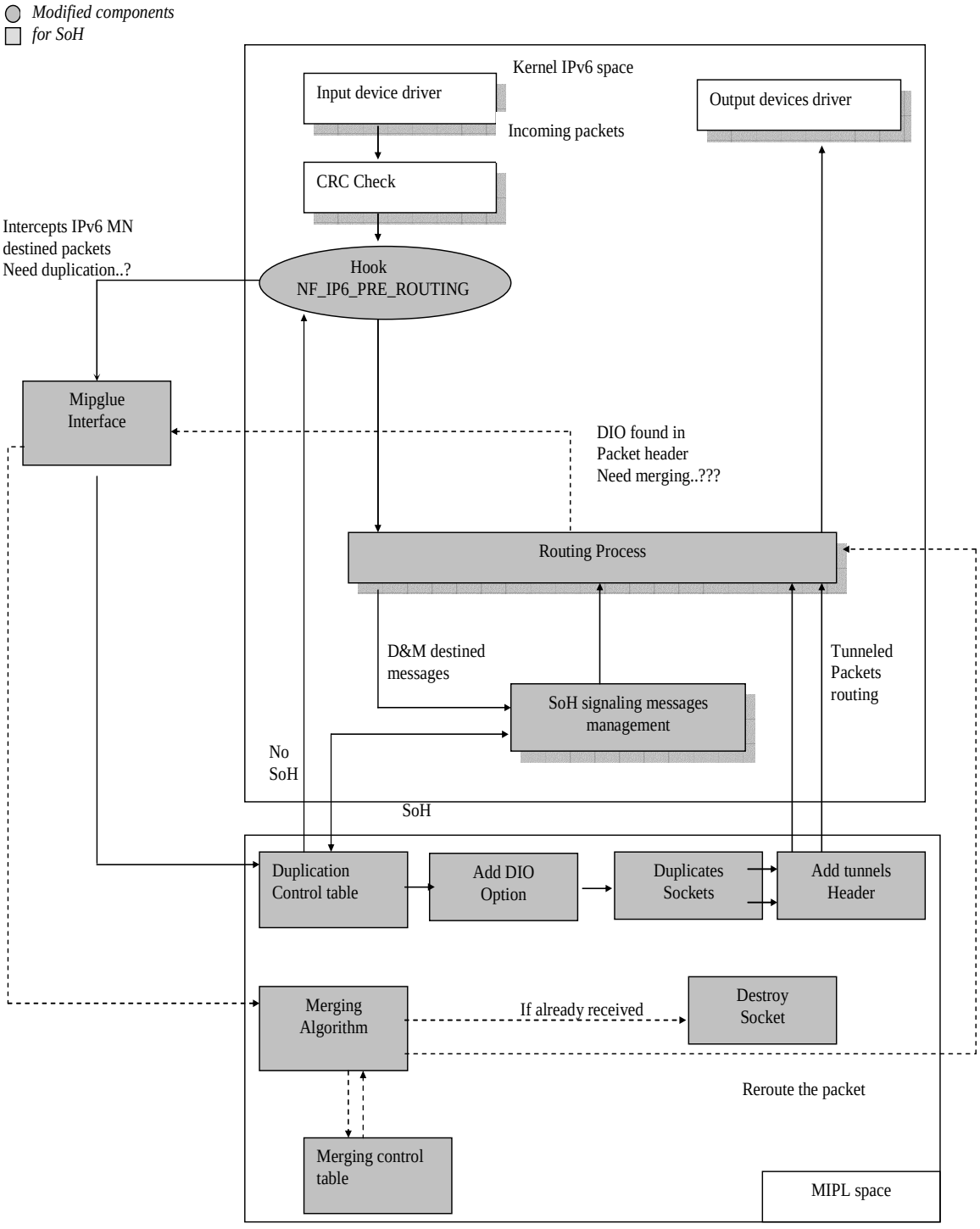


Figure VII-3 D&M router implementation outline.

2.3. Mobile Node

All required MN soft handover mechanisms are extended either in MIPL code, option header parsing process or default route management in the core of IPv6 routing stack. In following we describe the implementation details.

D&M agent discovery: As illustrated in chapter 3, ARs broadcast the IPv6 address of their respective D&M agent using the modified RtAdv daemon. The MN with soft handover capabilities, at the reception of the RtAdv message is able to correctly parse and analyze the MAP option in each message. Using this information the MN detects the D&M agent existence and extracts its corresponding IPv6 address. Using its primary interface identifier IID and the collected D&M agent address, the MN can auto-configure its Primary CoA.

Handover detection in multihoming situation: The Figure VII-4 gives an overview of data structure related to ARs management and movement detection in MIPL soft handover. The pointer Prim-router identifies the router serving currently as primary interface default route, the pointer second-router is the router serving as secondary interface default router in case of soft handover. The handover or interface disconnection can only be done with this second-router. The pointer next-router is an MIPL basic pointer which is temporarily assigned to the next handover-to router. A list of D&M routers is added using the neighbor discovery messages. It is used to hold relevant information such as current PCoA, lifetime, and the managed ARs for each D&M agent. In addition the AR structure is extended with several new fields, particularly LCoA field and pointer to the current D&M router. The handover process in MN is based on router events such as reception of RtAdv message. This function is also modified to avoid the handover to an AR used by the other MN interface and to mange the local registration within appropriate D&M agent.

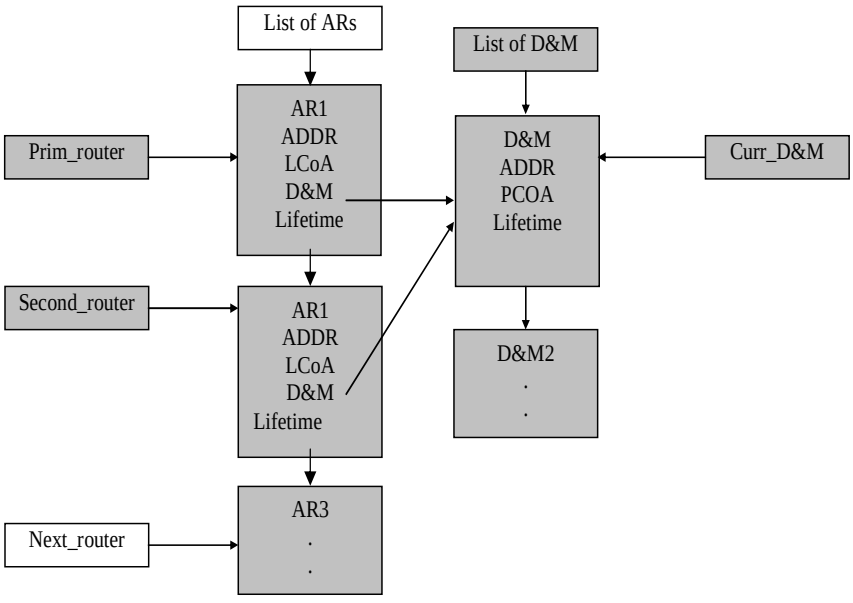


Figure VII-4 Overview of AR and D&M agent structures

Signaling messages: when the MN receives an RtAdv, it exploits ARs and D&M agents structures described above. It can using this information to updates the MCT tables, DCT tables, the routing table, generates RtSol messages and if necessary HA and CNs binding updates.

Duplication process: In order to duplicate any packet destined to the D&M agent, we have first to intercept it. The starting point of packet interception is the NF_IP6_LOCAL_OUT hook. The Modified MIPL daemon in MN installs this hook in kernel space at its loading process. The motivation to choose this hook is that MN duplicates only IPv6 packet locally generated. This duplication must be done before applying routing process. After the interception and if the MN is in soft handover state, the process sends the socket to duplication process in MIPL space. This one uses the current Sequence number to cerate a suitable new DIO option header and increments this sequence number. The process extends the socket that carries the IP packet with the size of the DIO and inserts this new option header. The process duplicates the resulting socket, encapsulates the packets in anew IPv6 header. Both duplicated packets will have the D&M agent IPv6 address as destination address.
Unlike the D&M agent, duplicated packets have the same destination but we need to route them through different routes. however in IPv6 routing table, we can not have two different entries with the same destination. IN order to fix this problem, we modify the MN routing table to support two default routes through different interfaces, we introduces a special IPv6 routing procedure to allow duplicated packets routing to the same destination through different interfaces. Finally we exploit these mechanisms to reroute the resulting duplicated sockets socket to the D&M agent.

Merging process: For the purpose of the merging process. We do not need any hook or interception mechanisms. The D&M agent carries the duplicates packets through a tunnel to the MN interfaces. All packets that need a merging mechanism will have the MN local care of address as destination IPv6 address. Thus, we first extend, as done for the D&M agent, the header parsing process with DIO parsing support. When the IPv6 headers parsing mechanism detects a DIO in a packet, it extracts the sequence number. Its sends this value and the source address of the packet through the “mipglue to the merging mechanisms in MIPL space. The merging mechanisms will determine using the information in MCT if the packets have been yet received or not.
If the IPv6 packet have been already received, the parsing mechanism in kernel space destroy the corresponding socket, otherwise the parsing mechanism ignore this option header and send packet to the upper layer. The Figure VII-5 depicts the MN full implementation architecture.

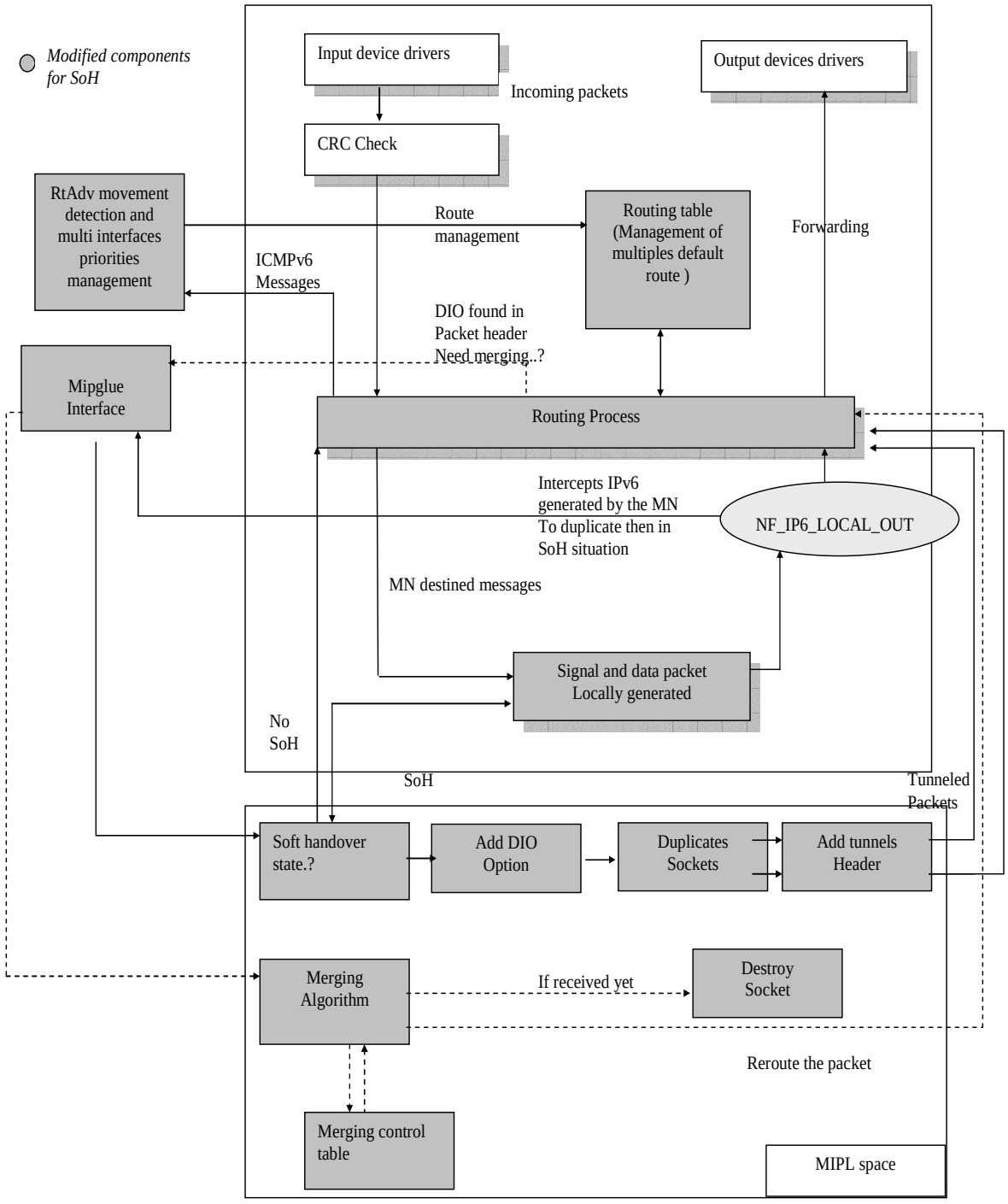


Figure VII-5 MN implementation architecture

3. Test Bed Configuration and Measurement Environment

The evaluation environment consists of hard, soft components and tools for the generation, monitoring and data analysis of different types of traffics. In order to evaluate the soft handover and mobile IPv6 handover approaches in a comparable environment, the testbed m generation and measurement tools keep the same configuration

The IPv6 test bed consists of seven nodes, as described in Figure VII-6, Two mobile stations and five fixed nodes. A manageable Ethernet hub interconnects the HA, D&M agent and three ARs. Access routers have two interfaces on Ethernet interface connected to the hub and 802.11 interfaces in mode Ad-Hoc used as wireless access point of MNs. Soft wares and IPv6 setup of the network components are described in bellow:

- Home Agent -HA/CN: is also serving as application server and CN. It is located in the core of the network with IPv6 address *fec0:106:2700::3/64*. Used SW: Linux Kernel 2.4.19 + MIPL 0.9.4.

- Duplication and Merging Agent-D&M: Located in the core of the network. With IPv6 address *fec0:106:2300::1/64*. Used SW: Linux Kernel 2.4.19 + MIPL 0.9.4 (setup as Modified HA) + HMIPv6 0.3 (Monash) + modified RtAdvD 0.7.2.

- Access Points -AP: They are three, with wireline and 802.11 wireless interfaces for each one. They broadcast RtAdv in wireless interfaces to indicate the address of D&M agents using MAP options. Soft: Kernel 2.4.19 + modified RtAdvD 0.7.2 (MAP option enabled).Their IPv6 addresses are : *fec0:106:1100::1/64, fec0:106:1200::1/64, fec0:106:1300::1/64.*

- Mobile Node1 – MN1: It has two 802.11 interfaces in Ad-Hoc mode in PCMCIA slots. When the MN is on the Home Network it has address *fec0:106:2700::4/64*. When MN travels to another network, within D&M agent range, it get a PCoA as Care of address and two local care of address to identify each one of their interfaces. Used SW: Linux Kernel 2.4.19 (modifications in default route management) +MIPL 0.9.4(Modified) + Monash HMIPv6 0.3 patch (Map option support and local registration option enabled) + Shell scripts to manage handovers scenarios and interfaces priorities.

- Mobile Node2 – MN2: Only a single 802.11 interface in Ad-Hoc mode.IPv6 home address *fec0:106:2700::4/64*. Used SW: Linux Kernel 2.4.19 +MIPL 0.9.4(Modified)+ Shell scripts to manage handovers scenarios.

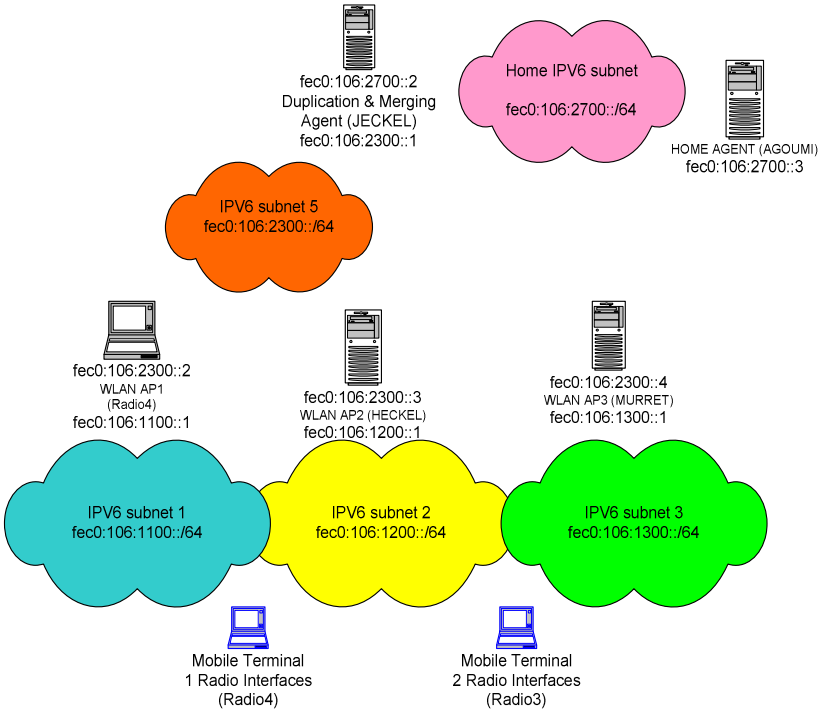


Figure VII-6 IPv6 platform

To evaluate soft handover mechanisms and perform comparison with basic mobile IPv6 handover scheme in described network, the following IPv6 tools are used as part of the common evaluation environment.

- **Netperf6**. For IPv6 load generation and data analysis, *netperf* [98] is a network benchmark tool that is commonly employed to measure various aspects of networking, such as data transmission and response time. *Netperf* consists of two parts: the netperf client and the server. When the client is executed with appropriate configuration options, the server is invoked automatically. A connection is established between client and server automatically.
- **Mgen6**. Mgen6 is composed of set of tools which allow us to take efficiency about IPv6 network using UDP flows. The tool *mgen6* [100] sends real time traffic pattern is such a way that the network can be filled with different types of load. Packets can be received using *drec* tools, which creates a log file with time stamps. This log can be analyzed by other tools to get statistics about packet losses, delay, jitter, and throughput and so on.
- **Trpr**. *TRace Plot Real-time* is a program which analyzes the output from *Mgen* log file and *tcpdump* packet sniffing. It supports a range of functionality for specific use of *gnuplot* graphing program.

- **Ping6**. This adaptation of ping uses the ICMPv6 protocol's mandatory ICMPv6 ECHO_REQUEST datagram to elicit an ICMPv6 ECHO_REPLY from the Correspondent. Datagram “ping” has an IPv6 header, and ICMPv6 header formatted as documented in RFC 2463.
- **VLC/VLS**. Video LAN Client [101] is a highly portable multimedia player for various audio and video formats (MPEG-1, MPEG-2, MPEG-4, DivX, mp3, ogg ...) as well as DVDs, VCDs, and various streaming protocols. It can also be used as a server to stream in unicast or multicast in IPv4 or IPv6 on a high-bandwidth network.
- **VIC**. The UCB/LBNL video tool, vic [102], is a real-time, multimedia application for video conferencing over the IPv4/IPv6. Vic is based on the Standard Real-time Transport Protocol (RTP)[99].
- **Ethereal.** For traffic monitoring, in particular for capturing and sniffing data and signaling message in wireless and wireline interfaces.

4. Measurements and Evaluation

To demonstrate the benefits of mobile IPv6 soft handover on both of wireless QoS and seamless handover, various practical experiences have been performed on different applications and transport protocols.
First experiences set aims to prove that the soft handover implementation done in the test bed is operational, bidirectional and allow simultaneously a transparent and seamless handover for both uplink and downlink data transmissions. The figure VII-7 describes the experience scenario in which three ARs are in triangular positions and two MN are performing circular handovers between these ARs. The first MN has two interfaces and performs soft handover; the second one has a single interface and uses basic mobile IPv6.

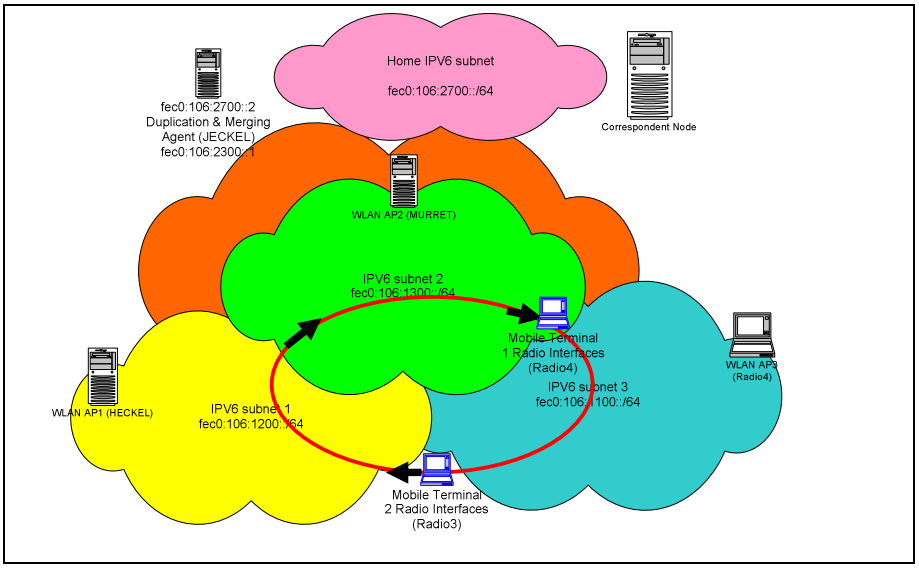


Figure VII-7 ICMPv6 experiences scenario

In following, a set of platform screen captures are exposed, each screen capture shows the concrete implementation of main control structures, data structures or simply one of soft handover network nodes.

Network control and data structure in MN idle state

First group of screen capture illustrates the stat of each component in the IPv6 access network before mobile node connection to the network. The figure VII-8 shows the AR2 snapshot. It illustrates in the left side the 802.11 wireless interface configuration parameters. In the right side, the RtAdv daemon dump shows the structure of RtAdv messages. The IPv6 address of the subnetwork and the IPv6 address of D&M agent via MAP option are broadcasted in the 802.11 interfaces.

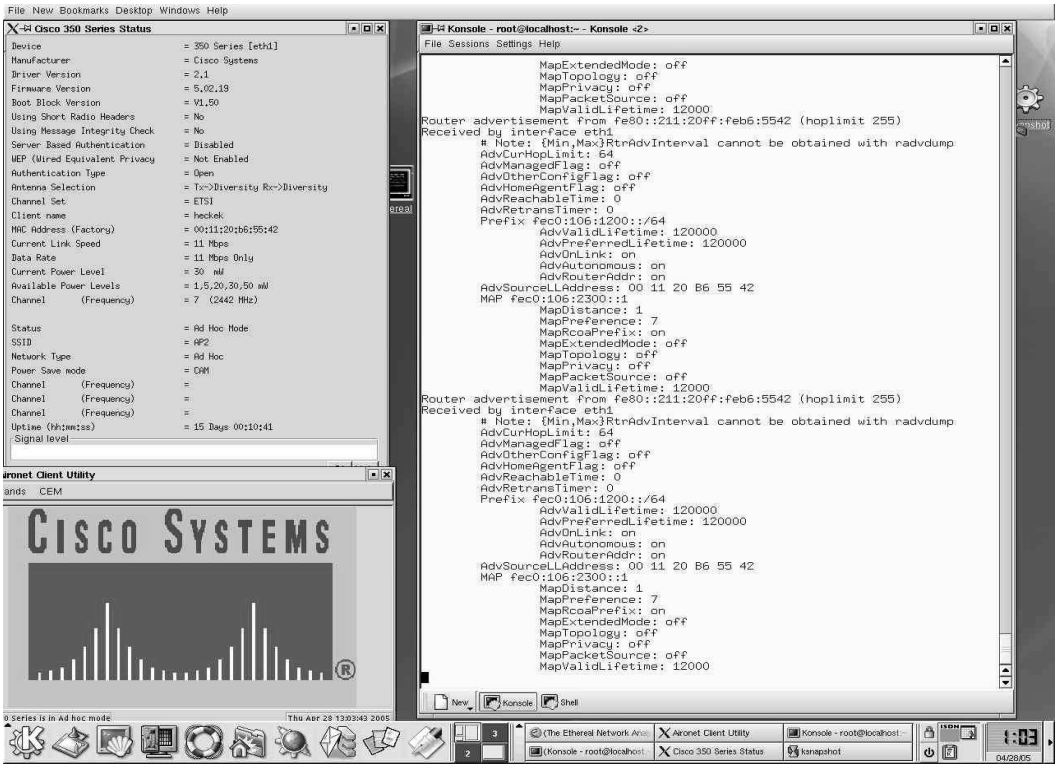


Figure VII-8 AR 802.11 configuration and MAP option in RtAdv

Network control and data structure in soft handover state

In following, a set of screen captures done in D&M agent, HA, and MN. They depict the information contained in the HA binding cache, the duplication control table and the data dumps of MN interfaces when this one is in soft handover stat between access router 1 and access router 2.

The figure VII-9 illustrates the MN binding cache entry in HA, this entry bind the MN home address with he primary CoA obtained from the D&M agent.

The figure VII-10 shows the DCT in the HA. In this table a MN binding entry binds the Primary CoA with MN two local CoAs created in each access router.

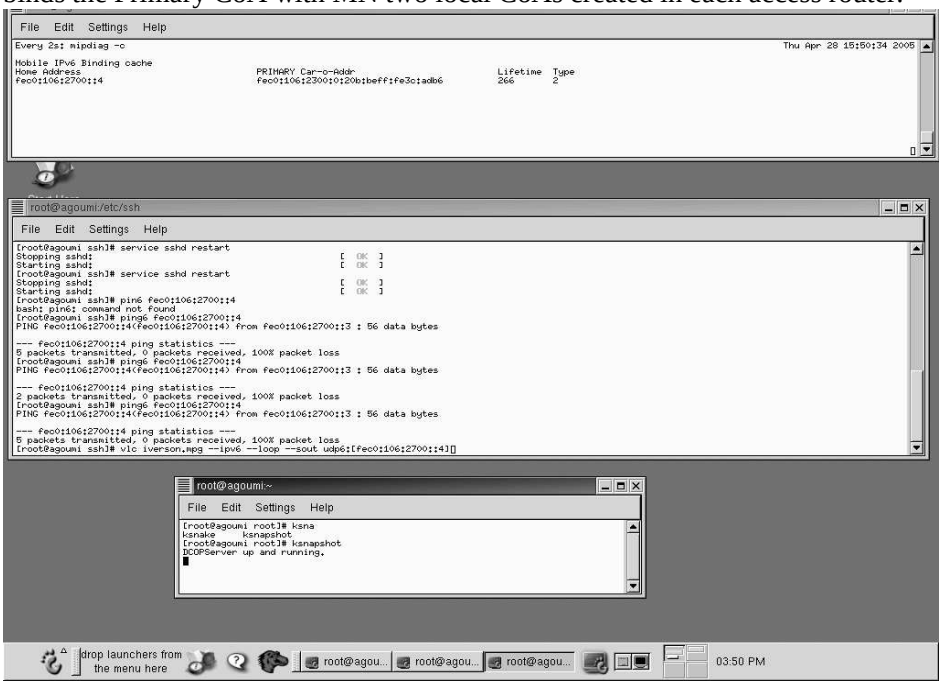


Figure VII-9 Home agent binding cache structure

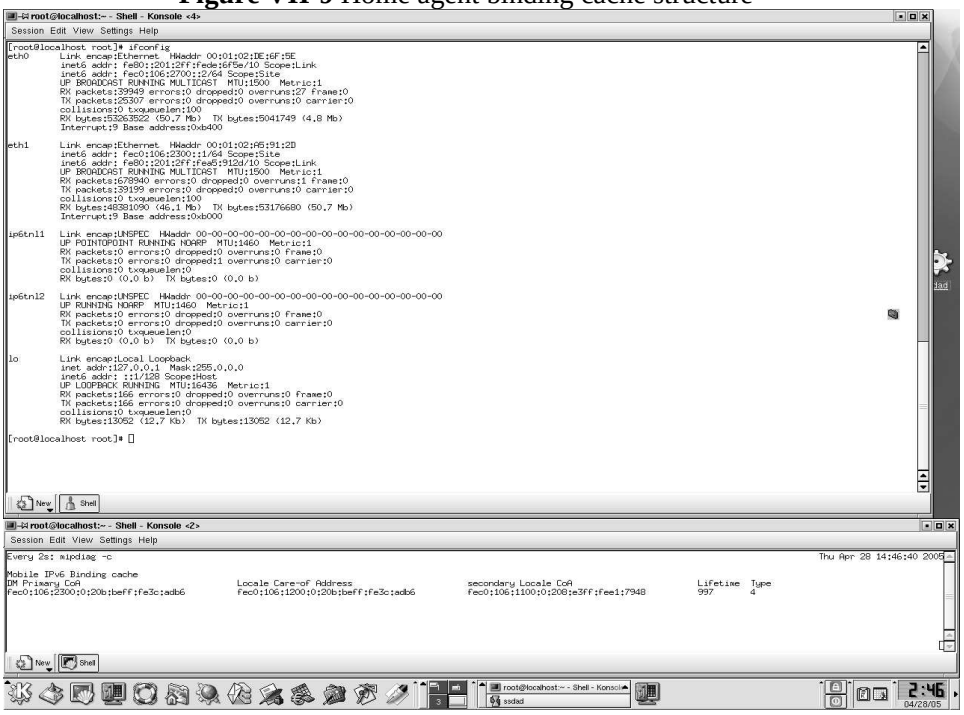


Figure VII-10 D&M agent DCT during a soft handover

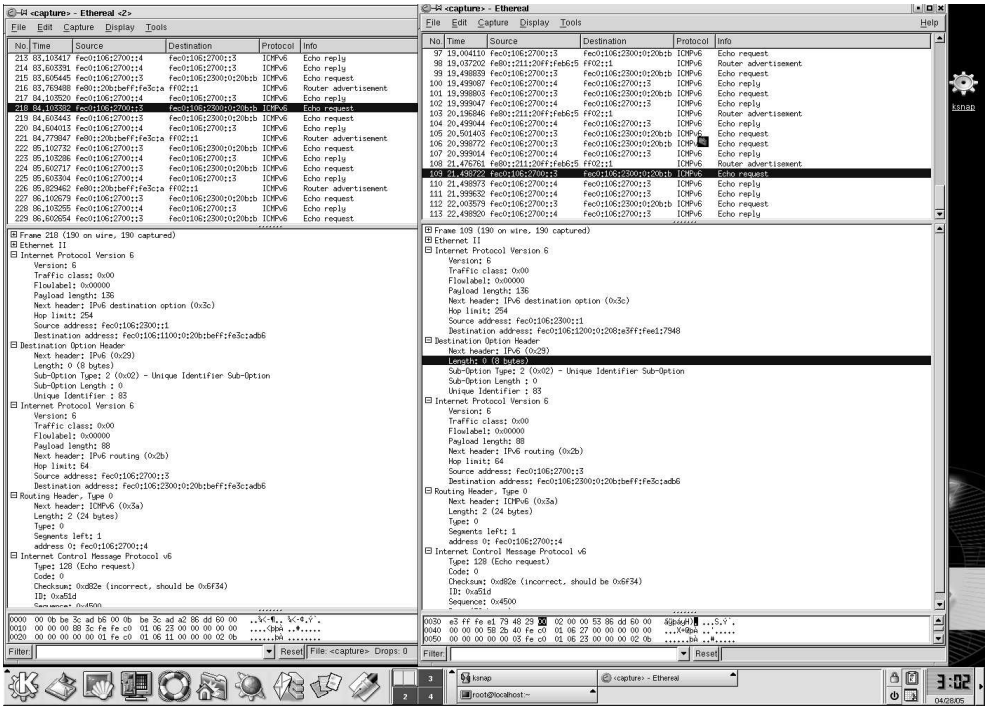


Figure VII-11 Duplicated Ping6 messages in MN

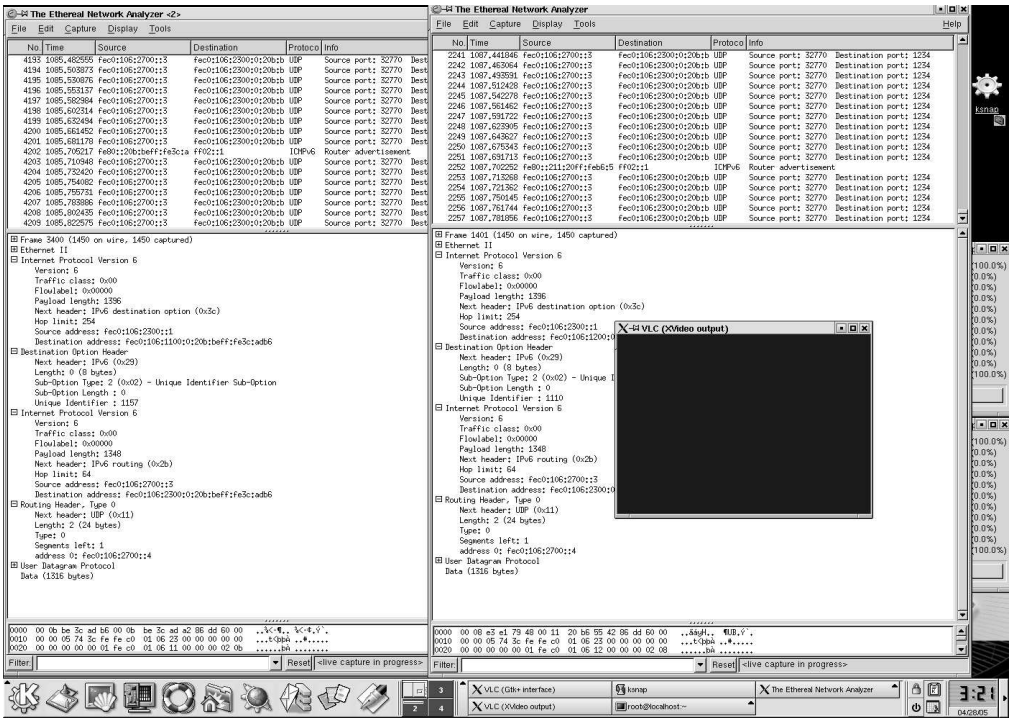


Figure VII-12 Duplicated VLC MPEG2 packets reception in MN

When the MN is in soft handover stat, it receives ICMPv6 and MPEG2 messages, through its two interfaces, from ping6 and VLC applications located in the CN. The figure VII-11 depicts ethereal dumps of MN interfaces. It shows simultaneous reception and emission of ICPMv6 echo request/reply messages between MN and the network through two interfaces. We can see that two duplicated packet carry same load but each one is tunnelled to a different MN Local care of address. In the same situation, figure VII-12 shows MN simultaneous reception of MPEG2 movie sent by other VLC client located in the core of the network.

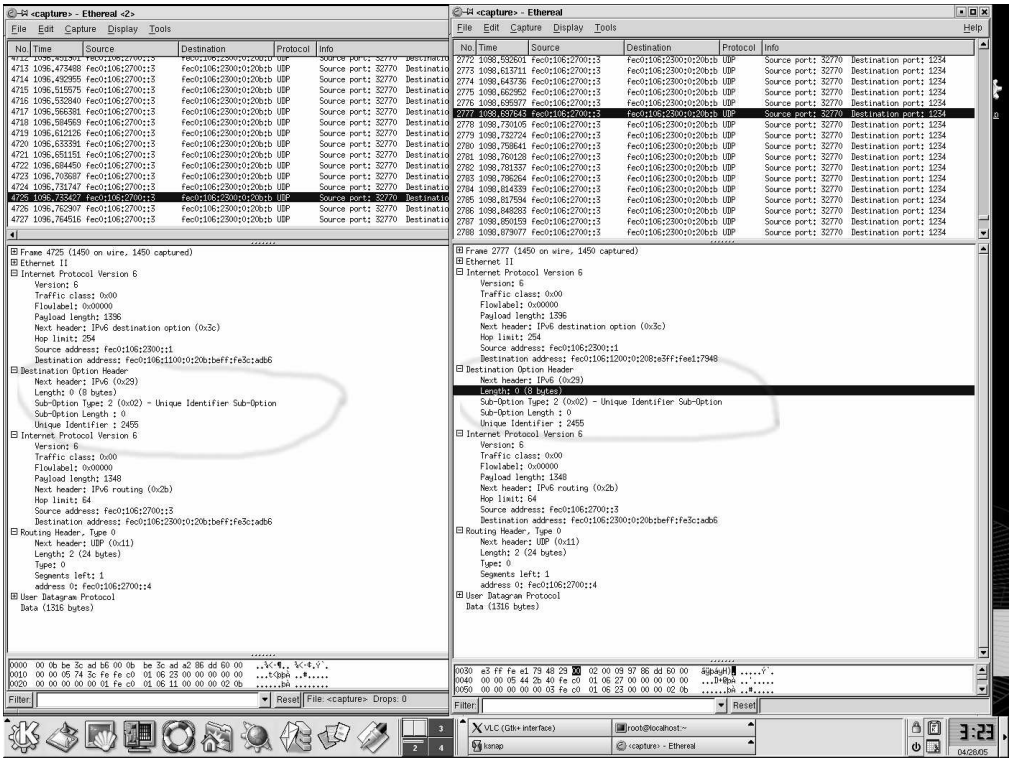


Figure VII-13 DIO illustration in duplicated UDP packets

Finally, the figure VII-13 depicts an Ethernet dump of duplicated UDP packets received by the MN through its two interfaces. It illustrates more precisely, the DIO option header introduced in each packet before the duplication in the D&M agent. Note that the sequence numbers of the two duplicated packet are simulars and the value is 83.

4.1. ICMP6 Bidirectional Flows

Figure VII-14 shows ICMPv6 packet loss ratio in ping6 session between CN, and MNs located at 5m far from ARs. In first experiences set, the CN pings the home address of single interface MN. It sends 20 ICMPv6 messages per second

to the MN. Each packet size is set 1400bytes. The CN considers that a message is correctly received if a single ICMPv6 acknowledgement message generated by the MN is correctly received.
During the session the MN performs handover between three ARs at different mobility rates. The same experiences scenarios are applied to the soft handover MN. However, for this experience, we activate the D&M router and the MN for each handover performs a bidirectional merging and duplication of packets.
Note that ping6 detects each duplicated ICMPv6 packet received from the IP layer. We use this tool, thus to prove that the handover is seamless, that duplication and merging mechanisms are bidirectional and that the merging mechanism is efficient to filter all duplicated packets for upper layers.

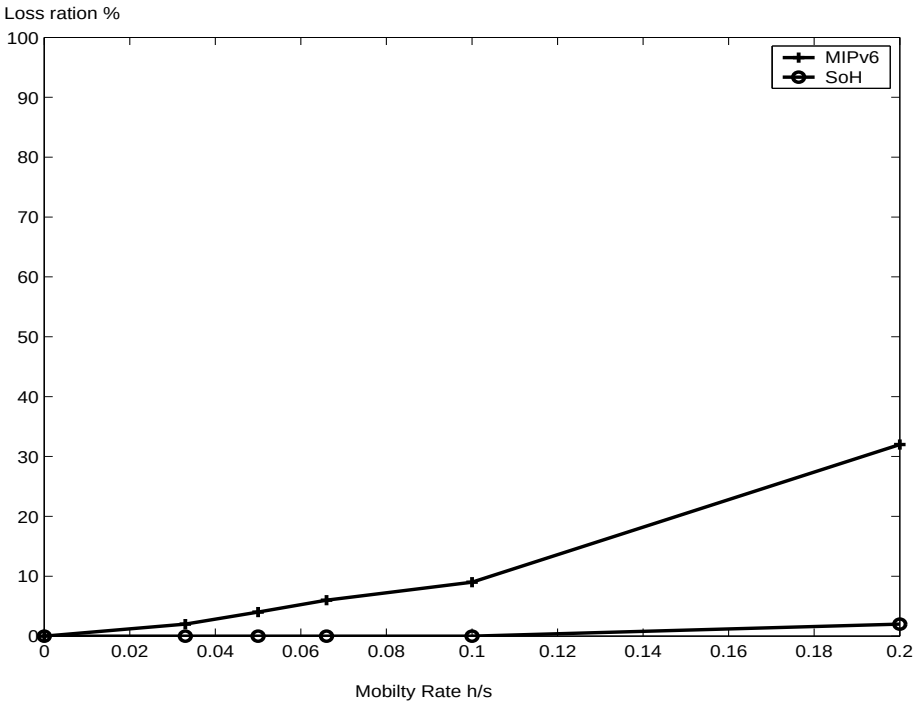


Figure VII-14 Loss ratio for bidirectional ICMPv6 traffic

Note that for the remind of experiences, RtAdv messages interval is set between 0.5s and 1,5s, However, the duplicate address detection is not performed after an IPv6 address autoconfiguration. We can see from Figure VII-14 that, the bidirectional ICMPv6 packet loss in mobile IPv6 increases with higher values of mobility rate. That is normal, each handover introduce MN disconnection and packet loss. Using the soft handover, there is no bidirectional packet loss, and in addition, what we can not read from the graph is that the ping6 did not register any duplication packet during soft handover sessions. These results validate our soft handover signaling feasibility. It validate also that the proposed merging mechanisms is efficient for merging duplicated packets in the two ways simultaneously.

4.2. UDP Performances

We use MGEN6 to generate and capturing UDP packet downlink from the CN to the MN and TRPR to interpret *drec* log files. The same experience parameters are used to evaluate the UDP performances using basic mobile IPv6 and soft handover.

Handover only measurements

The first experiences set aims to validate simulation results and to prove that soft handover allow a transparent and a seamless handover across IP access routers. The goal of these UDP-based experiences set is to isolate the handover process from the signal degradation phenomena and compare the performances of mobile IPv6 and soft handover on each of this phenomenon. We use MGENv6 to investigate the performances of the two approaches in the platform. The two MNs are located in the center of a triangle limited by ARs; the signal strength from each AR measured by the MN is ~ -62 dB. The Figure VII-15 illustrates the experience scenario.The same experiences setups are used to evaluate the two handovers approaches. The CN generates UDP flow to the two MNs at 125 kb/s.

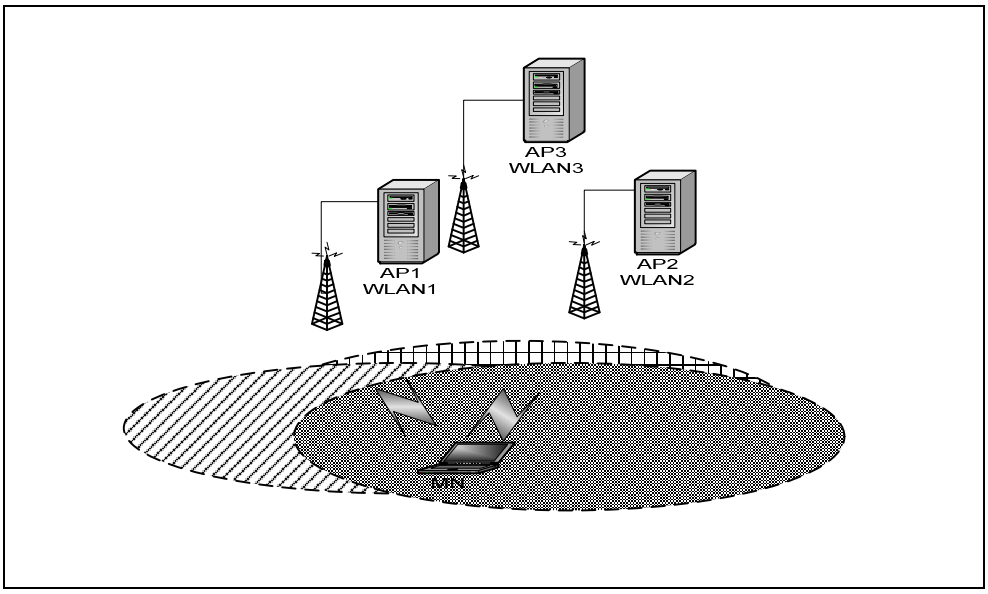


Figure VII-15 second UDP tests scenario

The figure V-16 shows the average reception throughput of two MNs. Considering the MN using a single connection to the network, and performing basic handover through ARs; the effect of each handover disconnection is clearly identified by a sudden disruption of reception throughput. Considering the MN that uses two connections simultaneously and soft handover to roam

between ARs, we register a stable throughput reception. The soft handover is completely transparent and has no effect on reception throughput.

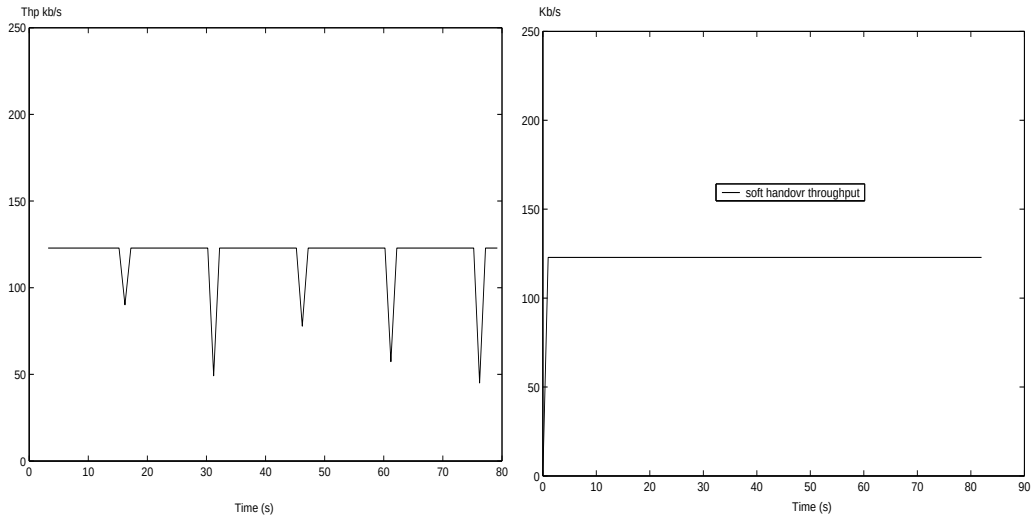


Figure VII-16 mobile IPv6 and soft handover effect in UDP throughput

Soft handover efficiency on signal degradation:

The second experiences set aims to evaluate the efficiency of duplication and merging mechanisms in improving overall wireless link when the MN is in border of two coverage areas.

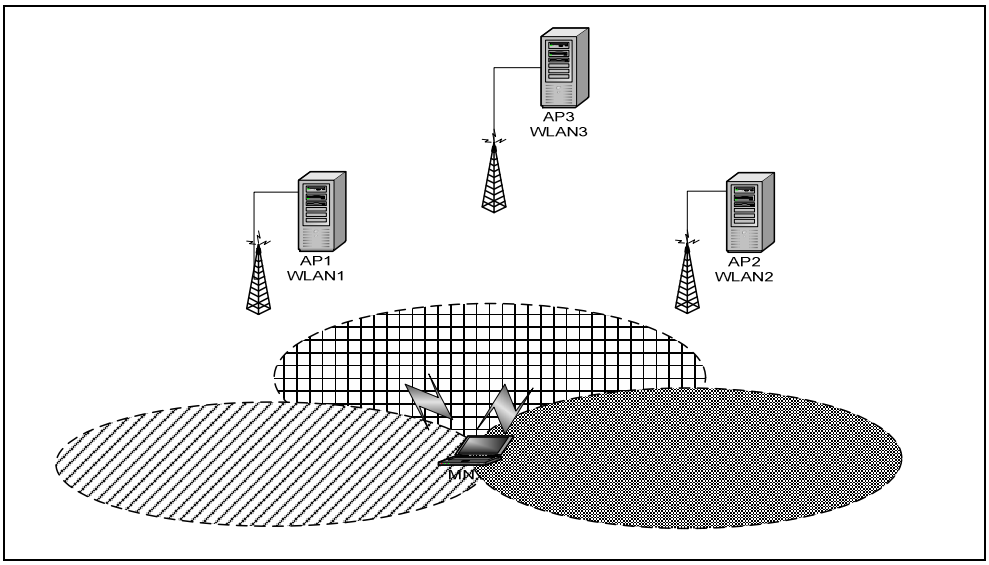


Figure VII-17 Signal degradation scenario

To perform these experiences, the MN is located far away from the three ARs, such as the signal strength from each AR and the MN is between -80~ -85 dB. First MN has only one connection to AR. The initial state of MN2 is two connections to AR1 and AR2 with duplication and merging mechanisms enabled. There is no roaming scenario between ARs and the Figure VII-17 illustrates the experiences scenarios. The figure V-18 shows the average reception throughput of two MNs.

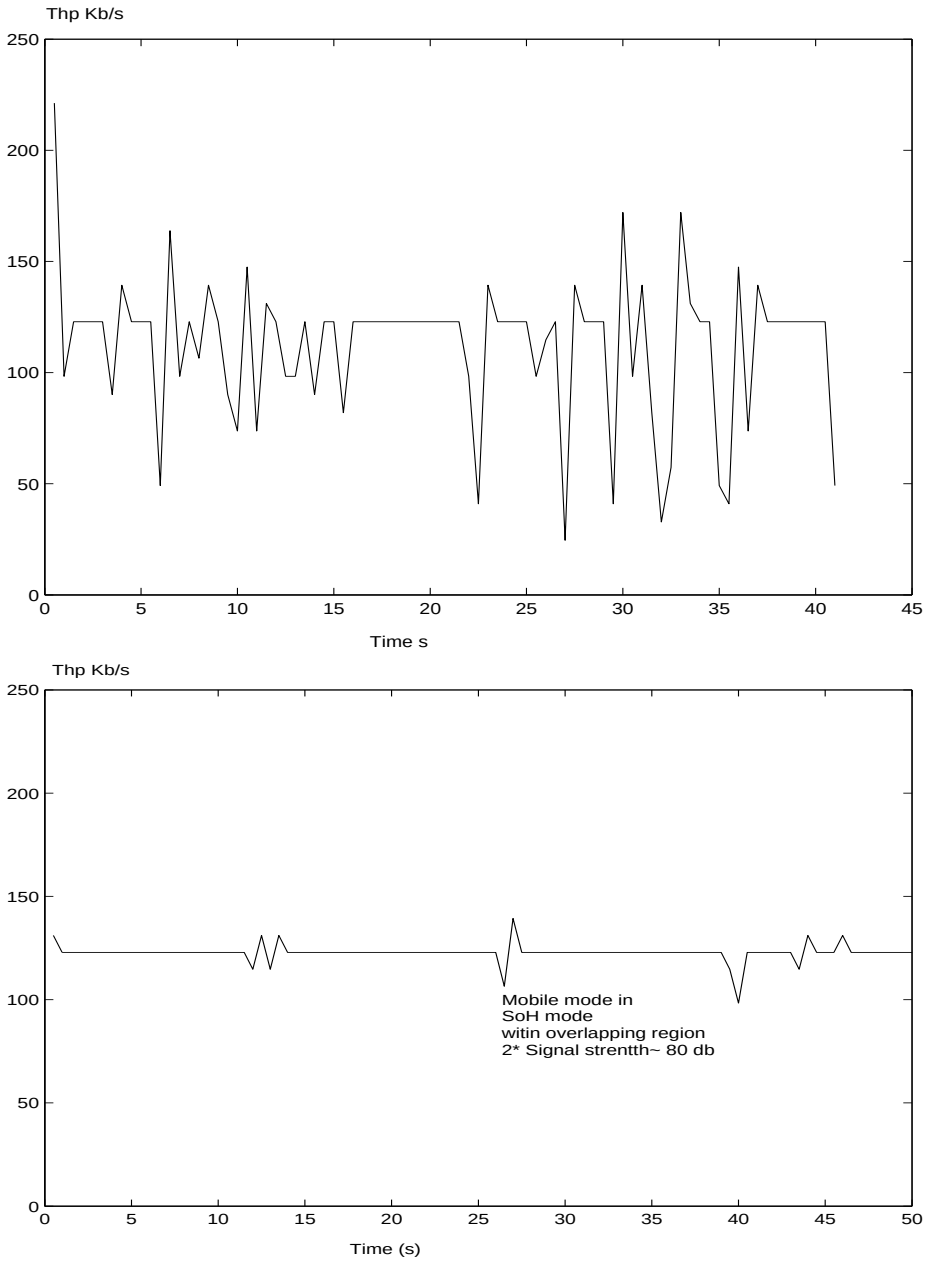


Figure VII-18 UDP throughput and signal degradation

Considering the MN using a single connection to the network, the UDP throughput at reception is perturbed by packets loss and MAC retransmissions caused by the weakness of the signal strength. Using two connections simultaneously in soft handover state, with duplication in D&M agent and merging enabled in MN. We register a better reception overall connection between the CN and MN (less packet loss and fewer jitters). Hence, soft handover improves sensibly the overall reception throughput quality.

The combined phenomena evaluation

More generally, to analyse the combined effect of handover and signal degradation, we keep both of the two MNs in their positions (Weak signal strength). Using a shell script we trigger 802.11b roaming at different mobility rates during the UDP session. The Figure VII-19 shows UDP packet loss ratio of soft handover and basic mobile IPv6 handover at different mobility rate.

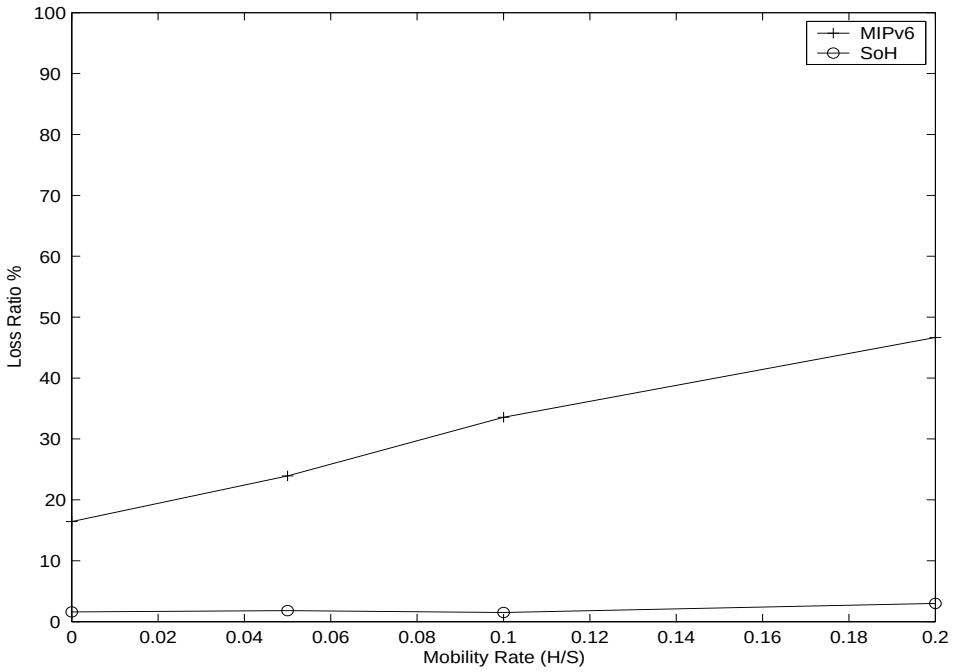


Figure VII-19 UDP loss rate measurements

Mobile IPv6 registers 18% of UDP packet loss without performing handovers. The weak signal strength is the unique responsible of this packet loss rate. When MN performs in addition handovers, the MN disconnection delay introduces additional packet loss rate, and a higher handover rate generates a higher packet loss rate, until 50% at 0.2 h/s. Using the soft handover the loss ration is stable on 3.5%. This value stay stable even the MN performs soft handover at 0.2 h/s.

5. Conclusion

We present in this chapter our experience and measurement results on the implementation of mobile IPv6 soft handover mechanisms. This implementation requires the introduction of new mechanisms and a set of new components in a basic mobile IPv6 test bed.

The first modified component is the mobile node. The soft handover mobile node compare to the basic mobile IPv6 node implement additional mechanisms and features. It has two wireless interfaces and is responsible for multiple interfaces dynamic priorities management in IPv6 layer, soft handover detection and D&M agent discovery, soft handover signaling management, and data bidirectional duplication, merging and special routing when multihomed.

The home agent maintains a mobile node home address/regional address table, it intercept packets sent to it and redirects them to the new mobile location. It uses the basic MIPL stack without modifications.

The Duplication and Merging Agent is a conventional IPv6 router locates in the core of the network, it maintains mobile regional address/local addresses, it intercepts packets sent to the mobile regional address and duplicates them to the actives interfaces. It allows also the merging of duplicated packets issued by the mobile node through its different interfaces.

Access routers: They have a wireless and wireline interfaces. They broadcast router advertisement RtAdv in wireless interfaces to indicate the address of D&M Agents using MAP options, and allow the mobile node to detect the handover in IP layer.

A set of measurements results are obtained through a set of basic and soft handover experiences preformed using the platform and two MNs. The main goals of these experiences are to validate the proposed protocol, confirm simulation results and depict the soft handover efficiency on reducing signal degradation and handover effects on real applications. We use Ping6 echo request/echo reply messages sent from the network toward the MN to measures the bidirectional packets loss and redundancy using soft handover and mobile IPv6. Measurement shows that the soft handover suppresses packet loss and no duplicated packets are registered by ping6 application. That proves that the soft handover is seamless, bidirectional and that the duplication and merging mechanisms are efficient.

UDP measurement splat in two main parts show that 1) soft handover compare to basic mobile IPv6 allows a transparent roaming of MN through overlapped coverage area 2) the duplication and merging mechanism is really efficient to improve the overall quality of wireless connection in the border of overlapping coverage areas.

CHAPTER 8

VIII. Conclusion & Outlook

In this dissertation the challenge of supporting mobile IPv6 soft handover in packet switched mobile networks is addresses. It is argued that today's wireless communication systems were developed and are evolving independently. They offer handover and mobility support but are based on homogeneous networking technology. Next generation networks is expected to gather and manage all these wireless communication technologies in the concept of Network of inter-networks. The internet architecture, protocols, and applications provide flexible services with universal and heterogeneous networking technologies at perceptively lower costs. Nevertheless, the IP protocol lacks the support of node mobility. The protocol was designed initially for fixed internet nodes. The dichotomy of IP address key (any MN IP address define simultaneously the node and its location in the network, in terms of physical connection) is the principal reason. Mobile IP is the basic, classical, and simplest solution to mange nodes mobility in IP-networks. When a node becomes mobile, the networks assign a temporary IP-address in addition to the home address. Additional mechanisms route indirectly all mobile node destined packets to its new location. This solution has been widely criticized for its drawbacks including the triangular routing and poor handover performances.

Mobile IPv6 is the evolution of mobile IP in IPv6 networks. It exploits the IPv6 features, such address autoconfiguration, and option Headers to improve the overall mobile IP performances. Moreover it provides additional mechanisms to fix natively the triangular routing problems. Nevertheless mobile IPv6 does not improve the mobile IP handover performances. Long mobile node disconnection when performing handover, can introduce data loss, additional end-to-end transmission delays and jitters, which perturb the communication.

In the dissertation different existing IP-based handover approaches are described and analyzed. The goal of this theoretical analysis is to show the consequences of the different IP handover techniques on an open transmission

session between a correspondent node located in the core of the network and the mobile node. The requirements for an efficient IP–based handover are identified.

It has already been recognized that the soft handover approach in circuit switched networks offer a number of attractive feature for seamless mobility support. No mobile disconnection means transparent handover, and path diversity means improvement of overall mobile node wireless link in overlapping region. The utilization of soft handover over heterogeneous networks through pure IP mobility mechanisms is an attractive perspective. Nevertheless it poses a number of challenges that have been insufficiently or not addressed se far. First for all, mobile IPv6 does not support multihoming management. Also, the network needs to intercept mobile node data flows, and duplicate them through mobile node different connections to provide path diversity. The heavy load of duplication process can not be done in the centralized home agent. We propose a new structure namely duplication and merging agent. It is an IPv6 router located in the core of the network. It performs multihoming signaling and data interception and duplication. There is no sequence number in IPv6 packet. Therefore, in order to identify duplicated packets, we introduced a new option header that allows duplicated packet identifications. The duplication process is asynchronous, because of the heterogeneity of potential wireless access technologies. Other Challenges arises from the mobile multi-interfaces handover management in IPv6. Basic IPv6 process allows the mobile to get only one default route. In routing table, we can not have more than on entry for one destination. A dynamic priorities process is proposed in the core of the MN to manage soft handover, and a set of modifications are proposed to fix the routing table anomaly. The duplication process also is implemented in the mobile to allow a bidirectional soft handover. Finally a merging process algorithm is proposed, it is located in the core of the mobile and the D&M router. It exploits the new option header to guarantee than not more than one copy of each packet will reach the transport layer.

To investigate the feasibility and performances of such complicated systems, a combined approach of simulations, implementation, measurements and analysis are used. From the performances evaluation, following statements can be made. First for all, it could be seen that it is possible to provide universal soft handover mechanisms in IPv6 layer. The usage of these mechanisms over two Wireless LAN interfaces allows a completely lossless and transparent handover. Moreover, it can improve the overall transmission quality in wireless side of connection and it does not require a special interaction with MAC layer to trigger the handover. Therefore this solution requires more additional wireless resources, during the soft handover data load between the mobile node and the D&M agent is simply duplicated. The implementation process done in mobile node and access network provides an engineering validation of our mechanisms. Mobile IPv6 soft handover provides really a multihoming management and soft handover without major modifications to basic mobile IPv6 stack. During mobile node implementation, we fix a number of IPv6 related routing issues generated by multi-interfaces simultaneous connection and uplink data duplications. Experimental measurements validate and confirm simulation results done in Gemini2 simulator.

Nevertheless, a number of open issues do still exist. In particular, as the manager of soft handover mechanisms, the D&M agent needs to interact with an end-to-end QoS mechanism and an access network resources management system. The security issue have to been mentioned, the soft handover introduce two more additional complexities the mobile IPv6 security mechanisms: The multihoming and the heterogeneity of wireless access technologies. Finally, additional measurements and simulations work are necessary to determine more precisely the effect of soft handover on heterogeneous wireless access technologies and the soft handover initiation criteria and thresholds.

REFERENCES

[1]. IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," P802.11D6.2, Edition 1999.

[2]. IEEE Std 802.11b, 1999 Edition. Information technology- Telecommunications and information exchange between systems – local and metropolitan area networks- Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher speed physical layer (PHY) extension in the 2.4 GHz band.

[3]. European Telecommunications Standard Institute, ETSI HIPERLAN/1 standard, EN 300 652:1998, "Broadband radio access networks (BRAN); High-performance radio local-area network (HIPERLAN) Type 1". Functional specification.

[4]. E. P. Vasilakopoulou, G. E. Karastergios" Design and implementation of the HiperLan/2 protocol ". *ACM SIGMOBILE Mobile Computing and Communications Review*, April 2003

[5]. Bluetooth Specifications, Bluetooth SIG at http://www.bluetooth.com/.

[6]. E Ferrero, F.Potorti "Bluetooth and WIFI Wireless Protocols : A survey and A Comparison", *IEEE Wireless communications magazine*. February 2005.

[7]. X. Lagrange, P. Godlewski, S. Tabbane "Réseaux GSM" Edition *Hermes* ,5eme edition 2000.

[8]. 3GPP TS 23.009, "Handover Procedures". GSM

[9]. T. Halonenm J, Romero, J.Melero "GSM, GPRS and EDGE Performance ".*edition Wiley* 2003.

[10]. 3GPP TS 23.101, V4.0.0, " General UMTS architecture ", April 2001

[11]. H. Holma, A. Toskala, "WCDMA for UMTS: Radio access for third general mobile communication". *John Wiley &Sons* 2000.

[12]. Glisic, Savo G, Leppanen, Pentti A " Wireless communications : TDMA versus CDMA" *Kluwer Academic , 1997, p. 540 - ISBN : 079238005*

[13]. Darpa Internet Program. " Internet Protocol" RFC 791. September 1981.

[14]. C. Horning “A Standard for the Transmission of IP Datagrams over Ethernet Networks” FRC 894, 1984.

[15]. J. Mogul “Internet Standard Subnetting Procedure” RFC 950, 1985

[16]. R. Braden. “Requirements for Internet Hosts – Communication Layers”. RFC 1122, October 1989.

[17]. C.Perkins., “ IP encapsulation within IP” , IETF, RFC 2003, 1996.

[18]. Cui Hongyan; Cai Yunlong; Wang Ying; Zhang Ping; “ Design and implementation of all IP architecture for beyond 3G system“. *Personal, Indoor and Mobile Radio Communications, 2004. IMRC 2004*. 15th IEEE International Symposium on Volume 1, September 2004

[19]. Zahariadis, T.B.; Vaxevanakis, K.G.; Tsantilas, C.P.; Zervos, N.A.; Nikolaou, N.A.; “Global roaming in next-generation networks”. *Communications Magazine, IEEE Volume 40, Issue 2*, February 2002

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

[21]. C. Perkins **“**Mobile networking through Mobile IP”. *Internet Computing, IEEE Volume 2, Issue 1*, January 1998

[22]. H. Chaskar, Ed “Requirements of a Quality of Service (QoS) Solution for Mobile IP “, RFC 2582, September 2003.

[23]. A. Chheda, “A performance comparison of the CDMA IS-95B and IS-95A soft handoff algorithms,” *Vehicular Technology Conference, 1999 IEEE 49th*, Vol. 2, pp. 1407-1412, 1999

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

[25]. R. Hinden and S. Deering. IP Version 6 Addressing Architecture. RFC 2373, July1998.

[26]. P. Nesser, “ An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA “ RFC 1917, February 1996

[27]. IEEE. Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority. IEEE Standards tutorials. *http://standards.ieee.org/regauth/oui/tutorials/EUI64.html*

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

[29]. A.Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). RFC 2463, December 1998.

[30]. S. Deering. ICMP Router Discovery Messages. RFC 1256, September 1991.85.

[31]. S. Thomson, Bellcoro, T. Narten, “IPv6 Stateless Address Autoconfiguration.” December 1998

[32]. R.Droms, J. Bound and all “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)” RFC 3315. July 2003

[33]. S. Kent, R. Atkinson. “IP Authentication Header“, RFC 2402, November 1998.

[34]. A. conta, S. deering “Generic Packet Tunneling in IPv6 Specification”. RFC 2473 December 1998.

[35]. J. Postel “ User Datagram Protocol” RFC 768 , August 1980.

[36]. Peng Sun; Sung, S.Y, “Enhancement of binding update for mobile IP” *Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference on* November 2002 Page(s):542 – 543.

[37]. Johnson D., Perkins C. Optimization in Mobile IP, IETF, Draft-ietf-mobileip-optim-11.txt, September 2001.

[38]. D. Johnson, C .Perkins, J. Arkko, “Mobility Support in IPv6” Internet Eng Task Force RFC 3775, June 2004..

[39]. Vaughan-Nichols, S.J. ”Mobile IPv6 and the future of wireless Internet access”. *Computer Volume 36, Issue 2,* February. 2003 Page(s):18 –20

[40]. Nikander, P.; Arkko, J.; Aura, T.; Montenegro, G.; “Mobile IP version 6 (MIPv6) route optimization security design”. *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th Volume 3,* 6-9 October. 2003 Page(s):2004 - 2008 Vol.3

[41]. C. Castelluccia, “HMIPv6: A Hierarchical Mobile IPv6 Proposal,” *ACM Mobile Computing and Communications Review, vol. 4, no. 1, pp. 48–59*, January 2000.

[42]. H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, “Hierarchial Mobile IPv6 Mobility Management (HMIPv6),” IETF Draft, June 2004, work in progress.

[43]. S.-H. Hwang, B.-K. Lee, Y.-H. Han, and C.-S. Hwang, “An Adaptive Hierarchical Mobile IPv6 with Route Optimization,” *in Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference 2003(VTC’S03), vol. 3*, 2003, pp. 1502–1506.

[44]. Campbell AT., Gomez J., IP Micro-Mobility Protocols, *ACM SIGMOBILE* vol.4,no.4, pp 45-54, October 2001.

[45]. Vivaldi, B. Ali, H. Habaebi, V. Prakash, and A. Sali, “Routing Scheme for Macro Mobility Handover in Hierarchical Mobile IPv6 Network,” in Proceedings of the *4th National Conference on Telecommunication Technology 2003 (NCTT 2003)*, 2003, pp. 88–92.

[46]. Eom DS., Sugano M., Murata M., Miyahara H. Performance Improvement by Packet Buffering in Mobile IP Based Networks, *IEICE Transactions on Communications*, vol. E83-B, pp. 2501-2512, November 2000.

[47]. K. Omae, T. Ikeda, M. Inoue, I. Okajima, and N. Umeda, “Mobile Node Extension Employing Buffering Function to Improve Handoff Performance,” in *Proceedings of the The 5th International Symposium on Wireless Personal Multimedia Communications 2002*, vol. 1, 2002, pp. 62–66.

[48]. Koodli R., Perkins C., A Framework for Smooth Handovers with Mobile IPv6, IETF, draft-koodli-mobileip-smoothv6-00.txt, juillet 2000

[49]. Perkins C., Wang KY., Optimized Smooth Handoffs in Mobile IP, *Proceedings of the fourth IEEE Symposium on Computers & Communications*, juillet 1999.

[50]. K. Govind, R. Chalmers, C. Perkins, “Buffer management for smooth handovers in IPv6” Internet Draft, March 2001.

[51]. M. Sulander, T. Hamralainen, A. Viinikainen, and J. Puttonen, “Flowbased Fast Handover Method for Mobile IPv6 Network,” in *Proceedings of the 59th Semiannual IEEE Vehicular Technology Conference(VTC’S04)*, May 2004.

[52]. R. Koodli, “Fast Handovers for Mobile IPv6,” *IETF draft*, January 2004, work in progress.

[53]. M. Torrent-Moreno, X. Perez-Costa, and S. Sallent-Ribes, “A Performance Study of Fast Handovers for Mobile IPv6,” in *Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks*, 2003, pp. 89–98.

[54]. K. El Malki, H. Soliman ” Simultaneous Bindings for Mobile IPv6 Fast Handovers , Internet Draft October 2003

[55]. S. Faccin, B. Patil, R.Purnadi, S. Sreemanthula “ Enhancements to Bi-directional Edge Tunnel Handover for IPv6”, Internet Draft, September 2001 .

[56]. X. Perez-Costa, M. Torrent-Moreno, and H. Hartenstein, “A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and Their Combination,” *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 4, pp. 5–19, 2003.

[57]. R. Hsieh, A. Seneviaratne, H. Soliman, and K. El-Malki, “Performance Analysis on Hierarchical Mobile IPv6 with Fast-handoff over End-to-End TCP,” in *Proceedings of the IEEE Global Telecommunications Conference 2002 (Globecom’02)*, vol. 3, 2002, pp. 2488–2492.

[58]. R. Hsieh, Z. G. Zhou, and A. Seneviaratne, “S-MIP: A Seamless Handoff Architecture for Mobile IP,” in *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Socities (INFOCOM 2003)*, vol. 3, 2003, pp. 1774–1784.

[59]. R. Hsieh and A. Seneviaratne, “A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP,” in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking 2003 (Mobicom’03)*, 2003, pp. 29–41.

[60]. Postel J., Transmission Control Protocol, IETF, RFC 793, 1981.

[61]. Stevens WR., *TCP/IP Illustrated Volume 1: The Protocols*, Addison-Wesley, Longman, Reading,Massachusetts, 1994.

[62]. H. Balakrishnan, S.Seshan, R.H. Katz “Improving reliable Transport and handoff performance in cellular wireless networks”. ACM wireless networks, December 1995.

[63]. K. Fall, S. Floyd “Simulation-based comparisons of Tahoe, Reno and SACK TCP” ACM SIGCOMM Computer Communication Review Volume 26 , Issue 3 July 1996 PP 5 - 21 .

[64]. Mathis M., Mahdavi J., Floyd S., Rmanow Q., TCP Selective Acknowledgement Option, IETF, RFC 2018, October 1996.

[65]. Doo Seop Eom, HeyungSub Lee, Masashi Sugano, Masayuki Murata, Hideo Miyahara. “Improving TCP handoff performance in Mobile IP based networks”. *Computer Communications 25(7): 635-646* (2002).

[66]. Fladenmuller A., De Silva R., The effect of Mobile IP handoffs on the performance of TCP, *ACM Mobile Networks and Applications*, 1999.

[67]. Ihara, T.; Ohnishi, H.; Takagi, Y.; “Mobile IP route optimization method for a carrier-scale IP network”**.** *Engineering of Complex Computer Systems, 2000. ICECCS 2000. Proceedings. Sixth IEEE International Conference* on 11-14 September. 2000 Page(s):120 - 121

[68]. Hartenstein H., Jonas K., Liebsch M., Schmitz R., Stiemerling M., Westhoff D., Performance of TCP in the Presence of Mobile IP Handoffs, *ICT 2001, IEEE International Conference on Telecom*, Bucharest, Roumanie, juin 2001.

[69]. Moret Y., Bonnet C., Gauthier L., Knopp R., Process and Apparatus for Improved Communication between a Mobile Node and a Communication Network, Office Européen des Brevets, n° 02368057.2, août 2002.

[70]. Zhang T., Chen JC., Agrawal P., Distributed soft handoff in all-IP wireless networks, *Proceedings of IEEE International Conference on Third Generation Wireless and Beyond (3Gwireless'01)*, San Francisco, CA, pp. 460-465, Mai 2001.

[71]. Farouk Belghoul Yan Moret, Christian Bonnet “A Multilevel Hierarchical topology of DM agents for MIPv6 Soft handover ” *World Wireless Congress SANFRANCISCO, USA 2004* PP 56-60

[72]. Farouk Belghoul Yan Moret, Christian Bonnet " Performance comparison and analysis on MIPv6, fast MIPv6 bi-casting and Eurecom IPv6 soft handover over IEEE802.11b " *59 IEEE VTC, MILAN 2004 Vol.5 PP 2672- 2676*

[73]. Farouk Belghoul Yan Moret, Christian Bonnet " Performance analysis on IP- based soft handover across ALL-IP wireless networks" *IWUC, PORTO,* Portugal 2004

[74]. Farouk Belghoul Yan Moret, Christian Bonnet " IP-based handover management over heterogeneous wireless networks" *LCN 2003, 28th Annual IEEE Conference on Local Computer Networks*, October 20-24, 2003, Bonn, Germany PP 772- 773

[75]. Farouk Belghoul Yan Moret, Christian Bonnet "Eurecom IPv6 soft handover:" ICWN 2003, *International Conference on Wireless Networks*- June 23th - 26th, 2003 - Las Vegas, USA PP 169-174

[76]. A. G. Gleditsch and P. K. Gjermshus. The Linux Cross-Reference, August 2001.*http://lxr.sourceforge.net/.*

[77]. GO/Core project at HUT Telecommunication and Multimedia Lab. Mobile IP for Linux (MIPL) mipv6-0.9-v2.4.7. http://www.mipl.mediapoli.com/.]

[78]. Sami Kivisaari. MIPL Technical Specification Tik-76.115, March 2000. url:*http://www.soberit.hut.fi/tik-76.115/9900/palautukset/groups/MIPL/su/palautus3.html*

[79]. The Linux Documentation Project, 2002. *http://www.tldp.org/docs.html.*

[80]. Pedro Roque and Lars Fenneberg. RADVD – Router Advertisement Daemon, November 2001. *http://v6web.litech.org/radvd/.*

[81]. Rusty Russell. Linux netfilter Hacking HOWTO, 2001. *http://www.netfilter.org/unreliable-guides/netfilter-hacking-HOWTO/.*

[82]. W. Stevens and M. Thomas. Advanced Sockets API for IPv6. RFC 2292, February 1998.

[83]. Harald Welte. SKB - Linux Network Buffers, October 2000. *http://www.gnumonks.org/ftp/pub/doc/skb-doc.html.*

[84]. Monash patch 0.3 for MIPL0.9.3 hierarchical architecture support. *http://www.ctie.monash.edu.au/ipv6/hmipv6.htm*

[85]. K. Wehrle and co, "The Linux Networking Architecture, Design and implementation of network protocol in the Linux kernel ".*Prentice-Hall 1st ed. ,* 2004.

[86]. R. Nelson, G. Daley and N. Moore. "Implementation of Hierarchical Mobile IPv6 for Linux", *in the proceedings of The Sixth International Symposium on Communications Interworking* (IFIP Interworking 2002), October 2002.

[87]. R. Wakikawa, K. Uehara, T. Ernst, “Multiple Care-of Addresses Registration”, draft-wakikawa-mobileip-multiplecoa-02.txt (obsolete).

[88]. N. Montavont, T. Noël, M. Kassi-Lahlou, " MIPv6 for Multiple Interfaces", draft-montavont-mobileip-mmi-01.txt, *Internet Engineering Task Force Draft*, October 2003

[89]. akikawa R., Uehara, K. and T. Ernst, "Multiple Care-of-Address Registration on Mobile IPv6", (draft-wakikawa-mobileip-multiplecoa-03.txt), Internet Draft, IETF, June 2004, Work in Progress.

[90]. Andrea Travasoni, “ Description of Tilab proposal to support Multi-homing by extending MIPv6 protocol”, WP2-tm, Daidalos Cons 2004 .

[91]. C. Bonnet; H. Callewaert, L.Gauthier, R.Knopp, A. Menouni, Y. Moret “ Open-Sourece experimental B3G Networks Based on Software-Radio technology”, *Software defined radio technical conference and produce exposition*, Orlando (Floride,USA), November 2003.

[92]. X. Yang, S. Ghaheri-Niri and R. Tafazolli, “Evaluation of soft handover algorithms for UMTS,” *Personal, Indoor and Mobile Radio Communications, 2000 11th IEEE International Symposiumon, Vol. 2,* pp. 772-776, 2000

[93]. Kevin Fall and Kannan Varadhan, editors. Ns notes and documentation. The VINT project. UC Berkeley, LBL USC/ISI, and Xerox PARC, February 2000. Available from *http://www-mash.cs.berkeley.edu/ns*

[94]. Opnet modeler: *http://www.opnet.com/products/modeler/home.html*

[95]. Pew, John A, “Guide to Solaris (2.1)”, Ziff-Davis Press , 1993, p. 625 - ISBN : 1562760874.

[96]. Linux Redhat distribution *http://www.redhat.com*

[97]. MIPL Mobile IPv6 implémentation for linux. *http://www.mobile-ipv6.org/software* .

[98]. NetPerf . *http://www.netperf.org/netperf/netperfpage.html*

[99]. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson “RTP: A Transport Protocol for Real-Time Applications”. RFC 1889, January 1996.

[100]. Mgen6, an IPv6 traffic generator. URL: *http://matrix.it.uc3m.es/~long/software/mgen6/*

[101]. VLC/VLS, video lan client/server: *http://www.videolan.org/streaming/*

[102]. VIC, video conferencing tool, *http://www-mice.cs.ucl.ac.uk/multimedia/software/vic*.

[103]. Orinoco WLAN PC Card Specification, Agere Systems, URL: *http://www.orinocowireless.com*.

Appendix A

"Description of extended modules, functions and data Structures in test bed implementation"

1. Duplication and Merging (D&M) Agent

- Functions and data structures modified or introduced in IPv6 stack

File name	Description of modification
Exthdrs.c /usr/src/linux/net/IPv6	In the function IPv6_parse_tlv, we add a code to manage the parsing of DIO header when receiving IPv6 packet, the DIO header is considered as special option header. When the routing mechanisms parse a DIO header, it extracts the sequence number and through mipglue Function-call, this value is passed to the merging mechanism located in MIPL stack. If the merging mechanism allows the reception of packet, we continue to parse the rest of the header. Otherwise the packet is destroyed.
Miplglue.c	Adds a call-back entry to allow IPv6 stack to call to merging function in MIPL daemon.

- Functions and data structures modified or introduced in MIPL code

<table>
<tr><th>File name</th><th>Description of modification</th></tr>
<tr><td>mipv6.c</td><td>Registration of Mipglue call to mipv6_merge function</td></tr>
<tr><td>HA.c</td><td>

Declaration and initialization of a new socket, this socket will be used to send duplicated packets to the MN secondary interface when performing soft handover.
Initialization of necessary resources required by this merging mechanism. This mechanism will merge the duplicated packets sent by the MN.
Installation of netfilter hook to intercept IPv6 packets before they inter routing process “ NF_IP6_PRE_ROUTING”, this hook intercepts the packets sent to the primary care of address of the MN.
The hook will send stolen packet to the function mipv6_intercept (modified). This function will handle each intercepted packets, if there is a soft handover and the MN get two Local care of address, this function will duplicate each intercepted packets, introduce DIO and tunnels it to the MN local addresses. We tunnel the packets manually; we don’t use Linux Kernel tunnel procedure, because of the insertion of the DIO.
This task is done by a new function called modify_duplicate_addr, which duplicate packets only when performing soft handover.
Creation of a new function mipv6_merge. This function is called by option header parsing process in IPv6 stacks, it performs merging process as described in soft handover mechanisms

</td></tr>
<tr><td>bcache.h</td><td>

Modification of the structure of binding cache entry to allow a binding between a primary CoA and two local CoA.

<table>
<tr><td>PCoA</td><td>LCoA</td><td>LCoA2</td><td>Callback</td><td>Soft handover time out</td><td>…..</td></tr>
</table>
</td></tr>
</table>

bcache.c	▪ Modification of the function of mipv6_bcache_add to allow management of multiple binding and creation or destruction of secondary tunnel. ▪ Creation of new function called mipv6_bcache_get_first to look for locale addresses in binding cache table.

2. Access Routers:

Linux machines running patched RADVD 0.7.2 daemons with MAP option capabilities enabled to broadcast the D&M Agent existence and IPv6 address of D&M and current subnetwork.

3. Home Agent:

A standard MIPL home agent which acts also as correspondent node.

4. Mobile Node

- Functions and data structures modified or introduced in IPv6 stack

File name	Description of modification
Exthdrs.c /usr/src/linux/net/IPv6	In function IPv6_parse_tlv, we add a code to manage the parsing of DIO header when receiving IPv6 packet, the DIO header is considered as special option header. So if we find a DIO header, just extract the sequence number and through Mipglue Function call, we call the merging mechanisms, if the merging mechanism allows the reception of packet, we continue to parse the rest of the header. Otherwise the packet is destroyed.
Miplglue.c	Add a callback entry to allow IPv6 stack to call to merging function in MIPL daemon
Route.c	Add a function “find_special_route” this function is used by MN to find the route, when tunneling duplicated packet through the primary and secondary interfaces.

- Functions and data structures modified or introduced in MIPL code

File name	Description of modification
mipv6.c	Registration of Mipglue call to mipv6_merge function
MN.c	▪ Declaration and initialization of new socket, this socket will be used to send duplicated packets to the MN secondary interfaces when performing soft handover. ▪ Initialization of necessary resources needed by merging mechanism. This mechanism will merge the duplicated packets sent by the MN. ▪ Installation of netfilter hook to intercept ipv6 packets created in the MN " NF_IP6_LOCAL_OUT", this hook intercepts the packets and duplicate them through the different APs when performing Soft Handover ▪ The hook, will call the function mipv6_intercept2.this function will handle each intercepted packets, if there is a soft handover and the MN get two Local care of address, this function will duplicate each intercepted packets, introduce DIO and tunnels it to D&M address but through different Access Points. We tunnel the packets manually; we don't use Linux Kernel tunnel procedure ▪ This task is done by a new function called modify_duplicate_addr, which duplicate packets only when performing soft handover. ▪ Creation of a new function mipv6_merge, this function is called by option header parsing process in IPv6 stacks, it performs merging process as described in soft handover mechanisms ▪ Modification of the function mobile_node_moved , in this function we will create the secondary default route to the new Access router through to new interface if we are performing soft handover.
MN.h	▪ Add a new data structure to the MN_info structure to control the Soft Handover, GCoA, CoA, SCoA, D&M agent address.

Tunnel.c	▪ We define the function which create the secondary default route for soft handover " add_special_route"
Bul.c	▪ Modify function mip6_bul_add to manage the special case of binding update sent through the secondary interface in case of soft handover
mdetect.h	▪ Add a data structure to store the information about the old access router when performing soft handover.
mdetect.c	▪ In function change router, add a code to manage Access router set in case of soft handover. ▪ In this function also we add a code to organize the IPv6 Binding update sent when receiving RtAdv, in soft handover. This organization is base on multiples interfaces priorities; only, the interface with higher priority is allowed to initialize a soft handover. The priorities are set by a Linux script , which performs layer 2 handover and increment interfaces priorities

5. Test Bed

In following Figure, we show two mobile nodes used in the test bed, a single 802.11 interface terminal and multi interfaces with soft handover capabilities terminal. The second picture shows the UMTS TDD mobile node. Finally the last picture represents a global view of the test bed: access networks, and mobile nodes**.**

Mobile IPv6 soft handover platform in Eurecom labs