ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2014-ENST-0023

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Informatique et Réseaux »

présentée et soutenue publiquement par

Tien-Thinh NGUYEN

le 23 mai 2014

Optimisation des Mécanismes de Mobilité pour les Flux Multicast basés sur IP

Directeur de thèse : **Prof. Christian BONNET**

Jury

M. Jean-Marie BONNIN, Professeur, Télécom Bretagne, Brest - France		Rapporteur
M. Thomas NOEL, Professeur, Université de Strasbourg, Strasbourg - France		Rapporteur
M. Walid DABBOUS, Chercheur, INRIA, Biot - France		Examinateur

TELECOM ParisTech
école de l'Institut Télécom - membre de ParisTech

THÈSE

Optimization of Mobility Mechanisms for IP based Multicast Flows

Tien-Thinh NGUYEN

A doctoral dissertation submitted to:

TELECOM ParisTech

In Partial Fulfillment of the Requirements for the Degree of:

Doctor of Philosophy

Specialty : Computer Science and Networking

Thesis Supervisor: **Prof. Christian Bonnet**

Jury:

Reviewers:

Prof. Thomas Noel - Université de Strasbourg, Strasbourg - France

Prof. Jean-Marie Bonnin - Télécom Bretagne, Brest - France

Examiner:

Dr. Walid Dabbous - INRIA, Biot - France

To my wife and my little son - Bi

Acknowledgements

First of all, I would like to extend my sincere thanks to my advisor Prof. Christian Bonnet for his valuable support and brilliant ideas. Throughout this thesis, he has always found the time for me to guide and encourage my research activities. I also very much appreciate his dynamism and his competences that made this thesis work a success. It has been my real pleasure to work with Christian.

I would also like to thank Prof. Jérôme Härri who helped me so much with his stimulating technical discussions and constructive publication reviewing. A special warm thank to my master advisor Michelle Wetterwald for her kindness and words of wisdom which facilitate not only my research but also my life.

I am grateful to the committee members of my jury, Prof. Jean-Marie Bonnin, Prof. Thomas Noël and M. Walid Dabbous for their valuable inputs and time spent reading this thesis.

I would like to express my appreciation to my colleagues and friends at Eurecom, for all the unforgettable enjoyable moments and their helps. I also wish to extend my warmest thanks to all my friends in France and Vietnam for all the wonderful time we spend together.

Finally, last but not least, I want to express my special gratitude to my parents, my wife and my son for their unconditional support, love and trust. They, together with another members in my big family, make my life full of kindness and happiness with their encouragement.

Abstract

With the development of wireless access technology as well as the explosion of mobile devices (such as smartphones, tablets, and vehicles), the next generation mobile network is not only restricted to provide the traditional voice services but also the data services. Also, the increasing penetration of the mobile devices is generating a huge number of data traffic over mobile networks. In all-IP mobile networks, IP mobility management is a crucial concept to meet the demand of ubiquitous Internet connectivity as well as new service requirements such as seamless handover across heterogeneous networks, consistent quality of experience and stringent delay constraints. In this context, the scalability and bandwidth efficiency from the multicast routing make the IP multicast a valuable solution from the application point of view to deal with a huge number of traffic, particularly, in mobile environments where users usually share frequency bands and limited capacity. But one of the major challenges for the multicast support is when considering mobility. It comes from the fact that the multicast protocols were designed to support the stationary multicast parties. As such, it raises some issues as a result of the interaction of IP multicast and IP mobility protocols such as service interruption, packet loss, routing non-optimal, and packet duplication, etc. In fact, the conventional IP mobility management (e.g., Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6)) which leverages on the centralized mobility management approach, brings several issues for the network operator like inefficient use of network resources, poor performance, and scalability issues. The concept of Distributed Mobility Management (DMM) aims to tackle these issues and helps the mobile operators address the challenges created by rising mobile usage while enhancing the overall customer experience.

In this thesis, our main objective is to deal with the multicast mobility-related issues. The solutions are proposed in the context of the evolution of the current IP mobility management: from the host-based to the network-based, and also from the centralized to the distributed mobility management. In more details, for a single PMIPv6 domain, we introduce a method to reduce the service disruption and leave latency. We then present a solution from the load balancing point of view to address the service disruption and packet duplication issue. As DMM has not been standardized, we propose an inter-domain mobility solution, which can be considered as a step in the evolution from PMIP towards DMM. Finally, we converge to a final architecture in a DMM environment that can offer various benefits and address most of the multicast listener mobility-related issues. Throughout this thesis, a near-to-real testbed is used to achieve the realistic results.

Contents

List of Figures

List of Tables

Glossary

List of Abbreviations and Acronyms

3GPP	3rd Generation Partnership Project
4G	Fourth Generation
AAA	Authentication, Authorization and Accounting
ALM	Application-Layer Multicast
ASM	Any-Source Multicast
aHMAR	Anchor HMAR
aNMAR	Anchor NMAR
AP	Access Point
AR	Access Router
A-LMA	Anchor LMA
A-AAA	Anchor AAA
A-MAG	Anchor MAG
BA	Binding Acknowledgment
BCE	Binding Cache Entry
BU	Binding Update
CBT	Core Based Tree
CDN	Content Delivery Network
cHMAR	Current HMAR
C-LBC	Central Load Balancing Controller
cMAR	Current MAR
CMD	Centralized Mobility Database
CMF	Context Management Function
cNMAR	Current NMAR
CN	Corresponding Node
CoA	Care-of-Address
COMMA	Common MMA
DHCP	Dynamic Host Configuration Protocol
DMM	Distributed Mobility Management
DMMA	Dynamic Multicast Mobility Anchor
DSMIPv6	Dual Stack Mobile IPv6
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
D-GW	Distributed Gateway
eNB	Evolved NodeB
EPC	Evolved Packet Core
ETF	Explicit Tracking Function
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Service
FA	Foreign Agent
FI	Fairness Index
FMIPv6	Fast Mobile IPv6
FPMIPv6	Fast Handovers for PMIPv6

GGSN	Gateway GPRS Support Node
GPRS	General packet radio service
G2V	Grid-to-Vehicle
HA	Home Agent
HMAR	Host-based Mobile Access Router
HMIPv6	Hierarchical Mobile IPv6
HeNB	Home eNodeB
HIP	Host Identity Protocol
HNP	Home Network Prefix
HoA	Home Address
HSPA	High Speed Packet Access
IANA	Internet Assigned Number Authority
ICMD	Inter-Domain Centralized Mobility Database
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IFOM	IP Flow Mobility
IMR	Intersection Multicast Router
IP	Internet Protocol
IPTV	Internet Protocol Television
L2	Layer 2
L3	Layer 3
LB	Load Balancing
LBC	Load Balancing Controller
LIPA	Local IP Access
LLQC	Last Listener Query Count
LLQT	Last Listener Query Timer
LMA	Local Mobility Anchor
LMD	Localized Mobility Domain
LTE	Long Term Evolution
L-GW	Local Gateway
MAC	Media Access Control
MAG	Mobile Access Gateway
MALI	Multicast Address Listening Interval
MANET	Mobile Ad hoc Network
MAP	Mobility Anchor Point
MAR	Mobile Access Router
MBMS	Multicast/Broadcast Multimedia Service
MBone	Multicast Backbone
MBSFN	Multicast/Broadcast over a Single Frequency Network
MCTF	Multicast Context Transfer Function
MC-Req	Mobility Context Request
MC-Res	Mobility Context Response
MFC	Multicast Forwarding Cache
MGMF	Multicast Group Management Function
MIH	Media Independent Handover
MIPv6	Mobile IPv6
MLD	Multicast Listener Discovery
MMA	Multicast Mobility Anchor
MMAP	Multicast by Multicast Agent Protocol
MMF	Mobility Management Function

MN	Mobile Node
MN-ID	Mobile Node's Identifier
MNP	Mobile Network Prefix
MoM	Mobile Multicast Protocol
MOR	Mobile Router
MOSPF	Multicast Open Shortest Path First
MPDSR	Multicast Protocol With Dynamic Service Range
MR	Multicast Router
MRIB	Multicast Routing Information Base
MSDP	Multicast Source Discovery Protocol
MTMA	Multicast Tree Mobility Anchor
MUMO	Multicast Mobility Management Module
NAI	Network Access Identifier
ND	Neighbor Discovery
NetLMM	Network-based Localized Mobility Management
NEMO	Network Mobility
NI	Node Information
NMAR	Network-based DMM Access Router
NS-3	Network Simulator NS-3
PBA	Proxy Binding Acknowledgment
PBS	Personal Broadcast Service
PBU	Proxy Binding Update
P-GW	Packet Data Network (PDN) Gateway
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Spare Mode
PIM-SSM	Protocol Independent Multicast - Source Specific Multicast
pHMAR	Previous HMAR
PLC	Power Line Communication
pMAR	Previous MAR
PMIPv6	Proxy Mobile IPv6
pNMAR	Previous NMAR
Proxy-CoA	Proxy Care-of-Address
QI	Query Interval
QRI	Query Response Interval
RIB	Routing Information Base
RPF	Reverse Path Forwarding
RV	Robustness Variable
SDN	Software Defined Networking
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SIPTO	Selected IP Traffic Offload
SMR	Session-to-mobility Ratio
SPT	Shortest Path Tree
SSM	Source-Specific Multicast
S-GW	Serving Gateway
S-AAA	Serving AAA
S-LMA	Serving LMA
S-MAG	Serving MAG

tLMA	Target LMA
TLV	Type-length- vector
tMAR	Typical location MAR
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBMoM	Range-Based Mobile Multicast
RP	Rendezvous-Point
RPT	Rendezvous-Point Tree
RO	Route Optimization
RS	Router Solicitation
RTT	Round-Trip Time
UDP	User Datagram Protocol
UE	User Equipment
UGC	User Generated Content
UML	User-Mode Linux
UNP	Update Notification Message
V2G	Vehicle-to-Grid
VoIP	Voice over IP
WiMAX	Worldwide Interoperability for Microwave Access

1 Introduction

1.1 Motivation and Problem Statement

With the development of wireless access technology as well as the explosion of mobile devices (such as smartphones and tablets), the next generation mobile network is not only restricted to provide the traditional voice services but also the data services. In other words, it is evolving towards all-IP systems. In fact, the mobile data services have become an essential part of many consumers' lives [1, 2]. So far, users are using their mobile devices not only for personal life but also for work on a regular basis [3, 4, 5]. As a result, the mobile data traffic has been almost doubled each year during the last few years[1] [1, 6]. This trend is expected to continue in the upcoming years, especially with the deployment of fourth generation (4G) networks. Despite the increasing volume of traffic, the average revenue per user is falling fast [7]. In addition, in all-IP mobile networks as mobile nodes may frequently change their point of attachment to the IP network, IP mobility management is a crucial concept to meet the demand of ubiquitous Internet connectivity as well as new service requirements such as seamless handover across heterogeneous networks, consistent quality of experience and stringent delay constraints. Mobility can be handled at different layers of protocol stack ranging from the link layer to the application layer, however, most of these mobility management protocols are located at the network layer. Mobile IPv6 (MIPv6), the first mobility protocol standardized by the Internet Engineering Task Force (IETF) for IPv6 networks, maintains the mobile node (MN)'s reachability when it is away from home. It is done by relying on a central mobility, namely Home Agent (HA). However, in MIPv6, the MN needs to perform the mobility-related signaling, that means the MIPv6 protocol stack is required at the MN. It is the main obstacle of the deployment of MIPv6 in the real world. For this reason, Proxy Mobile IPv6 (PMIPv6), as a network-based mobility management, helps to avoid the additional deployment in the MN so that the MN can be kept simple. In other words, mobility can be transparently provided to all legacy MNs.

The mobile network operators are being challenged by the increase of mobile data traffic (especially the video traffic) and the new requirements e.g., providing connectivity anywhere and at anytime with consistency of user experience, while preserving the economics of their networks and creating new opportunities for revenue growth. Faced with these challenges, the operators are seeking for innovative solutions to improve their network performance and efficiency, as well as to reduce the costs expended on network operation and maintenance. Two major focuses are: i) increasing the capacity of wireless communication systems; and ii) designing and implementing an efficient system to deliver the data. Regarding the first aspect, further dramatic increases in radio capacity of mobile broadband will come with

[1] The increasing traffic is mainly driven by mobile video traffic

the implementation of new wireless technologies such as Worldwide Interoperability for Microwave Access (WiMAX), High Speed Packet Access (HSPA) and Long Term Evolution (LTE). However, spectrum for operators is both limited and expensive. Thus, they are looking at different methods to increase the system capacity such as deploying femto and pico cells, together with selecting the offload traffic between the licensed and unlicensed spectrum (e.g., from 3G to WiFi). Considering the second aspect, the aim is to simplify the network architecture as well as optimize the data transmission costs. Accordingly, the mobile network is currently evolving towards flat architecture. One example is Local IP Access/Selected IP Traffic Offload (LIPA/SIPTO) architecture defined by the 3rd Generation Partnership Project (3GPP). Following the same idea, IETF has recently chartered the Distributed Mobility Management (DMM) working group which specifies the solutions to address the problems and limitations of the current centralized mobility management. In fact, the conventional IP mobility management (e.g., MIPv6 and PMIPv6) leverages on the centralized mobility management approach, thus, raises several issues for the network operators like inefficient use of network resources, poor performance, and scalability issues when considering a large number of mobile devices and their traffic demand [8, 9, 10]. DMM is one of the solutions to help the mobile operators address these limitations while enhancing the overall customer experience.

As Internet is widely deployed and spread across a large area, it carries a variety of common information resources and services. In a sharing world, the group communication service, which refers to the ability to send data to several receivers at the same time, is naturally becoming more and more important especially in some areas like multimedia distribution, gaming, and financial services, etc. In this context, the scalability and bandwidth efficiency from the multicast routing make the IP multicast a remarkable solution from the application point of view to allow the mobile networks to deal with a huge number of traffic, particularly, in mobile environments where users usually share frequency bands and limited capacity [11]. But one of the major challenges for multicast support is when mobility is considered. It comes from the fact that the multicast protocols were designed to support the stationary multicast parties. As such, it raises some issues as a result of the interaction of IP multicast and IP mobility protocols e.g., transparency, routing optimization, packet duplication, service disruption, packet loss and group leave latency, etc [11, 12].

Regarding the IP mobile multicast, after more than a decade of research and development efforts, many approaches have been proposed, but most of them are based on such host-based mobility management protocols as MIPv6, Fast Mobile IPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6). However, the main drawback of these protocols is that they require the MN to modify its IP stack to participate into the mobility signaling process. In fact, it is the major obstacle of the deployment of MIPv6 in the real world. Additionally, the previous IP multicast approaches cannot be directly applied in a network-based mobility management in which the MN is unaware of mobility process. To solve the aforementioned issues, the IETF has worked in different solutions highlighting the difference between the source and the listener multicast mobility problems in PMIPv6. However the proposed solutions remain unable to address the issues of scalability, performance optimization and compatibility with unicast mobility at the same time. In DMM, there is no complete solution for the multicast mobility support.

It is generally acknowledged that a proposed solution cannot be widely accepted without results from valid experimentation. Such validation nowadays can be obtained through various methods, each with its own advantages and limitations. Within the networking

field of research, the results' reliability is one of the most critical issues. Thus, the results credibility is directly related to the methods used, therefore improving them becomes of great importance. In this context, the most widely used method - simulation - sometimes lacks credibility. The lesser used but most credible method - real testbed - is too expensive and difficult to scale and manage.

In this thesis, our objective is to deal with the multicast-related issues raised when a multicast node moves in a network-based mobility management domain. In other words, the aim of this research is to find solutions that ensure:

- Keeping the MN unaware of mobility from the multicast service point of view;
- Minimizing the service disruption time to even satisfy the strict requirements for the interruption- and delay-sensitive services;
- Keeping the signaling/tunneling overhead as low as possible;
- Maximizing the available network resource (reducing the waste of resources and packet duplication), keeping the reliability and improving the scalability of the system;
- Minimizing the modifications of the mobility management and the multicast routing protocols to support IP mobile multicast.

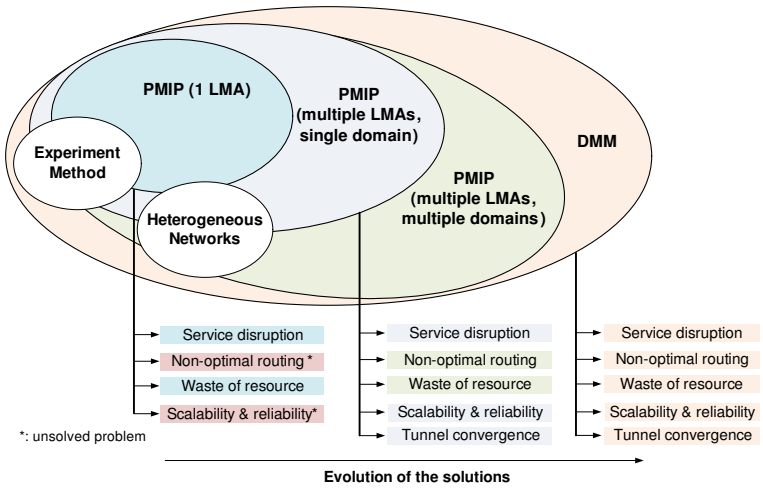


Figure 1.1 – Evolution of the solutions for multicast mobility.

The evolution of the solutions for multicast mobility is illustrated in Fig. 1.1. For a single PMIPv6 domain (with one local mobility anchor (LMA)), we introduce a method to minimize the service disruption time considering both cases: a mobile node with single or multiple interfaces. The waste of resources caused by a long leave latency is also reduced. On the other hand, the non-optimal routing; scalability and reliability issues are unsolved. Considering a single PMIPv6 domain with multiple LMAs, an additional issue is introduced - the tunnel convergence problem (or packet duplication). To improve the scalability and reliability for PMIPv6 network while addressing the tunnel convergence problem, the load balancing mechanism is proposed at an acceptable cost of service disruption. As DMM is still under discussion and has not been standardized, we provide an inter-domain mobility support which can be considered as a step towards the deployment of DMM. IP multicast

then will be considered in both the inter-domain and the DMM environments. Taking benefits of the previous proposed solutions, the dynamic multicast mobility anchor (DMMA) mechanism in DMM addresses almost all the multicast mobility-related issues such as service disruption, non-optimal routing, waste of resources, tunnel convergence and scalability. Additionally, throughout our thesis, a near-to-real testbed will be used to achieve the realistic results.

1.2 Thesis Contributions and Outline

The key contributions to the study of IP mobile multicast proposed in this thesis can be summarized as follows.

PMIP-based solutions

- *A method to minimize the multicast service disruption time during handovers inside a PMIPv6 domain*: This solution is based on the multicast context transfer and the explicit tracking function. Then, a PMIPv6 testbed has been deployed, which allows simulating the mobility of multiple multicast sources and listeners at the same time. A real implementation of the multicast context transfer function and the explicit tracking function has been deployed. Also, the listener part of Multicast Listener Discovery Version 2 (MLDv2) has been developed in NS-3.

- *A multicast-based load balancing mechanism among LMAs to solve the problem of bottleneck and single point of failure at the LMA*: This mechanism taking multicast into account helps to better distribute the load caused by the multicast flows in a PMIPv6 domain. Also, this solution can co-operate with the existing load balancing mechanisms to enhance the scalability and reliability of the system.

- *Mobility in heterogeneous networks discussions via a use case: electric vehicle charging service (ECVS)*: By using PMIPv6, the service takes care of the Electric Vehicle (EV) mobility, handling vertical and horizontal handovers between different communication technologies (e.g., Wireless LAN (WLAN), LTE and Power Line Communication (PLC)). The IPv6 address preservation in PMIPv6 is guaranteed by relying on the logical interface mechanism which helps to hide the change of interface to the IPv6 stack. Moreover, the logical interface keeps the MN unaware of the interface change as well as mitigates its impact on the service disruption.

DMM-based solutions

- *A solution for inter-domain mobility for PMIPv6*: It allows the data packets to be routed via a near-optimal way by bringing the mobility anchors closer to the MN while the control management can be placed anywhere in the network. This solution can be considered as a one step towards the deployment of DMM. A basic support for the multicast listener mobility in an inter-domain environment then is provided.

- *A dynamic multicast mobility anchor selection in DMM (DMMA)*: It enables a per-flow multicast support. From a multicast service perspective, it helps satisfy the requirements in terms of service disruption and delay, especially when considering the real-time services. The packet duplication and waste of resources (or leave latency) issues can be reduced. Also, it provides a mechanism to better distribute the load

among the Mobile Access Routers (MAR). The DMMA mechanism takes the advantages from the previous contributions into account, for example: i) the multicast context transfer and explicit tracking function are re-used to minimize the service disruption; ii) the load information is used as a metric for the multicast anchor selection; iii) the method of load collection is applied to collect others metrics; and iv) the operation of the central mobility database (CMD) is similar to the inter-domain central mobility database from the inter-domain PMIPv6 proposal.

In order to validate the solutions with a high degree of confidence, *an experiment method is used to achieve the realistic results at low cost.* This is a trade off between the simulation method which in some cases lacks of credibility and the real testbed which is typically too expensive, difficult to scale and manage. Based on this method, a testbed is deployed to conduct the experiments for the multicast mobility in PMIPv6. Additionally, this method can be generally applied for the experimentation in wireless mobile networks.

The work presented in this thesis is structured as follows. A part from the introduction and final conclusion, we divide the content of the thesis into three main parts. We present a brief description of the related works in the first part. Then, in part II and III, we discuss the solutions for the mobile multicast-related issues.

1. In the first part, we provide an overview of IP multicast and IP mobility. This part also highlights the issues and challenges when considering multicast in a mobile environment. Particularly, we make a brief introduction of the main approaches proposed by the IETF regarding their advantages and limitations. Based on this analysis, the solutions for the remained issues will be presented in the next parts. Also, we enlist the requirements for an effective performance evaluation of mobile multicast solution. We then propose an efficient method for experimentation in the wireless mobile networks. The testbed, which is developed based on this method, will be used throughout this thesis to validate the solutions.

   Results have been presented and / or published

   (a) in the Future Network and Mobile Summit (Futurenet 2012) [13]

   (b) within an official research deliverable of Medieval [14, 15]

2. The second part discusses several issues when a multicast node moves in a single PMIPv6 domain. Chapter 4 focuses on the service disruption issue. Chapter 5 proposes a load balancing mechanism taking multicast service into account to better distribute the load among LMAs, so as to improve the scalability and the reliability of the PMIPv6 domain. Chapter 6 discusses the mobility of a multihomed node in which the logical interface mechanism is used to hide the change of physical interface to the IP stack.

   Results have been presented and / or published

   (a) at the Wireless Communication and Networking Conference (WCNC 2013) [16]

   (b) at the 24th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2013) [17]

   (c) at the CNC workshop, 2014 International Conference on Computing, Networking and Communications (ICNC 2014) [18]

3. In the last part, we first propose an inter-domain mobility support for PMIPv6 based on the DMM concept in Chapter 7. Then in Chapter 8, we propose a dynamic multicast mobility anchor selection in DMM which enables a per-multicast flow support. The proposed mechanism helps satisfy the requirements in terms of service disruption and delay, especially when considering real-time services. Also, it provides a mechanism to better distribute the load among the MARs.

   Results have been presented and / or published

   (a) at the International Conference on Communications (ICC 2014) [19]

   (b) at the 78th Vehicular Technology Conference (VTC2103-Fall) [20]

   (c) at the Wireless Communication and Networking Conference (WCNC 2013) [21]

   (d) at the 9th International Conference on Networking and Services [22]

   (e) at the International Conference on Communications (ICC 2013) [23]

The contributions of this thesis have also been submitted to the Computer Networks journal, Elsevier [24] and will be submitted to the Wireless Networks journal, Springer [25].

Part I

Background Analysis

Overview of Part I

In this Part, we will introduce the fundamental notions of IP multicast, mobility management protocol as well as identify the issues and challenges when considering multicast in wireless mobile networks. We then enlist the performance evaluation metrics for IP mobile multicast. Next, we present an experiment testbed for IP mobile multicast which provides realistic results at a low cost. More than that, our experiment method in general can be applied for experiment in wireless mobile networks.

In Chapter 2, we describe the basic notions of IP multicast, its components and its applications in the Internet. To deploy the multicast service, two fundamental components are needed: group management protocols and multicast routing protocols. We then present in details of how an IP multicast service works from the Protocol Independent Multicast - Sparse-Mode (PIM-SM) and MLD protocols point of view. Regarding the IP mobility management protocols, starting from MIPv6 and its variants, we introduce PMIPv6 protocol and its enhancements. After discussing the limitations of the centralized mobility management such as MIPv6 and PMIPv6, DMM will be presented as a promising mobility management scheme for future networks. Based on the fundamental concepts of IP multicast and mobility management protocols, we highlight the issues and challenges when applying IP multicast in a mobile environment. Different impact factors on the multicast service are identified. At the end of this chapter, we highlight such issues as multicast service disruption time, packet loss, tunnel convergence problem, sub-optimal routing, end-to-end delay, and leave latency (waste of resources).

In Chapter 3, a list of specific requirements that would lead to the design of the target solutions is provided. We then define the performance metrics that are crucial to access the effectiveness of a mobile multicast solution. In the context of this thesis, we focus on such metrics as signaling overhead, handover latency (multicast service disruption time), end-to-end delay, packet loss and tunneling overhead. The qualitative metrics like easy-to-deploy and scalability are also taken into account. We then introduce an experiment method which in some cases is used to improve the degree of confidence of the solution's results. Additionally, it can be considered as a framework that aims to close the gap between research experimentation and real deployment.

Throughout this thesis, in order to validate the results, firstly, we use an analytical analysis. The proposed experiment method then, in some cases, is used to improve the degree of confidence of the results.

2
Reference Technologies and Challenges

In this chapter, we will at first introduce the basic notions of IP multicast and IP mobility management protocol. We then present some background on multicast support in mobile environments, as well as its associated problems. In the scope of this thesis, we focus on the network-based mobility management protocol i.e., PMIPv6. Thus, we will sketch the existing proposals for multicast mobility support in PMIPv6 mainly from the IETF point of view regarding their advantages and limitations. Also, the multicast mobility in DMM will be discussed.

2.1 IP Multicast

As Internet is widely deployed and spread across a large area, it carries a variety of common information resources and services. In a sharing world, group communication service, which refers to the ability to send data to several receivers at the same time, is naturally becoming more and more important especially in some areas such as multimedia distribution, gaming, and financial services, etc. In this context, IP multicast offers an effective and scalable mechanism to support group communication applications.
Unlike the traditional communication model where data is sent from a source to a destination (called unicast or one-to-one model) or to all the nodes in a specific scope (broadcast), multicast allows transmitting data to a set of users that are interested in receiving data destined to a specific group, referred to as a multicast group. Internet Protocol (IP) multicast (or IP multicast) was first proposed by Steve Deering in the late 1980s [26], and was then standardized by IETF in RFC 1112 [27]. IP multicast describes how nodes can send and receive multicast packets across IP networks. The first multicast session was executed to transfer the audio multicast over the Internet via the Multicast Backbone (MBone) in 1992 [28, 29].
In multicast, the sender only needs to send a single copy of data to reach all the group members, rather than sending a separate copy to each receiver. The intermediate routers then duplicate data packets until they reach the receivers. As a result, the multicast brings some advantages compared to the unicast and the broadcast mode such as efficient delivery to multiple destinations (e.g., reducing server load and eliminating traffic redundancy), thus improving overall resource utilization [28].
A multicast source can send the multicast data to the group at any time, without the need for prior registration/scheduling and joining the group. If a source desires to send data packets to the multicast group, it uses the group address as the destination address in its data packets. Moreover, the source is usually unaware of any group membership

details. Similarly, from receiver point of view, a host may join or leave a multicast group at any time without any restrictions on the location and the number of hosts in a group. Each multicast group is represented by an IP multicast address. The multicast address assignment is responsible by the Internet Assigned Number Authority (IANA)[1], as specified in [30].

After more than a decade of important researches and development efforts, IP multicast, in general, has been slowly deployed on the global Internet. The barrier of widespread deployment of multicast applications mainly comes from technical, administrative and business related issues as stated in [31]. Therefore, several alternative techniques for multicasting have been proposed [31], in which each alternative can be suitable for a specific environment. For example, application-layer multicast (ALM) [32] in which the multicasting functionality is implemented at the application layer instead of at the network layer as IP multicast does not require the change in the network infrastructure. Data packets are replicated at the end hosts, instead of the network routers as in IP multicast. ALM is suitable, for example, for the mobile ad hoc network (MANET) applications. Although ALM is much easier to deploy compared to IP multicast, IP multicast outperforms ALM (as well as other alternatives) in terms of robustness, security, performance, and scalability [31]. The new business models [33], a huge traffic demand (especially multimedia traffic), the revenue per data reducing phenomenon in the mobile operator networks, as well as the advantages of new multicast model (SSM) bring again the strong interest of IP multicast from both academy and industry. IP multicast is expected to play more important role in the future networks. As a result, this thesis focuses only on the case where multicast functionality is located at the network layer or IP multicast.

Since IP multicast is based on the User Datagram Protocol (UDP) as a transport protocol, which only provides best-effort delivery guarantees, multicast packets are delivered without reliability or congestion control (at the transport layer). For applications that require a reliable data transfer, additional mechanisms must be provided by the application layer e.g., reliable multicast transport protocols.

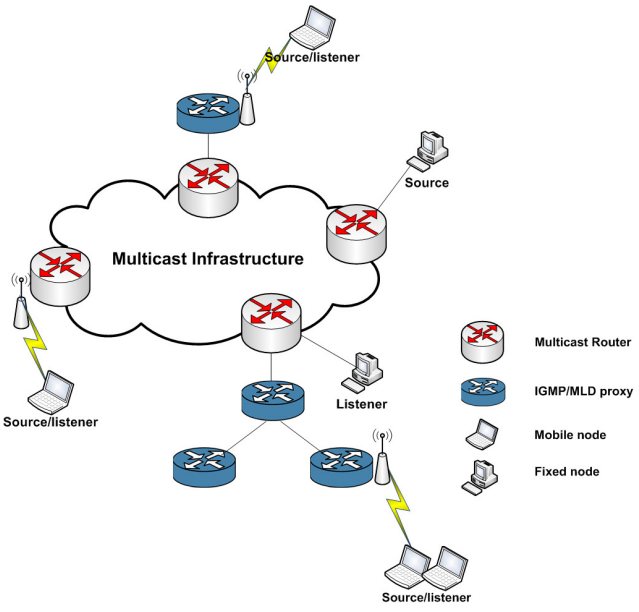


Figure 2.1 – An example of multicast deployment architecture.

[1]http://www.iana.org

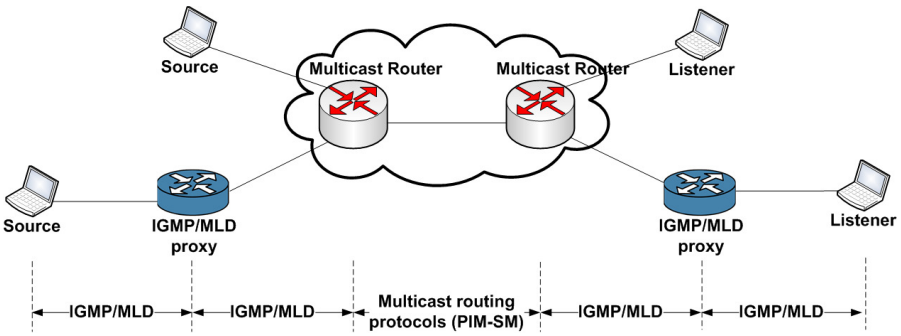


Figure 2.2 – A multicast deployment scenario: from protocols point of view.

In order to provide multicast service, two groups of protocol need to be deployed: multicast group membership protocols and multicast routing protocols. The multicast group membership protocols enable hosts to dynamically join/leave the group as well as make multicast routers (MR) aware of the interested receivers and manage their subscriptions. The multicast routing protocols enable a collection of MRs to build distribution trees to deliver the multicast traffic from sources to all the members of a multicast group. The multicast group membership protocols, depending on IP version, are Internet Group Management Protocol (IGMP) [34] for IPv4 and Multicast Listener Discovery (MLD) [35] for IPv6.

Regarding the multicast routing protocols, each protocol uses its multicast routing algorithm to build the multicast delivery tree. There are many multicast routing protocols such as Distance Vector Multicast Routing Protocol (DVMRP) [36], Multicast Open Shortest Path First (MOSPF) [37], Core Based Tree (CBT) [38, 39], Protocol Independent Multicast – Dense Mode (PIM-DM) [40], and Protocol Independent Multicast – Sparse Mode (PIM-SM) [41]. In this thesis, the considered multicast routing protocols are PIM-SM and the enhanced version of PIM-SM for source specific (PIM-SSM [41]). To avoid deploying a full-stack MR inside a given network due to its implementation and operational costs, IGMP/MLD proxy [42] which performs membership management, acts as a multicast Querier for its subnet and as a host for an upstream proxy/MR, is introduced.

Fig. 2.1 and Fig. A.1 show an example of a multicast deployment scenario from architecture and protocol point of view, respectively. As seen in Fig. 2.1, multicast sources/listeners can be a mobile node or a fixed node. The multicast traffic is routed from the sources to the listeners via the intermediate MRs and/or MLD proxies.

2.1.1 IP Multicast Applications

Taking advantages of multicast, various applications which can be classified into different groups following different criteria can be deployed. In terms of multicast model, the multicast applications can be placed into three main categories, as stated in [43, 44]:

- One-to-many (a single source sending to a set of receivers): A typical example is scheduled audio/video distribution (including Internet Protocol Television (IPTV), mobile TV, lectures, presentations, etc.). Also, the multicast application can be used to push media like news headlines, weather updates, sport scores and financial services. Software update also falls into this category.

- Many-to-many (multiple sources sending to a set of receivers): Applications such as audio/video conferencing, distributed online games, and collaborative environments,

in which some or all the participants become sources, are examples of the many-to-many model.

- Many-to-one (multiple sources sending to a receiver): Many-to-one applications include resource discovery (e.g., service location and device discovery), data collection (monitoring applications, video surveillance), and so on.

Following the service function, these applications fall into such groups as Mobile TV (live and interactive TV), Personal Broadcasting Service (PBS), Live Video Distribution (conferences, seminars, etc.), Multimedia Content Distribution (Video On-Demand), General Content Distribution (Data on Demand, Online Gaming), and Machine-to-Machine Distribution (e.g., Software distribution and navigation system updates) [45].

2.1.2 Multicast Model

At the time IP multicast was introduced, a *host group* model supported both one-to-many and many-to-many group communication (referred as Any-Source Multicast, or ASM). However, this model is also one of the main barriers for the widely multicast deployment. It is due to the fact that there are several deployment issues of the ASM model such as multicast address allocation and management, lack of access control (leading to the denial of service attacks), scalability and service provisioning [46, 47].
To promote the deployment of multicast, a new service model, the so-called Source-Specific Multicast (SSM), is introduced. The great advantage of SSM is the simplicity. SSM model also overcomes the limitation of ASM and is suitable for one-to-many applications. A range of multicast addresses (FF3x::/32 for IPv6) is reserved for SSM. In more details, SSM simplifies the multicast related mechanism by eliminating the need of the Rendezvous-Point Tree (RPT), RP, and Multicast Source Discovery Protocol (MSDP)[2]. To cope with SSM model, the group management protocol is required to support source filtering as described in [48]. Also, PIM-SSM [41], as an extension of PIM-SM, is specified to handle a source-specific model.

2.1.3 Group Management Protocols

Multicast group membership protocols consist of two parts. The first part, namely multicast listener one, is used by hosts/routers to announce their interest in receiving traffic destined to a specified group with their neighboring MRs. The second part, multicast router one, is performed by the MRs to discover the presence of the interested hosts of a given group and to manage their subscriptions for each of their directly attached link. IETF defines two multicast group membership protocols, i.e., IGMP [27, 49, 34] for IPv4 and MLD [50, 35] for IPv6. The current version of IGMP (IGMPv3 [34]) and MLD (MLDv2 [35]) share the same functionality. In this thesis, only MLDv2 is considered since we focus on the IPv6 network. The interaction between the two parts is done by using MLD messages.
From a multicast listener point of view, when the upper-layer protocols or application programs ask the IP layer to enable the reception of multicast traffic from a specific multicast address, a node will send an MLD Report message to its MR to join this group. The MR then joins the multicast group (if necessary) and forwards the multicast packets to the subscribed nodes. The MLD Report is also used to reply to the general queries which are periodically sent by the MR to learn about the multicast subscription information from an attached link. In addition, if the listening state of a node changes, the node will immediately report this change via a State Change Report message.

[2] The control plane for source discovery is now under the responsibility of receivers

From an MR point of view, the MR uses MLD to learn, for each of its directly attached links, which multicast addresses and which sources have listeners interested on that link (to support SSM). Thus, the router only needs to know whether there is at least one group member per network interface which is interested in receiving the multicast traffic of a multicast group, or not. However, the router can maintain the detailed subscription information regarding the multicast addresses, their corresponding subscribed hosts, and the associated network interface by means of the explicit tracking function [51]. Enabling the explicit tracking function can help reduce the multicast-related issues in a wireless environment such as signaling overhead and leave latency.
The basic operations of MLD are briefly described as follows:

- One MR in a subnet, the so-called Querier [35], periodically sends MLD General Query messages onto the link to build and update the multicast membership state of all multicast routes on this link.
- Nodes respond to these queries by sending a Current State Report message indicating their group memberships to all MLDv2 routers on the link. Whenever their listening state changes, they report these changes to the routers via a State Change Report message.
- All routers, upon the reception of the Report messages, update the memberships state on the link. If the Querier receives an MLD State Change Report indicating that the node desires to stop listening to a particular group, the Querier will make a query for the presence of other listeners subscribed to this group using a Multicast Address Specific Query, before deciding to stop forwarding multicast traffic for this group. Similarly, the Multicast Address and Source Specific Query is used to learn the membership state of a specified multicast address with specified source address.
- If a router does not receive a Report message for a particular group for a period of time, it will assume that there are no more members of the group on the link and can stop forwarding the multicast packets for this group.

2.1.4 Multicast Routing Protocols

IP multicast does not require a source sending to a given group to know about the receivers of the group, instead it is based on the multicast delivery trees to deliver the multicast packets. Multicast routing protocols are responsible for building the multicast delivery trees and forwarding the multicast packets along the trees to the appropriate receivers. Various multicast routing protocols, according to the type of the multicast tree they build, can be grouped into two categories: a source-based tree and a share tree.
The source-based tree (or shortest-path tree) protocols are based on the shortest path towards the source to build a tree to minimize the path cost from the source to each receiver. Thus, such a separate delivery tree is built for each multicast source of a given group. In this case, the multicast packets will be delivered along a shortest-path tree from the source to the members of multicast group in order to meet the objective of a low-delay multicasting [26]. Protocols such as DVMRP, MOSPF, PIM-SSM and PIM-DM use this kind of multicast delivery tree.
For example, DVMRP is the first multicast routing protocol proposed by S. Deering [26]. DVMRP is a flood-and-prune protocol in a sense that the source floods the multicast packets to the entire domain and the routers which do not have multicast listener for this group send a prune message to stop forwarding packet to them. In more details, the packets that do not arrive at a router on the appropriate interface (the interface from which the

router could forward a unicast packet to the source following the shortest path) are ignored. Otherwise, they will be forwarded to all, except the incoming interface. Based on IGMP protocol, the leaf routers which do not have multicast listener for this group prune back to the spanning tree. However, the multicast packets need to be re-flooded to detect the new listeners. As a result, the prune messages need to be sent periodically to remove the unnecessary links along the shortest path tree towards the source. All together, it leads to the scalability issue.
There is another type of algorithm, the so-called Shared Tree (or Core-based Tree) where a single tree is shared by all the sources of the same multicast group. In other words, the multicast traffic for each group is sent and received over the same delivery tree, regardless of the source. It is achieved by introducing a core router, the so-called Rendezvous Point (RP) which is a pre-defined router. The MR may statically store the address of RP or discover the address during the bootstrap phase [41]. When a source transmits a packet to a multicast group, the packet is first sent to the RP which then forwards the packet along the reverse shortest path tree (towards the RP) to reach all the listeners. Moreover, each edge router which desires to receive the multicast traffic has to join the tree by sending an explicit *Join* message towards the RP. Based on that, the multicast delivery tree is built. Comparing to the previous algorithm, CBT is better regarding network bandwidth since it does not require the multicast packets to be periodically forwarded to all MRs in the internetwork. Protocols such as CBT and PIM-SM use the core-based tree.
Additionally, the flooding mechanism is suitable for the case where the members of the multicast group are densely distributed across the network. These protocols using it as a distribution mechanism are called dense-mode protocols. On the contrary, in the widely distributed multicast environments where the group members are spread sparsely across the network, the flooding mechanism may cause a waste of bandwidth and performance issues. As a result, CBT with the explicit join mechanism is more suitable. The corresponding routing protocols are called the spare-mode ones.

2.1.4.1 Protocol Independent Multicast-Spare Mode/Source-Specific Mode

The name of Protocol Independent Multicast (PIM) derives from the fact that PIM does not have its own unicast routing protocol, instead it relies on the existing unicast routing protocols to build a separate multicast forwarding table. PIM-Spare Mode (PIM-SM), a spare-mode protocol, is the most widely used multicast routing protocol. PIM-SM is a dual-stack protocol for both IPv4 and IPv6. However, in the scope of this thesis, we focus on IPv6 part of this protocol which uses both the source-based and the shared-tree to deliver the multicast traffic.
In PIM-SM, a RP plays the role of a core of the multicast delivery tree in a sense that the source sends the multicast packet to the RP. When a listener wishes to receive multicast traffic from a group, it sends an MLD Report to its default MR (designated router or DR) which then joins the multicast delivery tree on behalf of the listener. As a result, the existence of the sources and the listeners are independent of each other. The detailed operation of PIM-SM is described as follows.
The PIM-SM operations consist of three phases as described in Fig. 2.3. In the phase one (see Fig. 2.3a), a multicast listener expresses its interest in receiving multicast traffic destined for a given group by sending an MLD Report to its DR. The DR then sends a PIM Join message towards the RP for that group. Since the multicast traffic can arrive from any sources, the Join message is denoted as (*, G) Join. The MRs on the path towards the RP of the (*, G) Join establish the multicast tree state for group G. Therefore, a multicast delivery tree with the root at the RP is constructed for group G, called RP Tree (RPT). Since the

RPT is shared by all the sources, it is considered as a shared tree. From a multicast source point of view, the source can start sending data packets destined for a group at anytime. The source's DR, upon receiving the multicast packets, unicast-encapsulates them and sends them directly to the RP (as known as the registering process). The RP, on the reception of the encapsulated packets, decapsulates them and forwards them natively following the multicast forwarding state onto the shared tree. The multicast packets are then replicated by the intermediate routers and reach the listeners. The encapsulation packets are called the PIM Register packets.

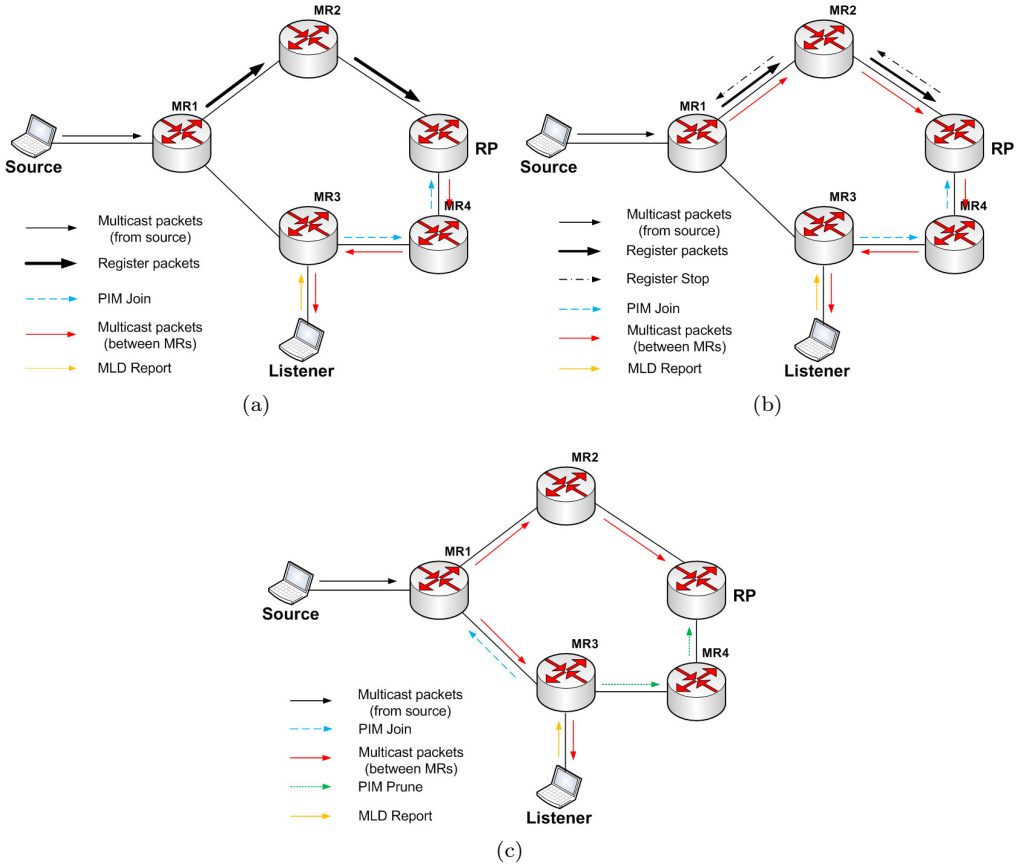


Figure 2.3 – PIM-SM operations: (a) phase 1, (b) phase 2, (c) phase 3.

In the phase two (see Fig. 2.3b), after receiving the PIM Register packets from a source S, the RP may decide to switch to a native multicast forwarding by sending a (S, G) Join towards the source S. Similarly, the (S, G) multicast tree, which is the shortest-path tree towards the source S, will be established. In the meantime, the data packet will continue being encapsulated to the RP. As soon as the multicast packets arrive natively at the RP, the RP sends a Register-Stop message to inform the source's DR to stop encapsulating the packets. At the end of this phase, the traffic will be routed natively from source S to the RP, and then along the shared tree to the listeners.

Fig. 2.3c illustrates the PIM operations in the phase three. As the traffic passes through the RP, it is usually not an optimal path from the source to the listener. Thus, the listener's DR may send a (S, G) Join towards the source to switch to the shortest path tree. Similarly, after receiving the multicast packets from the source, the listener's DR sends a Prune message to the RP (known as (S, G, rpt) Prune) to prune the unnecessary routes. At the

end of this phase, the multicast traffic is routed following a shortest-path tree from the source S to the listener.
The SSM model can be enabled at a PIM-SM router by using a subset of the PIM-SM protocol mechanisms. In more details, from an MR point of view, only (S, G) Join/Prune messages are generated by the router, and no (*, G) and (*, G, rpt) Join/Prune messages are generated. The packets related to (*, G) or (S, G, rpt) state should be ignored. PIM-SSM is backward compatible with PIM-SM, that means the router can only implement a subset of PIM-SM for SSM support.

2.1.5 IGMP/MLD Proxy

The operators, in some cases, may not desire to deploy the multicast routing function on the routers inside a given network due to the hardware, the implementation and operational cost of an MR. In this case, IGMP/MLD proxy (is referred as MLD proxy, from now on) [42], as a lightweight protocol compared to the complicated multicast routing protocols such as PIM and DVMRP, can be used to simplify the design and implementation of the router. It should be noted that MLD proxy only works in a single tree topology as can be seen in Fig. 2.1. This proxy performs the router part of MLD protocol on its subnet and the host part on its upstream interface. In other words, the MLD proxy function allows an intermediate node to appear as an MR to the downstream hosts and as a host to the upstream MRs. The MLD proxy device maintains a database as a multicast membership. The MLD proxy will forward the multicast packets arriving from an upstream interface to all the downstream interfaces that have the subscription information of this group. Also, if a packet arrives at the proxy from a downstream interface, it will be forwarded to the upstream interface and to all the downstream interfaces that have the subscription information of this group except the incoming one.

2.2 IP Mobility Management

Nowadays, the mobile data services have become an essential part of many consumers' lives [1, 2]. So far, the users have been using their mobile devices (e.g., smartphones and tablets) not only for personal life (e.g., making voice/video calls, sending email, watching video/TV, playing online games, and so on) but also for work (general and job-specific work applications such as multimedia conferencing, and distance learning, etc.) on a regular basic [3, 4, 5]. As a result, the mobile data traffic has been almost doubled each year during the last few years [6]. This trend is expected to continue in the upcoming years, especially with the deployment of 4G networks. The widely usage of mobile data services has been driven by the variety of different reasons such as: the increasing number of mobile devices which become more and more powerful and intelligent, the enhancement of wireless access technology in terms of coverage, speed and quality, as well as the explosion of mobile applications [6]. The mobility of the devices puts a new requirement on the mobile operators to provide connectivity anywhere and at anytime. Moreover, providing consistent and seamless services is required for satisfying user's expectations and fulfilling even highly application requirements in terms of service disruption on the move [52].
In all-IP mobile networks, IP mobility is a crucial concept to meet the demand of ubiquitous Internet connectivity as well as new service requirements such as seamless handover across heterogeneous networks, consistent quality of experience and stringent delay constraints. IP mobility can be handled at different layers of protocol stack ranging from the link layer to the application layer [53, 54, 55]. The link layer mobility management protocols

use the underlink information for mobility-related procedures when the MN roams among different physical points of attachment while keeping its layer 3 attachment (preservation of the IP address). The transport layer mobility management protocols [56, 57] provide an end-to-end mobility support without requiring to change the network layer infrastructure. Regarding the mobility protocols at the application layer, the most well-known protocol, Session Initiation Protocol (SIP) [58, 59], provides an end-to-end mobility management framework, which does not depend upon the network entities (e.g., HA) and can be deployed by any third-party application service providers. Due to the fact that most of the existing mobility management protocols are located at the network layer (since a network layer IP mobility is transparent to the upper layers as well as the applications [60, 55]), we focus on these protocols in our thesis.

Again, the mobility management protocols at the network layer can be classified according to different criteria such as the mobility range (micro- and macro-mobility) and the mobile host signaling (host- and network-based mobility) [53, 54, 61, 55]. Regarding the mobility range, the mobility management can be categorized into two types: the macro-mobility and the micro-mobility. The macro-mobility (global mobility or inter-domain mobility) refers to the mobility between different domains (with different architectures and access technologies) over a large area. MIPv6 and Host Identify Protocol (HIP) [62] fall in to this category. On the other hand, the micro-mobility (or intra-domain mobility) is referred as a mobility between different cells/subnets inside a single administrative domain. Some examples of micro-mobility protocol are HMIPv6, FMIPv6, and PMIPv6. Considering the mobile host signaling, the host-based mobility protocols such as MIPv6 and Dual Stack Mobile IPv6 (DSMIPv6) [63], require the host to participate in mobility-related signaling process. On the contrary, in the network-based mobility, the network entities handle the mobility process on behalf of the host.

As stated above, the increasing penetration of the mobile devices, such as tablets and smart phones is generating a huge number of data traffic over the mobile networks. The mobile data traffic is expected to grow to 11.2 exabytes per month by 2017, a 13-fold increase over 2012 [1]. Despite the increasing volume of traffic, the mobile data revenue per user is falling fast. Thus, the mobile network is evolving towards the flat network architecture in order to be able to cope with the huge amount of traffic and reduce data transmission costs. Examples of this trend are traffic offloading (e.g., LIPA/SIPTO) and content delivery network (CDN) [9]. Considering the conventional IP mobility management (e.g., MIPv6, PMIPv6) which leverages on the centralized mobility management approach in a flat architecture, it raises several issues for the network operator like the inefficient use of network resources, poor performance, and scalability issues [8, 9, 10]. To overcome these problems, a novel concept, the so-called distributed (and dynamic) mobility management (DMM) has been introduced. A lot of research publications [64, 65, 66, 67, 68, 69] carried out the analysis on different DMM approaches and compared them with the conventional mobility managements in terms of signaling cost, packet delivery cost, handover delay, packet loss and end-to-end delay. The results from these analysis showed that DMM is a promising mobility management scheme.

In this section, we will briefly introduce a various IP mobility protocols ranging from the host-based to the network-based, from the centralized to the distributed approach. We focus on MIPv6 as a typical example of the macro-mobility and host-based mobility; and PMIPv6 as an example of the micro-mobility and network-based mobility. Finally, DMM will be presented, mainly focusing on the network-based approach.

2.2.1 Centralized Mobility Management

2.2.1.1 Mobile IPv6

Mobile IPv6 (MIPv6) [70] is the first mobility protocol standardized by the IETF for IPv6 networks. As a global mobility protocol, MIPv6 maintains the mobile node's reachability when it is away from home. It is done by introducing a central mobility, namely Home Agent (HA) located at the MN's home network, which is a topological anchor point of the permanent MN's IP address (Home Address or HoA). Using its home address, the MN can communicate regardless of its actual location in the Internet. When the MN is away from home, it may obtain a temporal IP address (namely care-of-address (CoA)) which can be used in the foreign network for routing purposes. This address identifies the current location of the MN. The MN then registers its current topological location (CoA) with its HA by means of Binding Update (BU)/Binding Acknowledgment (BA) messages. The HA keeps track of the MN's current location by maintaining a binding association between the MN's HoA and MN's CoA (namely Binding Cache Entry - BCE). A bi-directional tunnel is then established between the HA and the MN for redirecting packets from/to the current location of the MN. In more details, the HA, acting as a topological anchor point of HoA, intercepts the packets addressed to the MN and tunneled them to the MN's CoA. On the other direction, the packets from MN are tunneled to the HA, before forwarding to the CN. However, a relevant drawback of MIPv6 is a triangular routing in which the packets have to pass through the HA, which is a typically longer route. To tackle this issue, the Router Optimization (RO) mode in which the MN communicates directly with the CN without passing through the HA is introduced. However, MIPv6 introduces several security vulnerabilities e.g., authentication and authorization of BUs during the RO process [71].
Additionally, MIPv6, as a global IP mobility solution, may cause a high handover latency (and packet loss) that could significantly affect the performance of the on-going sessions [72, 73]. The high signaling load is also required [72, 73]. Thus, it is not optimized to handle the micro-mobility management, where low-latency handover and low mobility-related signaling are essential. Various solutions have been proposed to improve the performance of MIPv6 such as Hierarchical Mobile IPv6 (HMIPv6) [74] and Fast Mobile IPv6 (FMIPv6) [75]. In HMIPv6, the Mobility Anchor Point (MAP) which is located at a local domain is introduced. Each MAP can be served as a local mobility anchor for a local domain. In this case, the mobile node sends BU messages to the local MAP rather than the HA when it moves inside a local domain. The MN sends BU message to the HA only when it moves between MAPs. As a result, the handover latency as well as signaling cost are reduced. On the other hand, FMIPv6 aims at reducing the handover latency and the number of lost packets. In this case, the handover is prepared in advance by using the lower-layer information, thus allowing the MN to configure a new CoA before it actually moves to the new subnet. As a result, the MN can use the CoA address immediately when it connects to the new subnet. The packets are also forwarded from the previous router to the new one, thus, reducing the number of lost packets.
As a host-based mobility protocol, in MIPv6, the MN needs to perform the mobility-related signaling by means of location update procedure. Consequently, the MIPv6 protocol stack is required at the MN. It is the major obstacle for the deployment of MIP in the reality. For this reason, the network-based localized mobility management (NetLMM[3]) is proposed to avoid the additional deployment in the MN so that the MN can be kept simple. Moreover, the complex security mechanism to authenticate the location update signaling can be avoided. In other words, the mobility can be transparently provided to all the legacy

[3]NetLMM WG: http://datatracker.ietf.org/wg/netlmm/charter/

MNs.

2.2.1.2 Proxy Mobile IPv6

Unlike MIP6 and its host-based extensions in which the mobility functions need to be deployed at both network and terminal, a new approach, namely network-based localized mobility management (NetLMM), enables the mobility support without the MN's evolving in the signaling process. In this case, the mobility procedures are handled by the network entities. Proxy Mobile IPv6 (PMIPv6) [76], as an extension of MIPv6, was standardized by the IETF as a network-based mobility management protocol. PMIPv6 provides the mobility support within a localized area, namely a Localized Mobility Domain (LMD) or a PMIPv6 domain. While moving inside a LMD, the MN remains its IPv6 address. Thus, from IP layer point of view, the MN is unaware of mobility. This is achieved by introducing the network entity called the Mobile Access Gateway (MAG), which performs the mobility-related signaling on behalf of the MNs attached to its access links. In PMIPv6, the LMA, similar to HA in MIPv6, is responsible for maintaining the MN's reachability state and forwarding traffic from/to the current location of the MN. MN's traffic is always encapsulated and tunneled between the MN's LMA and the corresponding MAG. Each LMD consists of several LMAs and multiple MAGs, as illustrated in Fig. A.2.

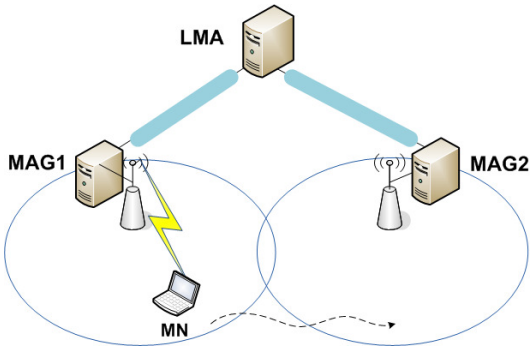


Figure 2.4 – The architecture of a PMIPv6 domain.

Compared to MIPv6, PMIPv6 brings some benefits such as: (i) avoiding the complexity of the protocol stack at the MN; (ii) supporting mobility without the MN's involvement; and (iii) reducing tunneling overhead (over the air) and decreasing handover latency [73].

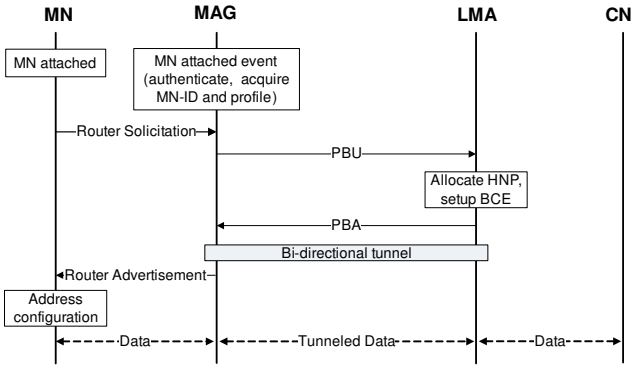


Figure 2.5 – Signaling when a mobile node attaches to the PMIPv6 domain.

The operation of PMIPv6 is briefly described as follows. Fig. 2.5 shows signaling for the

MN's initial attachment to a PMIPv6 domain. When an MN enters a PMIPv6 domain (attaches to a MAG), upon the detection of a new MN, the MAG fetches the MN profile, for example from an Authentication, Authorization and Accounting (AAA) server, and verifies if the MN is authorized for the network-based mobility service. Upon a successful authorization, the MAG sends a Proxy Binding Update (PBU) message to LMA to register a new MN. After receiving the PBU message, the LMA allocates a Home Network Prefix (HNP) to the MN, creates a BCE for this MN (including the MN's identifier (MN-ID, for example using the Network Access Identifier (NAI) [77], or its Media Access Control (MAC) address), HNP and the MN's MAG address (Proxy Care-of-Address or Proxy-CoA)). The LMA then replies by a Proxy Binding Acknowledgment (PBA) message including the allocated HNP. The MAG, on receiving the PBA, sets up the forwarding policy for the MN. A bi-directional tunnel is then established between the MAG and the LMA for redirecting the traffic from/to the MN. It is noted that the PBU/PBA messages are based on BU/BA messages with some specific extensions, respectively [76]. The MAG then sends a Router Advertisement (RA) message including the allocated HNP to the MN. The MN, based on the HNP, configures its address and can use it to communicate with a corresponding node (CN).

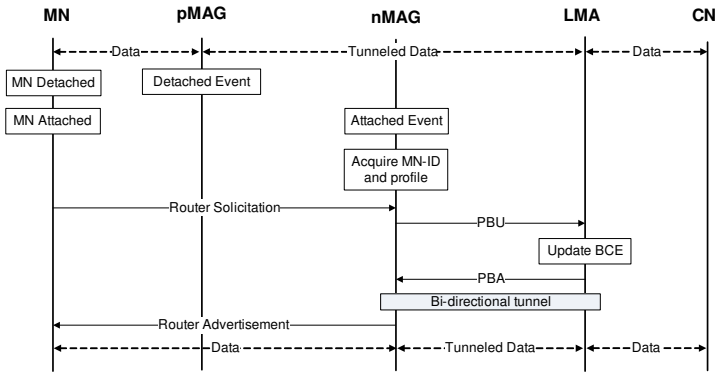


Figure 2.6 – Signaling when a mobile node performs a handover.

When the MN performs a handover from the previous MAG (pMAG) to a new one (nMAG), the similar process as in the registration step will be executed to update the MN's current location at the LMA (see Fig. 2.6). In this case, the nMAG obtains the same HNP prefix for this MN and can emulate the MN's home network (through sending RA messages with the same HNP). As a result, the MN is not aware of the mobility and continues to use the same IP address as before. Moreover, the link shared with a given MN of all the MAGs in the domain should be configured with the same link local address to make sure that the MN does not detect link changes as well as avoid the potential address collision issue [76] during the handover process.
Similar to FMIPv6, Fast Handovers for PMIPv6 (FPMIPv6) [78] provides a fast handover mechanism for PMIPv6 in order to minimize the handover latency and the packet loss. Again, a bi-directional tunnel is established between the previous MAG and the current one to forward the packets to/from the MN. Also, the MN should provide information about the target network to the pMAG through L2 signaling. However, it inherits potential risks of erroneous movement and out-of-order packets delivery problem from FMIPv6

Extensions to PMIPv6 Typically, the performance of a mobility management protocol is measured using such well-known metrics as signaling cost, handover latency, and packet

loss. The signaling cost consists of the location update cost and the packet delivery cost. Handover latency is defined as the total time needed to complete the handover procedures. During this time, the MN cannot send or receive any packets. The handover latency typically consists of layer 2 handover duration and layer 3 one. The packet loss is the amount of lost packets originated from or sent to an MN during its handover.
Various papers have been proposed which aim at improving PMIPv6 in terms of handover latency and signaling cost. In [79, 80], the authors applied the paging technologies to PMIPv6 to reduce the location update signaling cost for the mobile host in the idle mode. In [81], the authors used the Neighbor Discovery (ND) message of IPv6 to reduce the handover latency and packet buffering at the MAG. In this case, the pMAG sent the MN's profile to the neighbor MAGs through ND message. Similarly, in [82], the pMAG sent the MN's HNP to the adjacent MAGs in advance in order to perform the address configuration quickly after MN's handover. In [83], the improvement on handover latency was achieved by using the IEEE 802.21 Media Independent Handover services.
Similar to in MIPv6, in [84, 85], different route optimization schemes for PMIPv6 were also considered. Thus, the traffic could be routed in a better route bypassing the LMA. Unlike MIPv6, one of the main drawbacks of PMIPv6 is that the inter-domain handover is not supported. Thus, inter-domain mobility support in PMIPv6 has been proposed in [86, 87, 88, 21].

2.2.1.3 Mobility Management in the Current Cellular Networks

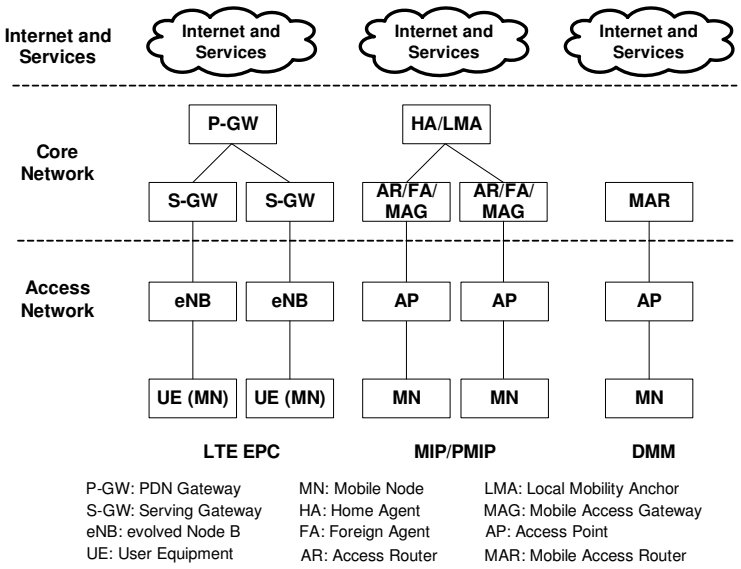


Figure 2.7 – Mobile network architecture.

The current mobile network architecture is highly centralized and hierarchical [64]. Following the hierarchical architecture, the network elements can be placed into three levels: Internet and services, core network, and access network. For example, the 3GPP cellular network consists of SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). The evolved packet core (EPC) network [89] includes a packet data network gateway (P-GW), serving gateway (S-GW), and evolved Node B (eNB) as shown in the leftmost of Fig. 2.7. Thus IP mobility protocols, such as PMIPv6 and DSMIPv6, which have been adopted as IP mobility protocols for the 3GPP EPC architecture, are inline with

the centralized and hierarchical of the network architecture.
Following the hierarchical architecture, the centralized mobility management protocols rely on the mobility anchor (HA in MIPv6 and LMA in PMIPv6) to enable the mobility support. Therefore, both the mobile context and traffic encapsulation need to be maintained at the mobility anchor. The number of mobile devices and their traffic demand increases exponentially make the centralized mobility management solutions encounter several problems and limitations as stated in [9, 10]. Among them, we just highlight the following issues:

- *Sub-optimal routing and end-to-end delay*: Since the data traffic always traverses the central mobility anchor, it often results in a longer route, especially when the CN and the MN are close to each other but far from the anchor. The same thing happens in case of Content Delivery Networks (CDN), in which the content providers place their data to the edge of the network. As a result, the end-to-end delay will be increased.
- *Scalability problem*: Maintaining MN's context and processing the packets from/to the MN usually require resources of the mobility anchor as well as the networks (require more bandwidth of the links close to the mobility anchor), thus reducing the scalability of the system.
- *Resource waste*: The mobility service is always provided even for the sessions that do not require the mobility management support e.g., the sessions which launch and complete while the node is connected to the same layer 3 point of attachment, or the sessions which can handle mobility at the application layer e.g., SIP-based sessions. Thus, by providing mobility support for the MN/service when it is really needed, the network resource (e.g., reducing signaling load) can be saved.
- *Reliability*: The central mobility anchor in general poses a bottleneck and single point of failure.

2.2.2 Distributed Mobility Management

As stated in the previous section, the mobile network is currently evolving towards the flat architecture. To cope with this evolution, distributed mobility management (DMM) solutions have been proposed. DMM concept aims at addressing the limitations of the centralized mobility approach (e.g., bottleneck and single point of failure, etc.) raised when a large number of mobile devices and data traffic are considered in a flat architecture [9, 10]. DMM is currently a hot topic which gains much interest from both the academia and the industry. The IETF has recently chartered the Distributed Mobility Management (DMM) working group[4] which specifies the solutions allowing for setting up IP networks supporting a distributed anchoring model. The key concepts of DMM are: i) the mobility is distributed among network entities and placed as close as possible to the MN e.g., at the router edge of the access network; and ii) the mobility management is dynamically provided for the sessions that really require service continuity.
Following the DMM requirement (REQ4) in terms of reusing/extending the existing IETF IP mobility protocols (i.e., MIPv6 and PMIPv6, and so on), the existing proposals (e.g., [90, 91]) aim at making these solutions work in a distributed manner by deploying multiple mobility anchors (HA in MIPv6 and LMA in PMIPv6) at the edge of the access network, serving as the default gateway of the mobile node. From the IETF point of view, there are two main groups of solutions: the host-based and the network-based. The host-based approach provides a global (as well as a local) mobility support for the MNs while the network-based provides a local mobility support for the MNs moving in a single domain.

[4]IETF DMM WG: https://ietf.org/wg/dmm/charter/

2.2.2.1 DMM from IETF Point of View

Host-based DMM Approach The terminology used by this subsection names an access router that provides the host-based DMM mobility support is a Host-based Mobile Access Router (HMAR). The HMAR, similar to HA, is a mobility anchor which allocates a network prefix to the MN and maintains the binding cache for its registered MNs. The current HMAR (cHMAR) is the one to which the MN is currently attached, while the anchor HMAR (aHMAR) of an address/session is the one where the prefix in use is allocated (and the session is initiated using this address as the source address).

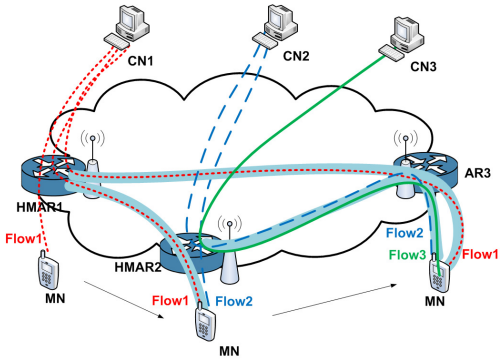
In the host-based approach, the MN is required to participate to the signaling process. There are two main schemes for the host-based approach. In the first scheme, the tunneling for the handover session is established between the anchor HMAR and the MN as similar to the MIPv6 protocol. In the second scheme, the tunnel is established between the current HMAR and the anchor one.

Regarding the first host-based DMM scheme as proposed in [92, 68], whenever an MN attaches to a HMAR it gets an IPv6 address. The cHMAR plays the role of HA for the address allocated at its network. While attaching to the cHMAR, the MN can start new communications (flows) with the CNs using the current address as the source address of the flows. These new flows are then routed in a standard way without the tunneling mechanism. When the MN performs a handover, if these ongoing flows are still alive, these flows are routed via the routers where the flows were originally initiated (aHMAR) using the tunneling mechanism. Thus, the MN needs to register its current topological location to each aHMAR (corresponding to each active HoA in use) by means of BU/BA messages. In this case, the current HoA actually plays the role of CoA. A bi-directional tunnel is then established between each aHMAR and the MN. Thus, the traffic passes through the mobility anchor via the bi-directional tunnel. Fig. 2.8 and Fig. 2.9 represent an example scenario of host-based DMM support.

It is noted that the MN should perform a location update process for each active IP address. As a result, it requires the MN to manage the list of active HoAs and the associated aHMARs, as well as the list of active sessions using the corresponding HoA. Moreover, the MN needs an additional mechanism which allows to select the right IP address to use for each session. The binding cache of the HMARs and the list of active sessions of the MN are illustrated in Fig.2.8b.

Additionally, as a global mobility, another scenario should be taken into account in which the MN moves to a typical access router's area (without supporting the host-based DMM) as discussed in [69, 67]. In this circumstance, the MN should select one among the active IP addresses to be served as the source address, and the associated aHMAR as the HA. The MN then performs the normal MIPv6 operation. For example, as shown in Fig.2.8, the MN attaches to a typical access router (AR3). After getting a prefix (Prefix3::/64), the MN configures its IP address (Pref3::MN/64). When the MN starts a new session (Flow3), it selects HoA2 and HMAR2 as the source address and the corresponding HA, respectively. As a result, the Flow3 is routed via the tunnel HMAR2-MN. Regarding the ongoing flows, the Flow1 and Flow2 are then routed via HMAR1 and HMAR2 using the tunnel HMAR1-MN and HMAR2-MN, respectively.

As stated earlier, the MN needs to inform all active aHMARs about its current location by means of BU/BA messages. Thus, the mobility signaling cost (over the air) is relatively high. As a result, the second host-based DMM scheme is proposed in order to reduce the mobility signaling cost of the MN (see Fig.2.10). In this case, the MN only needs to exchange the BU/BA messages with the current mobility anchor [66]. The BU includes the MN's prefixes in use and the corresponding aHMAR. Based on this information, the BU/BA messages



(a)

HMAR1's Binding Cache

HoA	CoA
Pref1::MN	Pref3::MN

HMAR2's Binding Cache

HoA	CoA
Pref2::MN	Pref3::MN

MN's Binding List

HoA	Anchor	Flow
Pref2::MN	HMAR2	Flow3
Pref2::MN	HMAR2	Flow2
Pref1::MN	HMAR1	Flow1

(b)

Figure 2.8 – Mobility management in the host-based approach (scheme 1): (a) Operation description. (b) Binding cache.

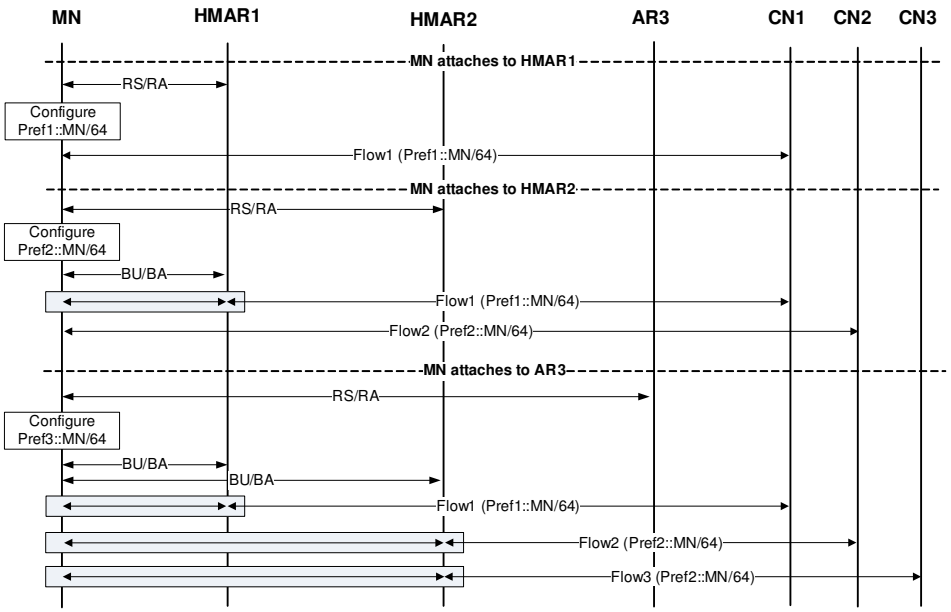
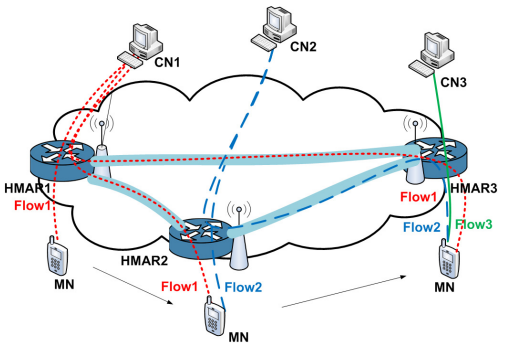


Figure 2.9 – Signaling for the mobility management in the host-based approach (scheme 1).

are exchanged between the cHMAR and each aHMAR which allows establishing the tunnel between them. The active sessions are then routed via the corresponding aHMAR utilizing the tunneling mechanism. Again, if the MN moves to a typical AR's area, the tunnel is established between the MN and the aHMAR as similar to the previous host-based scheme.

It is important to note that the MN keeps the information of the active HoAs and their associated aHMAR when having at least one active session using this HoA. Otherwise, the information will be deleted. Thus, in this thesis, we suggest that at least one HoA should be considered as a global address and should be kept throughout its lifetime e.g., an address allocated at the MN's typical location.



(a)

HMAR1's Binding Cache

HoA	Tunnel
Pref1::MN	HMAR3

HMAR2's Binding Cache

HoA	Tunnel
Pref2::MN	HMAR3

HMAR3's Binding Cache

HoA	Tunnel
Pref1::MN	HMAR1
Pref2::MN	HMAR2
Pref3::MN	Null

MN's Binding List

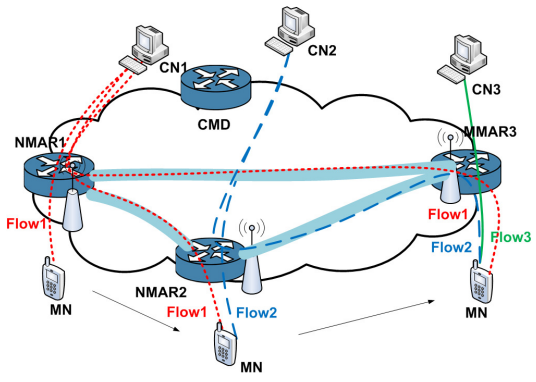
HoA	Anchor	Flow
Pref3::MN	HMAR3	Flow3
Pref2::MN	HMAR2	Flow2
Pref1::MN	HMAR1	Flow1

(b)

Figure 2.10 – Mobility management in the host-based approach (scheme 2): (a) Operation description. (b) Binding cache.

Network-based DMM approach Unlike the host-based DMM, the network-based approach does not require the MN to participate in the mobility signaling process. To do so, a new network entity, namely Network-based DMM Access Router (NMAR) is introduced. The NMAR is an access router supporting the network-based DMM mobility. The NMAR thus performs both LMA's and MAG's functionality. Acting as a MAG, the NMAR detects the attachment of the MN, while as an LMA it allocates a HNP to the MN. Again, we introduce two logical NMARs: i) a current NMAR (cNMAR) is the NMAR to which the MN is currently attached; and ii) an anchor NMAR (aNMAR) is the NMAR to which the MN's HNP is allocated (the session is initiated).

Similar to the host-based DMM, when an MN attaches to a NMAR, it obtains an IPv6 address. Typically, it uses the current IP address to start new sessions. The data traffic is routed using the normal IP routing without any tunneling mechanism. If the MN performs a handover and some sessions are still alive (namely handover sessions), the mobility management procedure is activated as follows. The cNMAR, acting as the MAG, exchanges PBU/PBA messages with the aNMAR which acts as the LMA of the flows initiated at the aNMAR. Once the PBU/PBA signaling is completed, a tunnel is established between the cNMAR and the aNMAR for the sessions initiated at the aNMAR. However, an important question raised is that how the nNMAR learn about the addresses of the aNMARs.



(a)

NMAR1's Binding Cache

HoA	P-CoA
Pref1::MN	NMAR3

MN's Binding List

HoA	Anchor	Flow
Pref3::MN	NMAR3	Flow3
Pref2::MN	NMAR2	Flow2
Pref1::MN	NMAR1	Flow1

CMD's Binding Cache

MN_ID	(Prefix, Anchor)	Current
MN_ID	(Pref3::, NMAR3), (Pref2::, NMAR2), (Pref1::, NMAR1)	NMAR3

(b)

Figure 2.11 – Mobility management in the PMIP-based approach: (a) Operation description. (b) Binding cache.

There is several mechanisms allowing the nNMAR to know the address of the aNMARs. The first method [90] relies on a centralized database (namely centralized mobility database, or CMD) which stores the mobility-related information of each MN in the domain such as the list of MN's HoAs, the associated aNMARs' address as similar to in [93]. Although it ensures that the mobility process is totally transparent to the MN, this mechanism introduces again a centralized anchor, however, for control plane only. The data plane is still fully distributed among the network entities. That is the reason why this scheme is considered as a partially distributed scheme. The second method relies on the information provided by the MN as specified in [65]. In other words, the NMAR retrieves the address of the anchor NMARs from the MN. As a result, the MN is no longer transparent to the mobility process. Therefore, in some papers [69, 66] this method is considered as a host-based scheme as stated above.

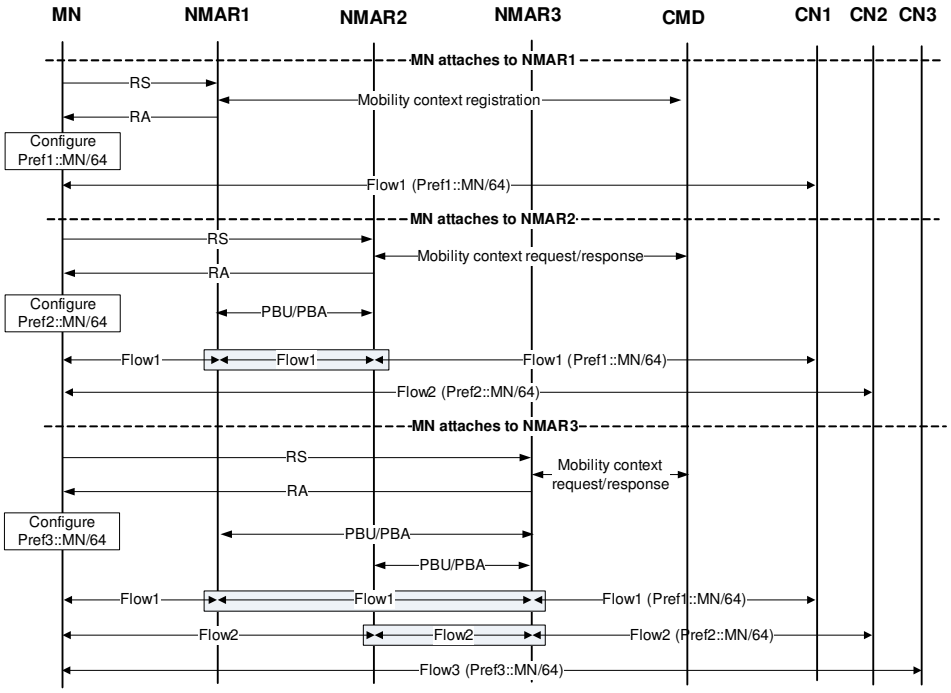


Figure 2.12 – Signaling for the mobility management in the network-based approach.

The diagram in Fig. 2.12 depicts the operations of the partially distributed DMM. When an MN attaches to the network-based DMM domain (for example at NMAR1), after detecting the presence of a new MN by means of receiving a RS message (including the MN's ID), the NMAR1 allocates a HNP (Pref1::/64) for the MN. It then sends a mobility context request (MC-Req) message including the MN_ID and the Pref1::/64 to the CMD to register the new prefix and retrieve the existing mobility context of the MN (if exist). The CMD then checks its mobility database for this MN. Since it is the first time the MN is attached to this domain, there is no entry for it. Therefore, the CMD creates an entry (for the MN) including the MN_ID, Pref1::/64 and the associated NMAR (NMAR1). The CMD sends a mobility context response (MC-Res) message indicating that the information of the MN is successfully registered. Afterwards, the NMAR1 sends a RA including the allocated prefix (Pref1::/64) to the MN. Based on this information, the MN configures its IPv6 address (Pref1::MN/64) and starts a new communication with the CN1 (Flow1), following the normal way. As the MN moves to the access network of NMAR2, the NMAR2 allocates a

new HNP (let say Pref2::/64) for the MN. It then sends a MC-Req message to the CMD for the new prefix registration and for retrieving the existing mobility context of the MN. Upon receiving the MC-Req message and searching its mobility context table, the CMD updates the MN's mobility entry corresponding to the new prefix (as in Fig. 2.11). The CMD then replies by a MC-Res message including the MN_ID and the list of its active prefixes, and the associated NMARs (in this case is Pref1::/64 and NMAR1). Upon the reception of the MC-Res message, the NMAR2 updates its BCE and routing for Pref2 and sends a RA to the MN which includes the Pref2::/64. The PBU/PBA messages are then exchanged between the NMAR2 and the NMAR1 to sets up the bi-directional tunnel between them for the Flow1. Regarding the MN, after receiving a RA, it configures its IP address (Pref2::MN) and uses it to start a new communication with the CN2 (Flow2) in a normal way. The similar thing happens when the MN moves to NMAR3. In this case, the Flow1 and Flow2 are routed through the NMAR1 and NMAR2, respectively. In the mean time, the Flow3 which is initiated when the MN attaches to NMAR3, is routed in a normal way without the tunneling mechanism.
Besides, there are proposals which apply the DMM concepts into the PMIPv6 domain. For example, in [94], the locally assigned prefixes mechanism within a PMIPv6 domain is proposed. In this case, the MAG can attribute its own prefix (the so-called local prefix) to the MN which can be used for the communication by passing the LMA when the MN is currently attached to the MAG. The MN can still use the IP address allocated by the LMA in a typical PMIPv6 way.

2.2.2.2 DMM Consideration in 3GPP

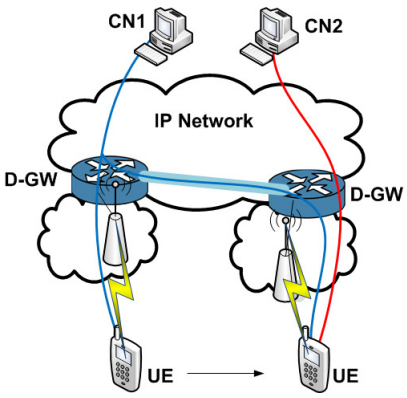


Figure 2.13 – Mobility management for 3GPP

In order to deal with a huge number of traffic demands as well as the revenue per data decreasing phenomenon, 3GPP proposes such traffic offload mechanisms as SIPTO, LIPA and IP Flow Mobility (IFOM). The main idea is that the user data can be routed bypassing the core network based on certain conditions. In more details, SIPTO supports offload of certain types of traffic directly to the Internet and away from the mobile core network. It is done by selecting a set of S-GWs and P-GWs that are geographically/topologically close to the User Equipment's point of attachment (UE is an MN following the 3GPP terminology). However, the offloaded traffic cannot access the operator services. On the other hand, LIPA enables a UE connected via a Home eNB (HeNB) to access the IP capable entities in the same residential/enterprise IP network without the data traversing the mobile operator's core. Although, SIPTO/LIPA is similar to DMM in terms of traffic offloading (mitigating the traffic aggregation at the core network), there is a limited mobility support. For ex-

ample, LIPA supports only the mobility between HeNBs managed by the same Local-GW (L-GW) while SIPTO enables mobility support for the case S-GW/P-GW is at/above Radio Access Network (RAN). In other words, 3GPP has not yet considered the mobility of UE, which may result in service disruption when a UE is on the move. In fact, SIPTO/LIPA can be considered as a step towards DMM from conventional centralized/hierarchical approaches. It comes from the fact that based on SIPTO/LIPA the functionality of P-GW is distributed by deploying multiple L-GWs. In the next step, by re-using the existing S5 interface (PMIPv6 tunneling), the mobility between the L-GWs can be enabled. From that point, it is feasible to support DMM in LTE/SAE by simply installing the DMM functionality at the distributed L-GWs (called Distributed Gateway or D-GW) as illustrated in Fig. 2.13.

2.2.3 Other Considerations

2.2.3.1 Mobility across Heterogeneous Networks

With the evolution of mobile communication systems (wireless technology and network architecture), heterogeneous networks provide the possibility to greatly increasing capacity at a low cost. In this context, the seamless mobility across different types of wireless access technology e.g., WLAN, WiMAX and LTE needs to be taken into account. Regarding the network infrastructure, IEEE 802.21 Media Independent Handover (MIH) services allow optimizing the handovers between heterogeneous IEEE 802 and cellular networks. The handover performance can be enhanced using the layer-2 information available from IEEE 802.21 services. From the mobile node point of view, to maintain the session continuity, additional techniques (as specified in [17]) should be considered which allow the MN to obtain the same IPv6 address after handover across different access technologies. Among them, the logical interface technique [95] can help to hide the different access technologies, thus, the changing of interface is transparent to the IP stack. Moreover, the interfaces of the MN can be active at the same time, which helps reducing the handover latency.

2.2.3.2 Network Mobility

Network Mobility (NEMO)[5] refers to the mobility of an entire network which changes its point of attachment to the Internet. Thus, the main purpose of NEMO support is that it allows every node in the mobile network to be reachable while moving around. Moreover, the mobility should be transparent to the nodes insides the mobile network. The basic network mobility support is based on MIPv6 to enable the network mobility in an IPv6 network.

In order to provide the mobility support for a Mobile Network, a specific gateway called Mobile Router (MOR) is introduced. The MOR will be connected to the fixed infrastructure and provides connectivity to the nodes inside the Mobile Network. Like the mobility support of a mobile node (host-based approach), the NEMO basic support (as specified in [96]) is also based on the bi-directional tunnel between the MOR and its HA to enable mobility support when the MOR is away from home. Thus, as a topological anchor point of MOR's address, the data packets addressed to the mobile network are delivered to the HA, which then tunnel them towards the MOR. The MOR, after removing the tunnel headers, forwards the data packets to the destination inside the mobile network. Note that similar to normal MIPv6 operation where the binding association between the HoA and the CoA is maintained in the Binding Cache, in NEMO, the HA might also keep the Mobile Network Prefixes (MNP)

[5]NEMO IETF WG: http://datatracker.ietf.org/wg/nemo/

in the corresponding BCE. As a result, in a large-scale development, the MNP allocation should be considered as in [97].

2.2.3.3 Comparison between the Mobility Management Approaches

As stated earlier, the performance of a mobility management protocol is typically measured using such metrics as signaling cost, handover latency, and packet loss. Based on these metrics, various papers have been presented to evaluate the performance of the mobility management protocols.
Comparative performance analysis for the host-based mobility management protocols e.g., MIPv6, FMIPv6, HMIPv6 and F-HMIPv6 in terms of signaling cost, handover latency, and packet loss has been carried out in [98, 72, 99]. In [73, 100, 101], the authors also took into account the network-based mobility management protocols e.g., PMIPv6 and FPMIPv6 in the comparative performance analysis. From these analysis, some conclusions are: i) Using layer 2 information generally helps to reduce the handover latency and packet loss at a cost of signaling overhead. However, it depends on each link-layer technology; ii) The network-based mobility management protocols reduce the signaling overhead over the air of the MN compared to the host-based mobility protocols; and iii) Typically, the handover latency and the signaling cost depend on the network topology in use. In other words, the hop distance between the network entities is an important factor influencing the performance of these protocols.
Regarding DMM, a lot of research publications [64, 65, 66, 67, 68, 69] have carried out the analysis on different DMM approaches, compared them with the conventional mobility managements in terms of signaling cost, packet delivery cost, handover delay, packet loss and end-to-end delay. The results from these analysis showed that DMM is a promising mobility management scheme. In details, in [64] the authors conducted a simulation to compare DMM and MIPv6 (with handover optimizations). The simulation results showed that DMM outperforms MIPv6 in terms of handover delay and TCP delay. In [66], both qualitative and quantitative comparison for centralized mobility management protocols and DMM protocols are provided. Also, the comparison in terms of handover latency, signaling cost and data delivery cost has been conducted in [67].

2.3 IP Mobile Multicast

The increasing penetration of the mobile devices, such as tablets and smart phones is generating a huge number of data traffic over mobile networks. The majority of this traffic is video data: estimates say that mobile video traffic will account for 66.5% of total mobile data traffic by 2017 [1]. In this context, the scalability and the bandwidth efficiency from the multicast routing make the IP multicast a remarkable solution from application point of view to allow mobile networks to deal with a huge number of traffic, particularly in mobile environments where users usually share frequency bands and limited capacity [11]. In other words, when a large group of users is simultaneously interested in the same content, the multicast can provide significant advantages compared to the unicast in terms of resources efficiency both from the perspectives of the network and of the servers [28]. However, one of the major challenges for multicast support is when mobility is considered.
About the IP mobile multicast, after more than a decade of research and development efforts, many approaches have been proposed, but most of them are based on such host-based mobility management protocols as MIPv6, FMIPv6 and HMIPv6. However, the main drawback of these host-based mobility management protocols is that they require the MN to modify its IP stack to participate into the mobility signaling process. As a result, the

previous IP multicast approaches introduced in [11, 12] cannot be directly applied in a network-based mobility management in which the MN is unaware of the mobility process. Recently, a base development of multicast listener support in PMIPv6 has been adopted by the IETF. However, it does not provide any specific optimization and performance enhancements such as service disruption and packet loss, sub-optimal routing, and packet duplication. Several solutions have been proposed in order to address couple of issues. In this section, we give a brief overview to the multicast mobility-related problems and enlist some possible solutions in MIPv6 to highlight the main idea of these proposals. Based on that, we then take a deep analysis on the multicast mobility in a PMIPv6 and a DMM environment.

2.3.1 Overview of Multicast Mobility in Mobile IP

In order to enable multicast in Mobile IP (both Mobile IPv4 and Mobile IPv6), two basic approaches have been proposed i.e., bidirectional tunneling and remote subscription. Both approaches have their own advantages and drawbacks. The bidirectional tunneling hides the movement of the multicast nodes by tunneling the multicast traffic via the mobility tunnel between the node and its HA at the cost of triangular routing (leading to a long delay) and tunnel convergence problem. On the other hand, in the remote subscription approach, the multicast node has to rejoin the on-going multicast sessions after each handover, leading to the potential significant service disruption. In addition, more serious problems can be raised in case of source mobility such as address transparency and routing state maintenance [11, 12]. Further enhancement should also be considered in order to meet the additional requirements in terms of service disruption and packet loss for the real-time services. Therefore, various methods have been proposed to improve the two essential solutions. In [12, 11], the authors provides a survey of numerous proposals for the multicast listener as well as the source mobility.

From listener point of view, several solutions [102, 103, 104, 105] have been proposed to construct an efficient multicast delivery tree. In more details, the Mobile Multicast Protocol (MoM) [102] aims at solving the tunnel convergence problem by selecting one HA which serves as a common HA (per group) for all listeners subscribed to a multicast group at the same visited network. In other words, a single tunnel between the selected HA and the FA is used for multicast delivery between the home network and the foreign network. The Range-Based Mobile Multicast (RBMoM) [103] trades off the shortest delivery path and the frequency of multicast delivery reconstruction, however, it introduces much of complexity. The Multicast Protocol With Dynamic Service Range (MPDSR) [104] enhances RBMoM to reduce the number of multicast tree reconstructions and multicast service disruption time. In general, MoM, RBMoM and MPDSR can be considered as an enhancement of the bidirectional tunneling approach. The Multicast By Multicast Agent Protocol (MMAP) [105], as an enhancement of the remote subscription approach, uses the tunnel between the previous foreign network and the current one for delivering the multicast traffic to reduce the tunnel convergence problem and the service disruption. In [106], the authors proposes combining the bidirectional tunneling and the remote subscription. They also discusses the practical aspects of the bidirectional tunneling approach. Besides, [107, 108, 109] mainly aim at addressing the problem of packet loss and multicast service disruption by extending the fast handover protocols for multicast support.

From multicast source point of view, the bidirectional tunneling approach preserves the transparency of the movement of the source. However, it suffers the triangular routing, long service latency, and inefficient in packet delivery which impact the overall listeners. The remote subscription approach helps to address these issues, yet, the movement of the

source causes the address transparency and tree reconstruction. Thus, the multicast routes should be updated to reflect the current location of the source in an appropriate manner to effectively avoid the packet loss. There are two main types of solution in which the traffic will be injected to the old tree or the overall delivery tree will be reconstructed [11]. The additional complexity is raised in case of SSM. For example, in [110, 111], the authors propose a tree morphing protocol to address the address transparent issue allowing a continuous adaptation of multicast shortest path trees to the source mobility. However, the complexity and high signaling cost could be added, as all the MRs need to be extended. Similarly, in [112], the authors propose a state update mechanism by reusing the legacy multicast tree for a minimization of packet delay. In [113], the authors, based on the Host Identity Protocol, introduce multicast routing states which is independent of IP addresses. Further approaches can be found in [12, 11, 114].
Since all these mobile multicast protocols are designed for MIPv4 and MIPv6 which require the mobile nodes to participate in the signaling process, they cannot be directly applied to PMIPv6. Yet, the idea of these solutions can be re-used.

2.3.2 Multicast Mobility in PMIPv6

As the multicast protocols (group management and routing protocols) are originally designed for a fixed network, considering multicast in a mobile environment brings several challenges to the multicast service. The mobility of the node (e.g., the change of point of attachment and of globally reachable IP address) has different impacts on the multicast service, depending on such factors as the role of the node in the multicast session (source or listener), the considered multicast model (ASM or SSM), the multicast routing protocol, the multicast group management protocol and the mobility protocol in use as well as the wireless access technology. Therefore, the IP mobile multicast issues can be divided into four main groups: the general multicast problems (due to multicast protocols), the specific mobile listener problems, the specific mobile source problems and the deployment issues [11, 12, 115].

2.3.2.1 Multicast Mobility Issues

Prior to taking more details on the multicast mobility issues, we will look at some requirements of the multicast support in PMIPv6. First, the session continuity should be provided when a listener/source moves from one IPv6 subnet to another. In addition, the noticeable service disruption and the significant packet loss should be avoided during handovers. Especially, in the context of a network-based mobility management protocol, the mobile node should remain unaware of mobility from the network layer and the application point of view. Then, it is desirable to preserve the characteristics of multicast such as effectiveness of delivery (to avoid traffic duplication and tunneling overhead) and approximate optimal routing.

General Issues At the beginning, the multicast protocols are designed for a fixed environment using wired connection. Thus, considering these protocols in a mobile and wireless environment can raise several challenges. Particularly, considering the multicast group management protocols (IGMPv3 and MLDv2), which typically work in the wireless access network (MN and first hop AR), may lead to such issues as the multicast-related signaling overhead, the multicast service disruption and the long leaving latency [115]. Additionally, wireless is typically an unreliable media, that means variable bandwidth or packet losses, and overall wireless communications are more costly (both in power and processing

overhead). As such, the tuning of MLDv2 parameters (timers and values) [115] must be considered for obtaining an improved multicast service stability and for a better behavior during handovers. Regarding multicast routing protocols, the movement of source and listener results in several issues such as tree reconstruction, routing state maintenance and tunneling, etc [12]. Specifically, the tree reconstruction may lead to a long service disruption time and a significant packet loss. Adding to that, it is not easy to modify the multicast routing protocols according to mobility requirements.

Specific Multicast Listener Mobility Issues The mobility of a listener causes several issues for the multicast service. The issues and the possible solutions are described as follows:

- Service disruption and packet loss: Since the mobile node in the network-based mobility management is not aware of the mobility process, it cannot make multicast-related decisions, preventing a smooth multicast session resume. As a result, when a listener moves to a new MAG, it has to wait to express its interest in subscribing to the ongoing multicast channels until it receives an MLD Query (from a Querier). Thus, it experiences a certain delay in receiving multicast content due to the extra time related to the multicast service activation, the MLD Query/Report transmission (especially the multicast service activation which is typical in seconds). In other words, beside the layer 2 and layer 3 handover latency, the extra delay related to multicast service is added to the total latency. Also, if no buffer mechanism is used, the multicast traffic is discarded during handover, causing packet loss. This issue becomes more serious when the real-time services are considered, but can be reduced by using the context transfer function [14, 15, 116].

- Packet duplication: In some cases, the MAG can receive the same multicast packet from different LMAs or MRs. This happens when different tunnels MAG-LMA are used to deliver the multicast traffic. One possible solution is implementing MLD proxy with multiple upstream interfaces at MAG. Other possibility is taking advantage of the native multicast infrastructure to deliver multicast traffic, thus bypassing the tunnel [117].

- Sub-optimal routing and end-to-end delay: When the multicast traffic has to pass through the central mobility anchor (LMA), it often results in a longer route. Consequently, the end-to-end delay will be increased. This issue should be taken into account especially when the real-time and delay sensitive services are considered.

- Leave latency or network resource waste: Since the listener is unaware of mobility, it will not send an MLD report for explicitly leaving the group in the previous MAG (pMAG). As a result, if the last member of a multicast group moves to another MAG, the pMAG will continue to deliver the multicast traffic until it updates its membership information. Thus, it causes waste of network resource. Using the explicit tracking function [51] and the context transfer, in this case, could help.

In addition, the listener can receive the packet out of order due to handovers. In many wireless regimes, multicast-related signaling should be minimized to reduce the power consumption (of a limited capacity mobile devices) and network resource (with a limited capacity) in use. Again, tuning the MLD parameters [115] should be carefully investigated as a trade-off of signaling overhead and service disruption as well as waste of resources issue.

Specific Multicast Source Mobility Issues From a source point of view, it inherits some problems of the multicast listener mobility such as service disruption, packet loss and sub-optimal routing. Particularly, since the movement of a multicast source between different networks could impact overall multicast delivery tree, it may cause more severe problem in terms of service disruption and packet loss if multicast tree needs to be reconstructed. As in PMIPv6, the source keeps its IPv6 address when moving across a PMIPv6 domain, the address transparency issue is avoided. However, if the multicast traffic is routed directly from the MAG bypassing the LMA, it may lead to several issues such as packet overhead, encapsulation/decapsulation cost, source register tunnel management and sub-optimal routing [41, 118]. Additional issue may be raised from the multicast scoping and source active when considering inter-domain mobility. The impact of source mobility, in general, strongly depends on the multicast deployment scenario as well as the multicast model considered (ASM or SSM). In SSM, the traffic follows the shortest path tree rooted at the source to the listeners. As in PMIPv6, LMA always acts as a topological anchor of the source's address, the traffic has to pass the LMA after forwarding to the listeners. It leads to the non-optimal route. As a result, additional mechanisms are required to enable the optimal route in case of SSM. However, the simplicity feature, as a main advantage of SSM, should be taken into account. In ASM, the presence of the RP can help to hide the mobility of the source since the source address is preserved when it attaches to the PMIPv6 domain. However, when the listener's DR decides to switch to the shortest-path tree, the similar issues as in SSM should be considered.

Deployment Issues After more than a decade of important research and development efforts, IP multicast, in general, has been slowly deployed on the global Internet (lagging but still growing). The barrier of widespread deployment of multicast applications mainly comes from technical, administrative and business related issues as stated in [31]. Therefore, several alternative techniques for multicasting have been proposed [31], in which each alternative can be suitable for a specific environment. For example, the application-layer multicast (ALM) [32] in which the multicasting functionality is implemented at the application layer instead of at the network layer as IP multicast, does not require the change in the network infrastructure. Data packets are replicated at the end hosts, instead of the network routers as in IP multicast. ALM is suitable, for example, for the MANET applications. Although ALM is much easier to deploy compared to IP multicast, IP multicast over performance the ALM (as well as other alternatives) in terms of robustness, security, performance, and scalability [31]. The recent business models, a huge traffic demand (especially multimedia traffic), the revenue per data reducing phenomenon in the mobile operator networks, as well as the advantages of new multicast model (SSM) bring again the strong interest of IP multicast from both academic and industry communities. IP multicast is expected to play more important role in the future networks.

2.3.2.2 Solutions from the IETF Point of View

Following a typical multicast deployment architecture, multicast support can be enabled by deployed an MLD proxy and an MR function in the domain. In general, different proposals for multicast mobility in PMIPv6 are derived from the mapping the location of MAG and LMA into the typical multicast deployment architecture, as shown in Fig. 2.14. As a result, there are three approaches corresponding to the different roles of MAG and LMA as: i) MAG and LMA act as an MLD proxy and an MR, respectively; ii) MAG acts as an MLD proxy while LMA as an additional MLD proxy; and iii) MAG and LMA play the role of an MR.

The first approach, which is considered as a base solution by the IETF, enables the multicast support by deploying MLD proxy and the multicast routing function at MAG and LMA, respectively. This solution can also be considered as a tunnel-based solution due to the fact that the multicast traffic is routed via the mobility tunnel between LMA and MAG. In addition, LMA can also act as an additional MLD proxy (in the second approach). In the third approach, by deploying multicast routing at MAG, several issues can be avoided (e.g., sub-optimal routing, tunnel convergence problem) at a cost of operation and deployment from the multicast routing.

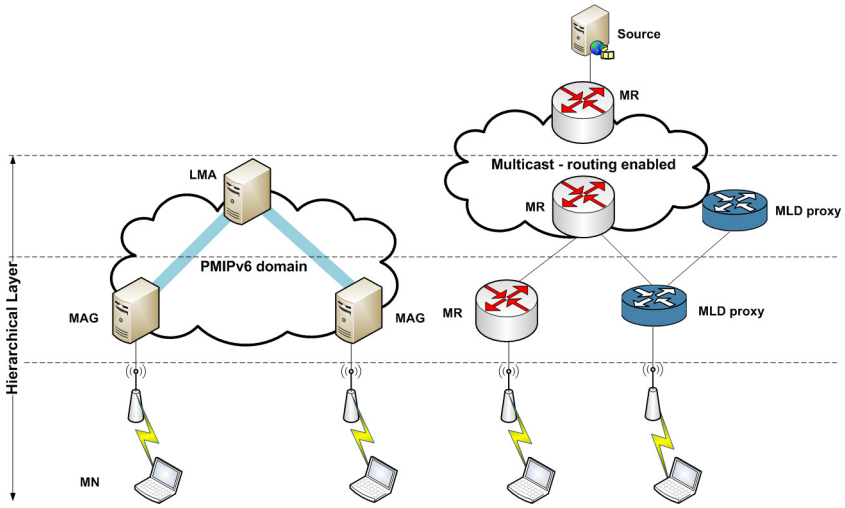


Figure 2.14 – Mapping PMIP entities into the multicast architecture

At the time PMIPv6 protocol was developed, it does not explicitly address the multicast communication. Consequently, a new IETF group, namely MultiMob[6], has been chartered for supporting multicast in a mobile environment. At this stage, the PMIPv6 multicast listener support was standardized while the multicast sender support is still under discussion.

Solutions for Multicast Listener Mobility

This subsection presents different possible solutions for multicast listener mobility in PMIPv6 mainly from the IETF point of view. Starting with a base solution which does not take any performance and optimization issues into account, we then consider the solutions for some specific issues as stated in the previous subsection.

Base Solution for Multicast Listener Mobility in PMIPv6 Recently, a base solution [119] has been standardized by the IETF for supporting multicast listener mobility in PMIPv6 without modifying the mobility and multicast protocol standards. It provides multicast listener support in PMIPv6 by placing MLD proxy function at MAG while LMA acting as an MR or an additional MLD proxy (see Fig. 2.14). The MLD proxy function is implemented at MAGs with the upstream interface being configured to the corresponding mobile node's LMA (ingress interface). As a typical MLD proxy operation, the multicast data arriving from an upstream interface will be forwarded to the downstream interfaces which have appropriate forwarding states for this group. Thus, all multicast traffic will pass through the MAG-LMA tunnel, just like the unicast traffic. This solution can be considered as a tunnel-based one. After each handover, the multicast traffic continues to

[6]MultiMob WG: http://datatracker.ietf.org/wg/multimob/charter/

deliver to the listener at the new MAG, and the service continuity is guaranteed accordingly. In addition, from the multicast service point of view, the listener remains unaware of the mobility. It is achieved since the new MAG, after obtaining the listener's subscription information by using the normal MLD operations, joins the on-going multicast flows on behalf of the listener. The base solution can be also applied for the multicast source [118]. Note that the LMA can also work as an additional MLD proxy, serving multicast traffic for the PMIPv6 domain. However, from the listener and the MAG perspective, there is no difference. Therefore, without loss of generality, we only consider the case where the LMA acts as an MR.

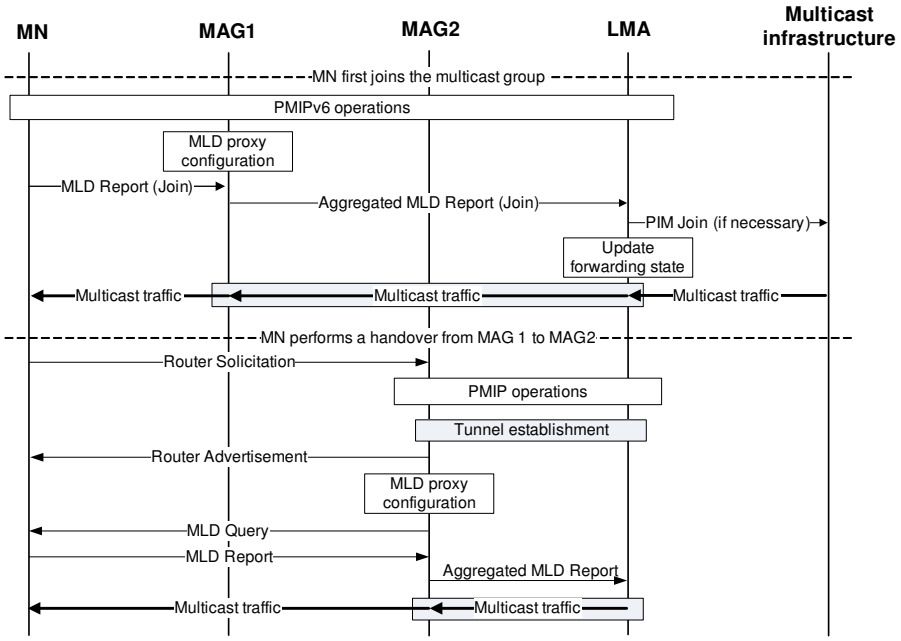


Figure 2.15 – Base solution for multicast listener mobility in PMIPv6.

Fig. 2.15 describes the multicast-related signaling for the base solution. When an MN is initially attached to a PMIPv6 domain (for example, attaches to MAG1), first, the standard PIMPv6 operation will be executed (e.g., MN's address configuration, MN's location update, tunnel establishment, for more details see Section 2.2). MAG1 then creates an MLD proxy instance (if necessary) which serves as an upstream router for all the nodes associated with the MN's LMA. Note that every MAG-LMA tunnel is a part of a separate MLD proxy domain. The proxy instance adds the MN to its downstream interface and configures its upstream interface towards the MN's LMA. When the MN expresses its willingness in receiving the multicast traffic from a group, it sends an MLD Report to MAG1. MAG1 then sends an aggregated MLD Report message to the LMA to join the group on behalf of the MN. The LMA, acting as an MR, joins the group from the multicast infrastructure, and updates its multicast forwarding state. After receiving the multicast packets, the LMA forwards them to the appropriate MAGs according to its forwarding state (via the LMA-MAG tunnel). MAG1 forwards the packets to the appropriate downstream interfaces and they finally reach the MN.

In case of handover (from MAG1 to MAG2), the basic PIMPv6 operation will be executed. Since the mobility is transparent to the MN, the MN will not send the unsolicited MLD Reports. Instead, MAG2, upon the detection of a new MN on its access link, adds the MN

to a downstream interface, and sends MLD General Query messages on its attached link. The MN then replies by an MLD Current State Report message indicating its current active multicast groups. Based on that, MAG2 can send an aggregated MLD Report message to the corresponding LMA to join the groups on behalf of the MN (in case MAG2 is not receiving such those multicast groups). After updating the multicast forwarding state, the LMA forwards the multicast packets to the appropriate MAGs (including MAG2). The multicast packets finally reach the MN.
Although the base solution is a simple way to enable the multicast support in PMIPv6, it does not address any issues as specified in the previous section. In more details, the utilization of tunnel for multicast flow results in the traffic redundancy (or the tunnel convergence problem) at the MAG. It is because different nodes, which attach to the MAG and associate to different LMAs, can subscribe to the same multicast group. There are several solutions for this issue such as extending MLD proxy to support multiple upstream interfaces [120], or using the direct-routing approach [117]. Also, since a lot of operations need to be executed to allow the MN to continue receiving the multicast traffic at the new MAG, it may cause a long service disruption and high number of lost packets. This issue can be mitigated by either using the context transfer from previous MAG/LMA to the new MAG [14, 116] or tuning the behavior of MLD for routers [115]. In addition, as the multicast traffic always passes through the MN's LMA, it may cause the sub-optimal routing problem. Possible solutions for this problem can be a localized multicast traffic and using a direct routing.

Direct-routing Solution In order to provide an optimal connectivity to a local content, the direct routing approach which uses native multicast infrastructure locally in a PMIPv6 domain is proposed [117]. In this case, the MLD proxy is implemented at MAG in which the upstream interface is configured towards an MR in the multicast infrastructure. Therefore, the direct routing approach helps avoid the tunnel convergence problem. One of the most important advantages of this approach is that multicasting functions are totally separated from the mobility anchor by using the native multicast infrastructure. As the result, the complexity of LMA is reduced since it does not have to deal with the multicast traffic processing. In addition, this approach may not make any packet overhead (tunneling overhead) as the multicast traffic is not transferred via the mobility tunnel. However, if the tunneling mechanism is used to set up the upstream interface of the MLD proxy towards an MR, the tunneling overhead can be re-introduced [117].
The multicast-related operation in the direct-routing approach is briefly expressed as follows. Once an MN is attached to MAG1, similar to the tunnel-based approach, a proxy instance at MAG1 adds the MN to a downstream interface and configures its upstream interface towards an MR in the multicast infrastructure. Again, when the MN expresses its interest in receiving the traffic destined to a multicast group, MAG1 sends an aggregated MLD Report message to its upstream MR to join the group on behalf of the MN. Afterwards, the multicast traffic traverses the multicast infrastructure and reaches the MN. The MN then performs a handover to the new MAG, namely MAG2. Since the MN is unaware of the mobility process, it has to wait until receiving an MLD Query to inform its multicast information state to MAG2 by means of the MLD Current State Report message. MAG2 then joins the multicast delivery tree on behalf of the MN. MAG2 has to get the multicast traffic from an MR in the multicast infrastructure which already has a multicast forwarding state for this group. In other words, the multicast delivery tree needs to be reconstructed. Thus, it may result in a noticeable service disruption and packet loss. Some mechanisms are required to make sure that the multicast session continues right after the MN is attached to the new MAG and minimize the overhead in reconstructing the multicast trees. To tackle

these issues, in [117], the authors propose to use a common upstream MR for all MAGs in the domain. Additionally, MAG can implement the MR functionality, in this case, MAG belongs to the multicast-enabled domain.
In the same document [117], the authors propose separating the multicast from PMIPv6 unicast to solve the tunnel convergence problem. In more details, the multicast tree mobility anchor (MTMA), acting as an MLD proxy or an MR, is introduced to serve as a topological anchor point for the multicast traffic. In other words, while the multicast traffic is served by the MTMA, the unicast traffic is served by the typical LMAs. Typically, the MTMA would be used to get access to the remote multicast content, while direct routing to the local multicast content. In this case, PBA message should be extended to convey dynamic policies on subscription via MTMA/direct routing.

Additional Considerations

In case of handover, several operations should be executed so that the MN can continue receiving the multicast traffic from the nMAG: i) Typical PMIPv6 operations (e.g., exchanging PBU/PBA, tunnel establishment and address configuration); ii) Acquisition of the MN's multicast subscription information at the nMAG: Since the mobility is transparent to the MN, the service continuity is responsible by the nMAG through joining the ongoing multicast channels on behalf of the MN. To do so, the nMAG first needs to get the active multicast subscription information of the MN. It is done by relying on the normal MLD operations or the multicast context transfer mechanism; iii) Joining and getting the first multicast packet: The nMAG then decides joining the on-going multicast channels from its upstream MR/or an additional MLD proxy. Afterwards, the MAG forwards the multicast packets to the MN. From the multicast service point of view, while the information acquisition operation may lead to the service disruption and signaling overhead, the joining process depending on the position and the role of the upstream MR can cause the service disruption, signaling overhead, tunnel convergence problem and tunneling overhead. Regarding the service disruption time, it depends on all the operations. However, from the multicast service perspective, only the subscription acquisition time and joining time can be reduced for accelerating the multicast delivery. As a result, there are two possible solutions for these issues. The first one [116, 108, 115, 16] aims at reducing the time for information acquisition operation. The detailed discussions on this solution will be provided in Chapter 4. The second one mainly focuses on reducing the time needed for the joining process. Moreover, in both solutions, the operations during handover can be executed in parallel.

Solutions for Multicast Source Mobility

Limited work on the multicast source mobility in PMIPv6 has been developed compared to the multicast listener mobility. From the IETF point of view, the base solution for the multicast source mobility in PMIPv6 is still under discussion. In [118], the authors suggest using the base solution for listener for source mobility. In this case, MLD proxy and MR function need to be deployed at MAG and LMA, respectively. As a proxy, the packets arriving from a downstream interface will be forwarded to all the downstream interfaces which have the subscription information of this group except the incoming one and to the upstream interface. As a result, the multicast traffic from a local source will reach all the listeners attaching to the same MAG and sharing the same LMA (serving by the same MLD proxy instance). Serving as an upstream MR, the multicast traffic will be transmitted to the LMA, which then will be forwarded along the multicast delivery trees according to the forwarding state to reach all the listeners.
After a handover, the source can continue to send the multicast packets as soon as the MLD proxy at the nMAG maps the source to the corresponding proxy instance and the standard

PMIPv6 operations are completed. The detailed operation is illustrated in Fig. 2.16. It is worthy to note that when the source and listeners are attached to the same MAG but associated to different LMAs, the traffic will be routed in a definitely non-optimal route from the source's MAG to the source's LMA, passing the listener's LMA and finally returning to the same MAG. This is called a detour routing issue.

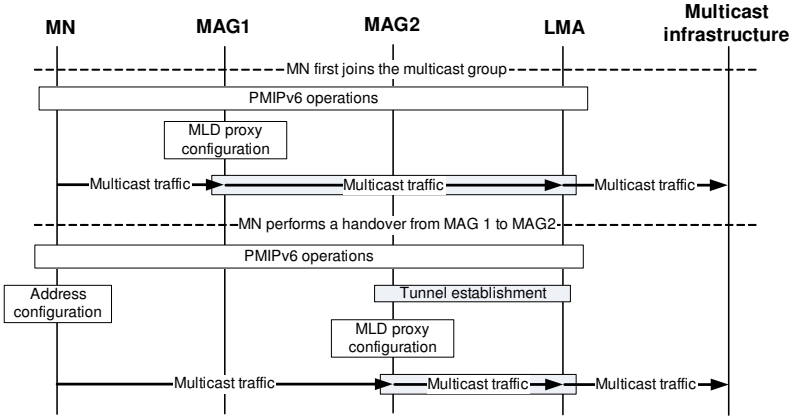


Figure 2.16 – Signaling for the multicast source mobility support in PMIPv6.

At the same document [118], the authors propose another possibility in which the multicast traffic is routed directly from MAGs to the multicast infrastructure bypassing the LMA (direct-routing). The direct routing can be supported by: i) MLD proxy deployment at MAGs with the upstream interface configured towards a common MR in the multicast infrastructure; or ii) the multicast routing protocol deployment at MAGs.
In the former case, a single proxy instance at MAGs with the upstream interface configured to the multicast domain will serve as a first hop multicast gateway (for all the attached listeners and sources), thus avoiding the traffic duplication and detour routing. In addition, the upstream interface of the proxies should be configured towards the same MR in order to avoid the multicast tree reconstruction during handovers (which may cause significant service disruption and packet loss). The reason is when the source moves from the pMAG to a new one and if the default MRs of two MAGs are different, the nMAG's MR does not have information of this channel. Consequently, it considers the source as a new multicast source, leading to the execution of the source registering process [118]. The nMAG's MR unicast-encapsulates the multicast packets and directly sends them to the RP which then sends Join messages towards the source to create the multicast delivery tree. Since the LMA acts as a global anchor point for the address of the source, the Join messages will reach the LMA which then simply discards the messages. As a result, the PIM cannot switch from phase one to phase two (or three) as it may cause several issues such as packet overhead, encapsulation/decapsulation cost, source register tunnel management and sub-optimal routing (for the listeners that are close to the source) [41]. The similar issue occurs when the multicast routing protocol is deployed at MAGs.

2.3.2.3 Alternative Proposals

Aside from IETF proposals, several research documents have been done to improve the standard multicast mobility support in PMIPv6. The purpose of these proposals is to address the performance and optimization issues such as the service disruption, the sub-optimal routing and the tunnel convergence problem.

From listener point of view, in [121], the authors propose two multicast listener mobility support mechanisms i.e., the LMA-based and the MAG-based, corresponding to the tunnel-based and direct-routing approach. The simulation is then conducted to evaluate the performance in terms of handover delay and signaling cost. In [122, 123], the authors propose the solutions based on the fast-handover approach to minimize the service disruption time and to prevent the packet loss during handovers. Again, the under link radio access technology needs to support layer-2 triggers and the solution strongly depends on the layer 2 access technologies.
In [124], the authors, following the idea of separating the management of the multicast traffic and unicast one in different LMAs (dedicated LMA for multicast traffic) in [117], provide a simulation framework to evaluate the dedicated LMA for multicast proposal. The simulation results show that this solution helps to reduce the multicast traffic load by reducing the traffic duplication.
In [125], the authors propose a solution similar to the direct routing approach, in which the MLD proxy is implemented at MAGs with its upstream interfaces configured to an MR in the multicast infrastructure. Then, the multicast context transfer is used to accelerate the multicast subscription acquisition at the predicted MAG. However, it may cause the issue in case of prediction failure.
Limited work [126, 114, 127] has been done for source mobility in PMIPv6. In [114], the authors propose the solution for the multicast source mobility similar to that in [118], however, a performance evaluation is provided. In [127], the authors extend PMIPv6 protocol to support multicast sender by introducing the Multicast Forwarding Cache (MFC) at MAG. Thus, MLD proxy functionality is not required at MAG. However, simulation is required to evaluate the performance of MFC as well as the interaction between MFC and the typical MAG functionality.

2.3.3 IP Multicast Mobility in Network-based DMM

In DMM, there is a limited work for the multicast support since the DMM is still in an early stage of standardization. So far, no complete solution has been found for multicast in DMM. Typically, all major aspects are inherited from the problem in a PMIPv6 domain, while an additional complexity is added. It is noted that this section only presents the issues and solutions when considering a multicast mobility in a network-based DMM environment. Since from now on we only consider a network-based DMM environment, for simplicity, a MAR supporting network-based DMM can be called MAR, instead of NMAR in the previous section. We recall some abbreviations introduced in the previous chapters to denote the role of MAR from a mobile node point of view:

- Current MAR (cMAR, or Serving MAR (sMAR)) is the MAR to which the MN is currently attached.
- Anchor MAR (aMAR) of an MN's address/session is the MAR where the prefix in use is allocated (and the session is initiated using this address as the source address).

2.3.3.1 Multicast Listener Support in DMM

Since DMM is still in its infancy, no complete solution has been found for the multicast support in DMM. As similar in PMIPv6, the multicast listener mobility support can be enabled in DMM by deploying MLD proxy at MARs [128, 22, 20]. In this case, when a multicast flow is initiated, the multicast traffic is received directly from the native multicast infrastructure via the cMAR. In case of handover, the traffic is routed from the anchor to the

current MAR via the tunnel between them (like the unicast traffic). In more details, when an MN subscribes to a multicast flow at MAR1, the MLD proxy instance at MAR1 sends an aggregated MLD Report message to its upstream MR (see Fig. A.3). The multicast packets are then transmitted directly from the multicast infrastructure to the MN via MAR1. The MN then performs a handover to MAR2. Following the network-based DMM approach, the tunnel is established between MAR1 and MAR2 for the active flows which are initiated at MAR1. After executing the standard DMM operations, an MLD proxy instance at MAR2 adds the MN to its downstream interface, and configures its upstream interface towards MAR1 (see Section 2.2 for more discussions about how the MAR2 knows the MAR1 address). MAR2, after obtaining the MN's subscription information by means of the normal MLD operation, sends an aggregated MLD report to the MAR1 to join the ongoing channels. Finally, the multicast traffic is transmitted from MAR1 to MAR2 via a tunnel between them and reaches the MN.

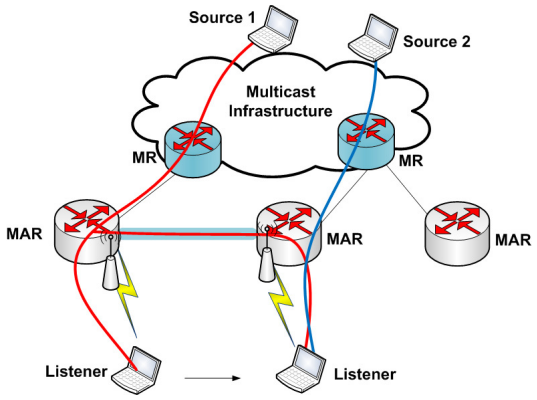


Figure 2.17 – Multicast listener mobility in DMM (MLD deployment at MARs).

However, this mode does not address any multicast-related issues. Among them, we just highlight the following issues:

- *Service disruption (and packet loss)*: When a multicast listener moves from the pMAR to the cMAR, several multicast-related procedures need to be executed to allow the listener to continue receiving the ongoing multicast channels. Consequently, it causes a noticeable service disruption (due to the multicast service activation, MLD response delay, and MLD Query/Report transmission). By using the multicast context transfer and the explicit tracking function, the service disruption time could be greatly reduced [16]. However, in some cases, it is far from the values required by specific services (e.g., interruption-sensitive services). For instance, in [22, 129], the authors showed that the multicast service disruption time strongly depends on the tunnel delay between the aMAR and cMAR. Hence, by reducing the tunnel delay, the service disruption time can be reduced [19].

- *Non-optimal routing and end-to-end delay*: Since the multicast traffic always traverses the aMAR, it often results in a longer route (e.g., when the source and the listener are close to each other but far from the listener's aMAR). In particular, when considering a significant large domain, it can cause a high end-to-end delay. Therefore, avoiding utilization of the mobility tunnel or shortening the tunnel could help [19].

- *Tunnel convergence problem*: In case of mobility, the utilization of the mobility tunnel for the multicast flow may result in the tunnel convergence problem. This issue

occurs when multiple instances of the same multicast traffic converge to an MAR, leading to the redundant traffic. It is because the multiple MLD proxy instances are installed at the MAR with their upstream interfaces configured to different aMARs. Since the purpose of DMM is moving the mobility anchors from the core to the edge of the networks, the number of mobility anchors in a DMM domain will be much more than that in a PMIPv6 domain. As a consequence, the tunnel convergence problem is supposed to be much more severe than that in PMIPv6, especially in highly mobile regimes. As stated in the DMM requirements [8], the multicast solutions in DMM should take this issue into consideration. In [130], the authors introduced a framework managing all multicast channels and controlling which channel should be received from the multicast infrastructure (for local content) or the previous MAR (for remote content). This solution helps to minimize the multicast traffic duplication. However, as only one upstream interface is configured at a time, it may cause the tunnel convergence problem again when an aggregated MLD Report is sent to the upstream interface. Thus, the tunnel convergence problem cannot be completely avoided. On the other hand, the problem can be solved by using an extension to MLD proxy to support the multiple upstream interfaces [120]. In this case, only one proxy instance will be installed at MAR with different upstream interfaces towards different aMARs (and its upstream MR). Hence, the MAR will receive only one instance of the multicast packet. Also, in a DMM environment, it is unfeasible to pre-establish all the tunnels between MARs since the number of MARs is supposed to be large. When considering the MLD proxy supporting multiple upstream interfaces in DMM, it may cause the complex tunnel management (e.g., maintenance of the tunnel and keep alive signaling). Another solution which helps to reduce the number of duplication traffic is proposed in [22].

Considering the MR function deployment at MARs, the MAR will decide to get the multicast traffic from an MR for an attached listener based on the Reverse Path Forwarding (RPF) check. As a result, the tunnel convergence, non-optimal route will be avoided. However, the movement of the listener causes the service disruption problem. Additionally, the operators may not want to support the multicast routing function on MAR due to its implementation and operational costs compared to MLD proxy.

2.3.3.2 Multicast Source Support in DMM

Similar to the multicast source mobility in PMIPv6, a limited work has been done for the source mobility in PMIPv6. Also, multicast source mobility in DMM inherits the issues from that in PMIPv6. In [14, 128], the authors propose to enable the multicast source mobility in a DMM environment by deploying MLD proxy at MAR. In case of handover, the multicast traffic will be routed from the current MAR to the anchor one via the mobility tunnel between them. Although this solution is simple and easy to deploy, it comes up again the sub-optimal routing when the source and listeners, after handover, are attached to the same MAR (but from different anchor MARs). When the MAR acts as an MR, it considers the source as a new source. Thus, it encapsulates the multicast packets and sends them to the RP (in case of ASM). The RP then sends a PIM Join message towards the source's aMAR to establish the SPT. Thus, the traffic first passes the aMAR and then the RP. In addition, if the mobility occurs after the DR's listener switches to the SPT towards source, the mobility will reset the SPT routing state, leading to a significant service disruption and packet loss. In case of SSM, the multicast delivery tree will be reconstructed based on PIM process. Again, it may cause a noticeable service disruption and a high number of lost packets.

2.4 Conclusion

As more and more applications and services in the Internet are based on the multicast technique, the multicast will play a crucial role in the future networks. So as to provide the multicast service, two groups of protocol need to be deployed: the multicast group membership protocols and the multicast routing protocols. The multicast group membership protocols are used to communicate between the hosts and their routers. Relying on MLDv2, we analyzed the role and operations of these protocols. Using MLDv2 protocol, a host informs its router about its interest of receiving/leaving a multicast group, while an MR manages its membership state information on the attached link. Various multicast routing protocols then have been presented, in which the PIM-SM protocol is insisted. Finally, to avoid deploying a full-stack multicast router in a given network, an MLD proxy is introduced as a lightweight solution.
Regarding IP mobility management protocols, there are a various IP mobility protocols ranging from the host-based to the network-based, from the centralized to the distributed approach. Typically, PMIPv6 as a network-based mobility management offers advantages compared to the host-based one in terms of complexity of the MN, signaling overhead and handover latency. However, PMIPv6, as a centralized mobility approach, relies on a centralized mobility anchor to support mobility. Thus, it causes several limitations when the number of mobile devices and their traffic demand increase. To tackle these limitations, DMM has been introduced. The research publications showed that DMM is a promising choice for the future networks.
Based on the analysis regarding IP multicast and IP mobility management protocol, we then highlighted the issues when considering IP multicast in different mobility management protocols. First, we have made a brief introduction on the multicast-related issues as well as the proposals for multicast mobility in MIPv6. We then made an in-depth analysis in PMIPv6 and DMM. In the context of our thesis, we focus on such issues as the multicast service disruption, packet loss, sub-optimal routing, tunnel convergence problem, and leave latency (waste of resources).

3
Performance Evaluation for IP Mobile Multicast

3.1 Introduction

In this chapter, we will define the performance metrics that are crucial to assess the effectiveness of the mobile multicast solutions. The performance metrics are typically based on such metrics for evaluation of a mobility management protocol as signaling cost, handover latency, and packet loss. Furthermore, the multicast-related metrics e.g., packet duplication, leave latency, end-to-end delay and tunneling overhead should be considered.
It is generally acknowledged that a proposed solution cannot be widely accepted without results from a valid experimentation, which can be obtained through various methods, each with its own advantages and limitations. Within the networking field of research, the results' reliability is one of the most critical issues. Thus, the results' credibility is directly related to the methods used, therefore improving them becomes of great importance. In this context, the most widely used method - simulation - sometimes lacks credibility. The lesser used but most credible method - real testbed - is too expensive and difficult to scale and manage. In this chapter, we propose a *hybrid* method which is a combination of virtualization and simulation. Through the study of a simple use-case showing mobility with PMIPv6, we demonstrate that our proposed method provides realistic results at a low cost. In other words, the near-to-real results can be achieved even with limited resources. This method can also be deployed in a distributed manner for increased scalability. Additionally, the others tesbted e.g., MIP, HMIP, and DMM can be deployed using the same method.
Throughout this thesis, in order to validate the results, firstly, we will use an analytical analysis. The proposed experiment method then, in some cases, will be used to improve the degree of confidence of the results. It can be considered as a framework that aims to close the gap observed between the research experimentation and the real deployment.

3.2 Performance Evaluation Metrics

At first, we identify the key requirements that need to be satisfied by the proposed solutions. Respecting these requirements, we then define the performance metrics that are crucial to assess the effectiveness of the solutions.

3.2.1 Specific System Requirements

In this thesis, our objective is to deal with the multicast-related issues raised when a multicast node is on the move. In other words, the aim of this research is to find solutions that

ensure:

- Keeping the MN unaware of mobility from the multicast service point of view;
- Minimizing the service disruption to even satisfy the strict requirements for the interruption- and delay-sensitive services;
- Keeping the signaling/tunneling overhead as low as possible;
- Maximizing the available network resource (reducing the waste of resource and packet duplication), keeping the reliability and improving the scalability of the system;
- Minimizing the modifications of the mobility management and the multicast routing protocols to support IP mobile multicast.

Based on these objectives, we will design novel solutions addressing the IP mobile multicast issues in both PMIPv6 and DMM environment. In the following, a list of specific requirements that would lead to the design of the target solution is provided:

- Only the network-based mobility management shall be studied to keep the MN unaware of mobility and to avoid modifications required at the MN;
- Network access technology independence and support for both single-homed (e.g., Wi-Fi or LTE) and multi-homed terminals (e.g., LTE and Wi-Fi) shall be provided. In other words, such a generic solution which does not depend on specific access technology shall be provided;
- Buffering technique shall not be considered. However, it can be used later to improve the proposed solution;
- The routing paths between sources and listeners shall be optimized;
- Mobility services shall be enabled only for IP flows which really need service continuity.

3.2.2 Performance Evaluation Metrics for IP Mobile Multicast

To evaluate the performance of a mobility management protocol, a set of metrics in general is considered including signaling cost (location update cost), handoff delay, end-to-end delay and packet tunneling cost [72, 73, 99, 131].
In wireless mobile networks, the mobility anchor is responsible for tracking the location of the MN to provide the mobility support. Thus, location management is crucial for the effective operation of wireless networks [132]. Location update is done by exchanging the signaling messages between the MN and the network entities (or between the network entities). In this context, the signaling cost is defined as the cost to update the location of the MN. It can be considered as a function of different metrics as the hop distance between the entities, the unit transmission cost over wired/wireless link, and the handover rates (intra- and inter-domain handover), etc. Signaling cost is an important factor since it influences the scalability of the system as well as the cost for data delivery. This metric becomes even more critical with the presence of wireless links whose have a limited capacity.
Regarding the handoff latency, it is defined as a period when a node cannot receive/send the packets while performing a handover. It is the time that elapses between the last packet received via the old router and the arrival of the first packet via the new router after a handover. During this period, the packets will be lost. Thus, it may result in noticeable service disruption, especially in case of delay sensitive applications like video and Voice over

IP (VoIP). The number of lost packets typically is proportional to the handover latency. In IPv6-based networks, QoS may be defined by packet loss, handoff latency and signaling overhead [72]. As a result, long handover latency and a large number of lost packets may degrade the quality of service. Thus, reducing the handover latency and the packet loss enhances the performance of user applications.
On the other hand, the end-to-end delay between two nodes is the summation of delays experienced along the path between these nodes. In general, the end-to-end delay consists of not only the transmission delay over the links but also the queuing and processing delay at the intermediate nodes [133]. Many popular multimedia applications, e.g., real time gaming, live video streaming, and conversational VoIP/Video, have strict delay requirement.
Regarding IP mobile multicast, the similar metrics as mentioned as above as well as the multicast-related metrics should be taken into consideration.

3.2.2.1 Signaling and Packet Delivery Cost

The signaling cost is the signaling overhead for supporting the handover of a multicast node, including the cost for the location update and the multicast-related procedures. It is defined as the total delivery cost of all signaling messages. According to [131], the signaling message delivery cost is calculated as the product of the message size, the hop-count distances and the unit transmission cost over wired/wireless link. Let α and β denote the unit transmission cost for the wired and the wireless link, respectively. Thus, the signaling message delivery cost over the wired link from node X to node Y is calculated as

$$SMC_{wd} = \alpha lh, \tag{3.1}$$

where l is the size of the message, h is the hop distance between X and Y. In case of wireless link, the message delivery cost can be expressed as

$$SMC_{wl} = \beta lh. \tag{3.2}$$

Note that typically the hop-count distance between two nodes via wireless link is 1. In some cases, for the sake of simplicity, the size of signaling messages is considered as identical. In this case, this value can be included in the parameters α and β. The signaling cost, as the accumulative signaling overhead, can be calculated as

$$SC = \sum_{all} SMC. \tag{3.3}$$

On the other hand, the packet delivery cost represents the accumulative cost to deliver multicast packets from the source to the listener per unit of time. It is proportional to the distance between the source and the listener, the size of data packets and the number of packets transmitted.

3.2.2.2 Multicast Service Disruption Time and Packet Lost

The multicast service disruption time (SD) is defined as a period when a multicast listener/source cannot receive/send the multicast packets. It is calculated as the total time needed to complete the mobility handover and the multicast-related procedures. Thus, the multicast service disruption time typically consists of: i) Layer 2 handover duration (t_{L2}) which is the reattachment time from the previous point of attachment to the new one. It depends on specific wireless access technology, for example, in case of 802.11 WLAN its includes the time for channel scanning, authentication, and association/re-association process; ii) Layer 3 duration (t_{L3}) caused by IP-related procedures; and iii) The delay due to

the multicast-related procedures, called t_M. t_M is defined as the total time taken to complete all the multicast-related procedures including the multicast knowledge gain, multicast subscription and transmission time for the first multicast packet from the multicast router to the listener after handover. As a result, the multicast service disruption time is defined as

$$SD = t_{L2} + t_{L3} + t_M. \tag{3.4}$$

To calculate the layer 3 and the multicast handover delay, we adopt the packet transmission delay model in [134], in which the packet transmission consists of the transmission time and the propagation time. According to [134], the transmission delay of a wired link can be calculated as

$$d_{wd}(l,h) = h(\frac{l}{BW_{wd}} + D_{wd}), \tag{3.5}$$

where h is the hop-count distances between two nodes, l is the length of the packet, BW_{wd} is the bandwidth of the wired link and D_{wd} is the wired link latency.
Unlike the wired transmission which can be considered as reliable, the wireless link is unreliable. Thus, the probability of link failure should be taken into account. The wireless transmission delay therefore is given by [134]

$$d_{wl}(l) = \frac{1}{1-q}(\frac{l}{BW_{wl}} + D_{wl}), \tag{3.6}$$

where q is the probability of the wireless link failure, BW_{wl} is the bandwidth of wireless link and D_{wl} is the wireless link latency.
For a sake of simplicity, the transmission delay in some cases can be considered as proportional to the distance, for example, with the proportion is τ for wired link and κ for wireless link. Thus, the transmission delay is simply given by

$$d_{wd}(h) = \tau h, \tag{3.7}$$

$$d_{wl} = \kappa. \tag{3.8}$$

On the other hand, the packet loss (φ_p) represents the number of lost packets during handover. Typically, the number of lost packets is proportional to the service disruption time and the packet arrival rate. As a result, it is given by

$$\varphi_p = \lambda_p SD, \tag{3.9}$$

where λ_p is the packet arrival rate.

3.2.2.3 End-to-End Delay

As stated earlier, the end-to-end delay consists of not only the transmission delay over the links but also the queuing delay and the processing delay at the intermediate nodes. However, for a sake of simplicity, the queuing delay as well as the processing delay are supposed to be small enough to be ignored in the performance analysis. As the result, the end-to-end delay represents the packet transmission delay from the source to the listener. The packet transmission consists of the transmission time and the propagation time. It is proportional to the distance between two nodes, the size of the packets, the bandwidth of the link and the link latency [134]. Typically, the packet transmission delay over a wired and a wireless link is different.

3.2.2.4 Other Metrics

In addition to the above-mentioned metrics, those as packet duplication, tunneling overhead, waste of resource, scalability, and easy-to-deploy should be taken into consideration. In the context of our thesis, the scalability issue will be considered in terms of load balancing among LMAs (together with the signaling cost). The packet duplication metric reflects the tunnel convergence problem.

3.3 Experimental Evaluation of Wireless Mobile Network

In networking research, there are various experiment methods such as: using a real testbed, simulation, emulation, virtualization and mathematical or theoretical modeling. Each method has its own advantages and limitations [135]. Using a real testbed is considered as the best experimental method. It implies, however, a higher cost of deployment and lack of scalability. Although simulation is quite popular thanks to its flexibility and easy-to-deploy features, the results obtained in some cases are not reliable. Emulation can be considered as a trade-off between simulation and a real testbed bringing more accurate results (compared to simulation) and lower cost (compared to the real testbed). Yet, emulation has limitations on deployment and scalability, which can be mitigated by using the technique of machine virtualization. Finally, mathematical modeling is sometimes used, but only in a simplified way, abstracting most of the complexity and reflecting it on obtained results. Furthermore, to help justify our approach on experimental method, we must mention that our case study concerns mobile environments and therefore we must keep in mind the most important requirements that an experimental method must focus on are accuracy, reliability, mobility, and scalability [136].
In this section, we introduce a near-to-real experiment environment which consists of a virtualized and simulated environment. The first part can be considered as the network infrastructure in which multiple virtual machines are connected together, while the second part is a wireless access network mainly composed by a wireless simulator. By combining these components we produced a method that can achieve a higher level of realism while keeping the advantages of the simulation method and still be able to run real software and real world protocols. Since this experiment environment is an open-source and easy to deploy, it can be reused by other researchers to set up their own experiment environment. Additionally, it allows the design and evaluation of small to medium scaled networks and deployed protocols whose results can be easily translated to the real world. These characteristics will be illustrated through the analysis of our case study using PMIPv6 [76]. Particularly, this method is suitable for following cases: i) fixed infrastructure; ii) mobility and mobile networks; iii) network and upper layer experimenting (e.g. mobility management, multicast, applications, etc.); iv) up to medium sized infrastructure networks; and v) large sized networks of mobile nodes.

3.3.1 Experiment Methods in Networking Research

This subsection introduces the most relevant experimental methods in the field of networking research, emphasizing their advantages and disadvantages. We start by the most popular method, simulation, and then move to real testbeds, emulation and mathematical modeling. We continue by addressing the required criteria to our work, which is supported by acknowledged good practices on credibility and confidence of experimental methods.

Simulation is the most common experimental method in networking research [137] [138], mainly due to the fact that simulation environments can provide large-scale flexible scenarios (in terms of topology, number of nodes) at a low cost. In addition, the capability of reliable reproduction and repetition of experiments is embedded. However, the main drawback of this method is the lack of credibility [139, 140]. In other words, the results of the simulation in some cases cannot be relied on, particularly for mobile network experiments, due to the complex environment of mobile wireless networks and the simplicity of the simulation framework. The varying degree of simplification has allowed the creation of several simulators for mobile wireless networks e.g., OMNet+++, Matlab, Glomosim (QualNet), NS-2 and NS-3. Each simulation tool has its own advantages and limitations [138]. The choice of a simulation tool depends on several factors such as cost, ease of use, level of complexity, availability of required model, community support, and particularly accuracy. Regarding accuracy, the results may be very different when using different simulation tools [141], making it difficult to choose the appropriate simulation tool.
On the other extreme of the experimental methods is the construction of a real testbed which uses a set of real hardware and software. In general, it is considered the best environment for experiment study, since this kind of method provides the most accurate and most realistic results [142]. Furthermore, it helps to find unexpected errors and limitations that could not otherwise be observed in the simulation. However, this method requires a high cost especially when a complex network topology and a large-scale experiment are considered. Also, additional effort may be required when considering the mobility of the nodes (e.g., unpredictable and hard to repeat, scaling of the geographical movement, mobility pattern and experiment management). The repeatability and reproducibility also present some serious challenges.
In the middle of the extremes, emulation has been introduced as a compromise between these two above-mentioned methods. The main advantage of this approach is that it helps to eliminate the practical problem with the real testbeds by completely controlling such external factors that may influence the experiment thus increasing repeatability and reproducibility. It can also provide the near-to-real results at a lower cost in comparison with the real testbed. However, the emulation experiment may still lack scalability and its not always easy to set up an emulation environment. Another possible method is the virtualization in which a whole network is created by the virtual machines. The advantage of this method is that the development of the software can be done on the real machine, tested on the virtual network of virtual machines, and later installed without any (or with minor) modifications on the real testbed. However, virtualizing wireless network interfaces as well as simulating mobility of the nodes are complex tasks [143, 144]. The oldest method is theoretical modeling with mathematical analysis, which uses a mathematical model to evaluate network performance. However, it is very difficult to model a realistic environment particularly in the case of mobile wireless networks. As a result, some simplifications are required.
Regarding one of the most important issues – credibility, in [139], the authors raised the credibility issue over a survey of over 2200 publications in the field of network simulation studies. They provided some guidelines to help to ensure a basic level of credibility of simulation experiments such as: i) the simulation experiments should be repeatable; ii) the method of analysis of simulation output data should be specified; and iii) the final statistical errors associated with the results should be provided. In conclusion, ideally, an experimental method would focus on some requirements such as controllability, repeatability, cost effectiveness, data collection, resource sharing, and particularly elements such as scalability, accuracy and mobility [136], are at the core of the trade-off or compromise that leads the researcher to choose his experimental method.

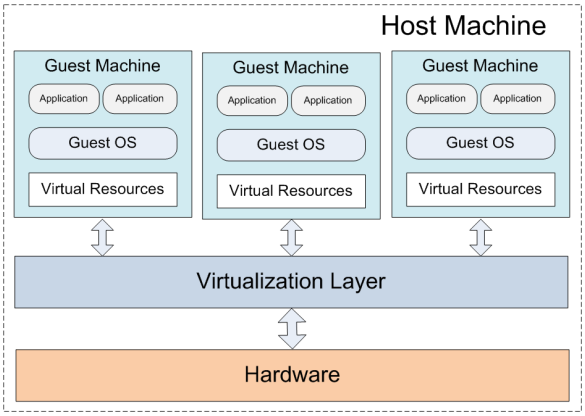


Figure 3.1 – An example of the virtualization technique.

3.3.2 Virtualization Technique and Virtual Networking

In this section, we introduce our approach and the different techniques considered for virtualization as well as the tools for virtual networking. We then focus on the tools that help to deploy the virtual networking such as Virtual Network User Mode Linux (VNUML)[1], and Netkit[2] regarding their advantages and their limitations.

3.3.2.1 Virtualization Techniques and Virtualization Tools

Virtualization is a mechanism which allows running multiple independent and simultaneous instance sets, of the machine's core software components (such as kernel, memory management, etc.), creating in practical terms a framework where these instance sets constitute the virtual logical machines (guest machines), which, when executed will share the physical resources of the single physical machine (host machine) [145, 146]. Since several virtual machines can be run inside a limited resource, then a virtual environment can help to extend the capabilities of a system at a low cost. Fig. 3.1 shows an example of virtualization technique. In this figure, the different guest machines run on the real machine. The guest machines use the virtual resources which are mapped to the sharing physical resources of the host machine (e.g., CPU, storage, and memory). The allocation and sharing of these resources is managed by the virtualization layer.
There are several virtualization techniques depending on the way the virtualization layer is implemented, the first technique is full virtualization (using binary translation) [146] in which the guest operating system (OS) acts as if it owned the hardware. That means the guest OS does not know that it is being virtualized and as a result, the guest OS does not require any modification. However, an additional mechanism, namely binary translation, is required to trap the instructions that are not compatible with the virtualization (non-virtualized) and translate them into the new instructions that will have the same effect on the virtual hardware. Some examples of the full virtualization technique are VMWare[3], and Virtual Box[4].
The second technique is paravirtualization (or OS assisted virtualization) [146]. Unlike the full virtualization technique, the guest OS is aware of the fact that it is running in a virtualized environment. Thus, the guest OS is modified from the standard OS to communicate

[1]VNUML Homepage: http://www.uni-koblenz.de/ vnuml/index.en.php
[2]Netkit Homepage: http://wiki.netkit.org/
[3]VMWare Homepage: http://www.vmware.com/
[4]Virtual Box Homepage: https://www.virtualbox.org/

directly with the virtualization layer in case of non-virtualized instructions. Thanks to this mechanism, the paravirtualization achieves better performance than the full virtualization. However, one of the main drawbacks of the paravirtualization is that it fails to support any OS which is unprepared for virtualization. The paravirtualization is, for instance, supported by Xen [147] and User-mode Linux (UML) [148], etc.
The last main virtualization technique is called hardware-assisted virtualization (or native virtualization) [149]. This technique requires the hardware to support the virtualization technology in order to simplify the virtualization mechanism. Since this technique is quite new, at this stage, it can only bring advantages in some limited cases [146], though its results look very promising. Kernel Virtual Machine (KVM)[5] is an example of the hardware-assisted virtualization.
When considering different virtualization tools in the context of network environment, a lightweight tool should be chosen in order to deploy as many virtual nodes as possible in a single physical machine. In this context, this chapter adopts UML since it is a relatively lightweight technique compared to the others [150]. UML is also one of the most popular virtualization techniques that can be deployed in a linux-based OS.
UML uses the paravirtualization technique (at kernel level) that allows running a virtual instance of Linux inside the host Linux OS as a normal system process. In these conditions, a virtual machine running with a UML kernel (modified kernel) and a root filesystem, can be assigned to the virtual resources and have a hardware configuration entirely separated from that of the host.

3.3.2.2 Virtual Networking in Linux

As mentioned above, there are many virtualization techniques. However, some may require a number of manual operations to set up a virtual network and interconnect virtual machines. That is why there are several tools which aim at building and configuring a virtual network environment easily and automatically. They are developed to simplify this task (such as VNUML, Netkit, and Marionnet[6], which rely on UML) and allow to design and test networks with different topologies and different configurations. The created virtual networks are able to communicate with both the host machine and, if possible, with any existing network connections residing on the host. Nevertheless, there are several limitations in the context described in this chapter:

- *Centralized deployment*: That means the entire virtual network is deployed inside just one host machine which limits the deployment size since resources are shared.

- *No wireless access technology support*: They fail to support wireless access connections such as WLAN, and LTE, since their deployment only considers static point-to-point connections.

- *Difficult to support different kernels and filesytems overall network*: Typically, only one kernel and filesystem are used for all the virtual machines. In some case, due to the conflict between the software requirements, it is impossible to use only one kernel version with the same components installed for all the network entities. Moreover, one configuration for all machines is not always a good option, e.g., the servers require much more resources than the mobile nodes. Also, while servers may require some additional software, mobile nodes do not.

[5]Kernel Based Virtual Machine (KVM) Homepage, http://www.linux-kvm.org/
[6]Marionnet homepage: http://www.marionnet.org/EN/

3.3.3 Wireless Simulation and Emulation

In reality, there are various wireless simulation tools (e.g., OMNet+++, Matlab, Glomosim, NS-2 and NS-3), with each tool having its own advantages and limitations. Thus, choosing an appropriate tool is very difficult since it can lead to unexpected results which cannot be exploitable in a real world deployment.
In this subsection, we also look at simulation tools which can provide the wireless emulation mode such as NS-2, NS-3. With such a tool included in our work, real and virtual machines can be connected via an emulated wireless connection. Since NS-3 is relatively new and intended to replace the aging NS-2 simulator, it has a good development momentum which incorporates a remarkable number of interesting features [151]. Those are the reasons why we selected NS-3 as the main tool to provide the emulation of wireless environment for the proposed testbed.
NS-3 is a discrete-event network simulator targeted for research and education. It relies on C++ and can be installed on common operating systems e.g., Linux, Windows, Mac OS. Furthermore, NS-3 provides an effective tracing method, called callback tracking system [151]. By using this technique, a reaction can be executed when a trace source generates a new event, for example, for cross-layer interaction, statistic collection, etc. Beside the traditional text file as the output of events, NS-3 provides another type of tracing called PCAP (network traffic capture) which then can be used by a network analyzer tools e.g., Wireshark [152], Tcpdump [153] to analyze the results.
In addition to the simulation capability of NS-3, the emulation is natively supported by using a type of virtual network device, named Tap Bridges. Thus, the real services/nodes can communicate with the NS-3 environment. This capacity allows deploying a *hybrid technique* as we used to develop the proposed testbed.

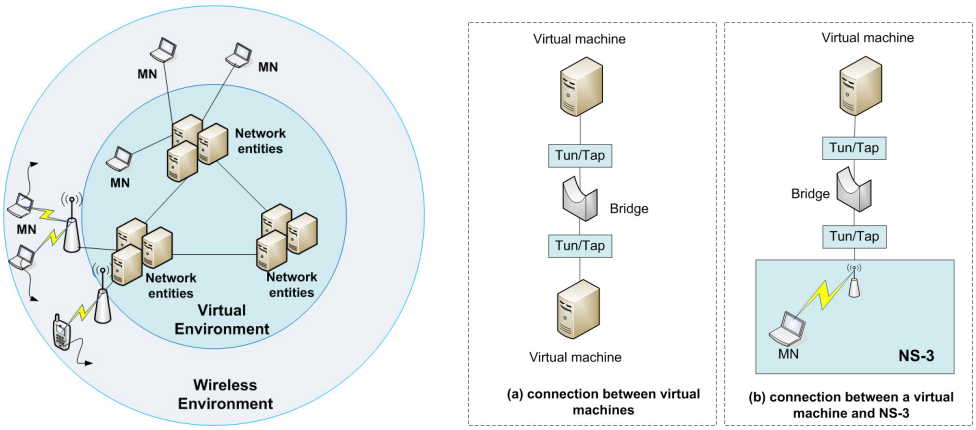
3.3.4 Requirements and Proposed Strategies

3.3.4.1 Requirements for a Wireless Testbed

Regarding the experiments in the context of mobile environments (focusing on the network and upper layers), there are some requirements briefly described as follow.
The first and the most important requirement is that the results of the experiment have to go in line with that from a real experiment. In other words, the experiment environment has to be able to provide realistic and reliable experiments. Then, the experiment environment should be able to emulate the mobility of several nodes by using a mobility pattern. Also, the flexibility in terms of network topology and mobility scenarios should be provided. The experiment environment should be reproductive, repeatable, and scalable in terms of number of network nodes, and it is important to use the virtualization tool that consumes fewer resources. Last but not least, the tools to collect and analyze results should be available and easy to use. Based on these requirements, a testbed environment is proposed as described in the following subsection.

3.3.4.2 Description of the Proposed Testbeds

Due to the limitations of the above-mentioned methods and the requirements for the wireless experiment, we provide an ultimate method using a near-to-real testbed - a combination of a virtualized and a simulation environment, as depicted in Fig. A.6. This method allows keeping the results close to the real experiment without significant efforts. It also provides a flexible simulation in terms of network topology, and mobility scenarios. This method also



(a) (b)

Figure 3.2 – Testbed Architecture: (a) Description of the testbed. (b) Connection between components.

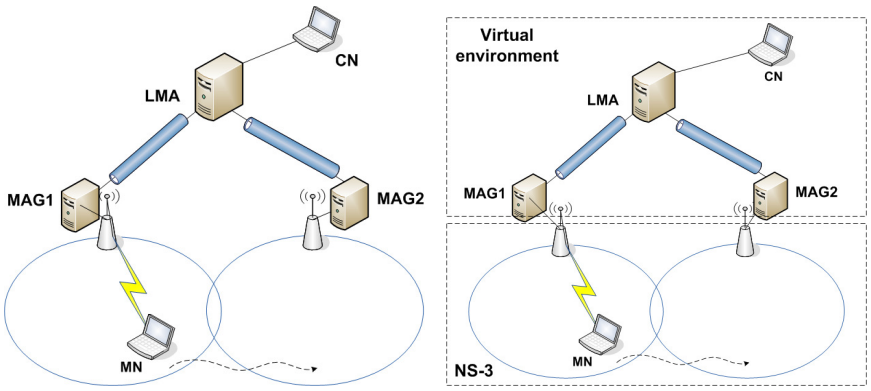
potentially allows the medium-scale networks in term of infrastructure nodes and large-scale in terms of mobile nodes.

A main drawback of using UML for a wireless experiment is that it only offers a virtual Ethernet interface (not a virtual wireless interface), which is why we propose a combination of an UML-based virtualized network and a wireless simulator to provide a wireless experiment environment.

In this approach, the first part of the proposed environment consists of the virtual machines connected together. It represents the network infrastructure. The second part provides the wireless environment by using NS-3 (access points (APs) and mobile nodes). A network analyzing tool (e.g., Wireshark) as well as PCAP trace file can be used to capture the network traffic between the virtual machines. We can then analyze the track files to obtain the results.

Regarding the first part, as seen in Fig. 3.2b, testbed environment is created by using the Linux bridge technique that allows connecting the virtual machines with the wireless interfaces present in the simulation environment. The virtual machines can be distributed among the different physical machines. However, a bit more effort is needed to create the network and experiment scenarios, in this example, we use a simple script. By using a virtual device (called TUN/TAP [154]), the VM can communicate with the physical networking infrastructure as well as other VMs. TAP device works at the Ethernet frame level while TUN device acts as a network layer device. Similarly, a machine inside NS-3 can be made similar to a real machine thanks to the TapBridge mechanism[7].

Regarding the second part, NS-3 is used to emulate the wireless environment and the mobility of mobile nodes. With NS-3, heterogeneous access networks can be provided e.g., WLAN, WiMAX and LTE. In addition, the mobile node's mobility pattern (inside NS-3 e.g., random walk, random waypoint, random direction, and Gauss-Markov mobility model) and external mobility pattern can be used to allow simulating flexible, more realistic mobility of the nodes.



(a) (b)

Figure 3.3 – The PMIP domain and the corresponding testbed: (a) A PMIPv6 domain, (b) NS-3 centered testbed.

3.3.5 Tesbed Deployment

In order to validate the performance of the proposed approaches in terms of flexibility and accuracy, we present a case study in which the mobility in a PMIPv6 domain will be experimented. We will then use PMIPv6 operational behavior as benchmark to compare the experiment results from our approaches with those from a real testbed and those from pure simulation. We have carefully deployed the same PMIPv6 parameters and scenario (following the existing real testbed) in our hybrid testbeds and in the NS-3 simulator. In addition, to obtain more realistic and reliable results from the proposed testbed, we follow some guidelines to collect and analyze the results which were proposed in [135].
As stated before, we have chosen to deploy our case study scenario across several platforms to demonstrate that the performance of our approaches is similar to the one provided by a real testbed. Therefore we deployed a PMIPv6 scenario containing a single MN, two MAGs connected to an LMA and a CN, as described in Fig. 3.3a. Since mobility is not the main purpose of this chapter, for the sake of simplicity, a very basic mobility model is used: the MN moves between two MAGs with a fixed speed and a fixed direction. Later however, other mobility patterns will be applied to provide a more flexible mobility of the MN.
The experiment is executed following these steps:

- The MN enters the PMIPv6 domain for the first time (attaches to MAG1);
- After configuring an IPv6 address based on the HNP allocated from the LMA, the MN uses its address to ping the CN;
- The MN then performs a handover to move to another MAG (MAG2). During handover process, the MN continues to ping the CN.

This scenario was then tested across three different types of platform: i) a real testbed as to represent the base benchmark; ii) our NS-3 hybrid testbed; iii) NS-3 simulation. In cases (i), and (ii), we have deployed the OAI PMIPv6 implementation [155], while in case (iv) we opted by the NS-3 embedded implementation to better show the performance difference.

3.3.5.1 Different Platforms

Real PMIP Testbed (R-PMIP) There is a real testbed [155] which was deployed in similar architecture as described in Fig. 3.3a. All the network entities in the testbed are

[7] Tap Bridge Model NS-3: https://www.nsnam.org/doxygen/classns3_1_1_tap_bridge.html/

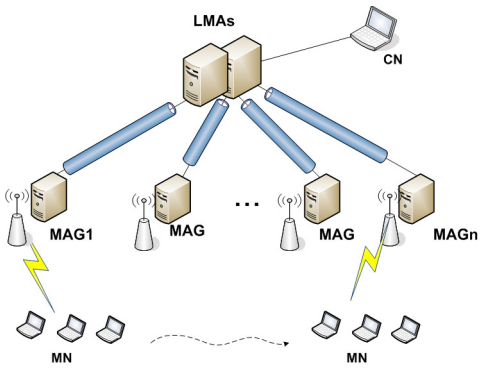


Figure 3.4 – Scalability testbed.

running Ubuntu 10.04 LTS.

Proposed Testbed (PMIP-NS3) The testbed, as indicated in Fig. 3.3b, is composed of one LMA, two MAGs (and two access points (APs)), one CN and one MN. All components are installed on a single physical machine running Ubuntu 10.04 LTS. The LMA, the MAGs and the CN are the virtual machines (UML) while the MN and the APs are NS-3 nodes. It is noted that the CN is a normal UML machine that does not need any specific requirements and functionalities. The run script, which automatically launches and connects the virtual machines together, is created (one time but executed for many times).

A *pure-simulation PMIPv6* (Pure-NS3) Based on the existing PMIPv6 implementation in NS-3 (called Pure-NS3 [156]), a simulation has been made using this implementation with the same network topology as in as well as the same result obtaining method and experiment parameters.

3.3.5.2 Scalability

Besides the comparison testing based on typical and very simple PMIPv6 case scenario, which states to the credibility of our work, we wanted also to give insight on how our proposals behave on a larger environment based on the same case study. Such analysis will demonstrate the capability to extend the range of scenario possibilities that can be researched using our developed methods as well as attest to its scalability, which is a critical, defining and differentiating feature of our work. To that aim we expanded the base case study into several scenarios comprising different topologies and a larger amount of entities, as can be seen on Fig. 3.4. In order to analyze the scalability we enlarged the case study topology in both number of LMAs/MAGs and number of MNs. We first do it separately to know how the resource consumption is affected when the number of each is changed, and finally we increase both to test how far we can push our approaches.

3.3.6 Evaluation

In this section, at first, we compare different approaches regarding high-level metrics and PMIP performance. We then focus on the proposed approach by measuring the resource usage in different experiment scenarios and in different steps. This section also discusses the limitation of the proposed approach regarding number of nodes and introduces some additional suggestions regarding those limitations.

Regarding the statistical evaluation and presented tables of results, it is noted that for the improvement of the credibility we performed the experiment a large amount of times. Based on the collected results, we calculate the average value and the standard deviation to improve the degree of confidence.

3.3.6.1 High Level Metrics

Table 3.1 – Comparison between Different Approaches: High Level Metrics.

Metrics	PMIP-NS3	R-PMIP	Pure-NS3
Detecting the software and hardware requirements	Yes	Yes	No
Detecting the conflict of the components, kernel version	Yes	Yes	No
Detecting unexpected errors during runtime	Yes	Yes	No
Detecting the limitations of PMIPv6 implementation regarding number of supported nodes (MAG, MN)	Yes	Yes	No
Observing the actual behavior of PMIPv6	Yes	Yes	Yes
Hardware cost	Low	High	Low
Portability	Yes	Yes	No

When testing a new application/protocol, in some cases, it is very important to make sure that all the components can work together in a unique environment. Also, observing the interaction between these entities as well as between the components inside each entity is required to guarantee that the application/protocol can work correctly.
Thus, while the R-PMIP and the PMIP-NS3 help to detect the software and hardware requirements, the conflict of the component as well as the unexpected errors during runtime, the Pure-NS3 cannot. To detect the limitations of PMIPv6 implementation regarding number of supported nodes (MAG and MN), our approach (PMIP-NS3) is a good choice. A real tesbed, in theory, can do the same, however, often unfeasible due to expensive cost and difficult to manage. The Pure-NS3 like the others allows observing the actual behavior of PMIPv6, however, only limited observation regarding messages exchanged between entities. Regarding hardware cost, the PMIP-NS3 and the Pure-NS3 require only one physical machine while the real testbed needs 5 physical machines, two wireless access points and one Hub. The number of required machines will be increased when a medium or large-scale experiment is considered. Another important aspect is that the PMIP implementation in our approach can be easily transfer into real word, while it requires re-develop in the Pure-NS3.
As in the PMIP-NS3, the MNs are the NS-3 nodes, it is suitable for the experiment that does not require any specific functions/components at the MNs. Vice versa, the extra effort is needed to deploy the additional components/functionalities required in NS-3. As a result, for the experiment which does not require a lot of MNs and requires some extra functions at MNs, instead of deploying the MNs inside NS-3, we can deploy UML machines as MNs e.g., a streaming source as discussed in [25]. In conclusion, Table 3.1 summarizes the comparison of three approaches regarding different aspects.

3.3.6.2 PMIPv6 Benchmark

Table 3.2 shows the performance of PMIPv6 regarding the average value (<x>, in ms) and the standard deviation (σ_x) from the different approaches. Two metric are considered i.e., home address registration and layer 3 handover latency. While the former aims at showing

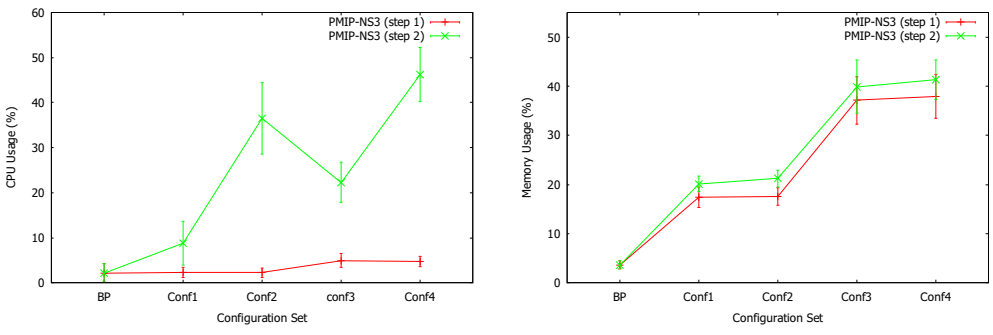
the performance of PMIPv6 using the virtual environment, the latter is used to illustrate the performance PMIP regarding the combination of virtual and wireless environment.
In the Table 3.2, we can see that the results from the Pure-NS3 are very different from those of the PMIP-NS3. The results from the PMIP-NS3 are quite close to those from a real testbed [155]. On the contrary, the results from the Pure-NS3 environment are totally different from that of the real testbed. Thus, it is obvious that the Pure-NS3 cannot be used for the performance study of the PMIPv6 as well as the service deploying in this PMIPv6 network.

Table 3.2 – Comparison between different approaches.

Metrics $< x >, \sigma_x$	**R-PMIP**	**PMIP-NS3**	**Pure-NS3**
Home address registration	(3.0, 1.3)	(5.5, 1.5)	(0.1, 0)
Layer 3 handover latency	(97.3, 12.3)	(110.6, 23.8)	(1.0, 0)

3.3.6.3 Scalability Evaluation

This subsection focuses on the PMIP-NS3 approach by measuring its resource usage regarding CPU and memory consumption depending on different stages and different configurations.
Several network topology configuration sets were defined. The sets are described in the fashion (number of LMAs, number of MAGs, number of MNs) and are constituted as follows: Conf1 (1, 3, 3), Conf2 (1, 3, 90), Conf3 (1, 10, 10), and Conf4 (1, 10, 90). The results were collected in two steps: i) step1: when the testbed is in the preparing mode (after the booting of all virtual machines and their required components; and ii) step 2: the testbed is in the running mode (when MNs attaches and performs handover inside the domain). During the experiment, the processors and the memory related statistics were collected each one second during 100 seconds to improve the credibility. It was done by using some tools e.g., mpstat and top. We also measure the "background processes" (BP) by using the same mechanism.
For instance, we can deploy a PMIPv6 domain with up to one LMA, 10 MAGs, one CN, and one MN (all of them are virtual machines) on a single physical machine even with a very limited capacity: CPU Intel Core 2 Duo T7500 (2.2 GHz), 2 GB of RAM (1066MHz) and a 320 GB HDD running Ubuntu 10.04 LTS. By using NS-3, this testbed can support up to 90 MNs (NS-3 nodes) which can move at the same time.



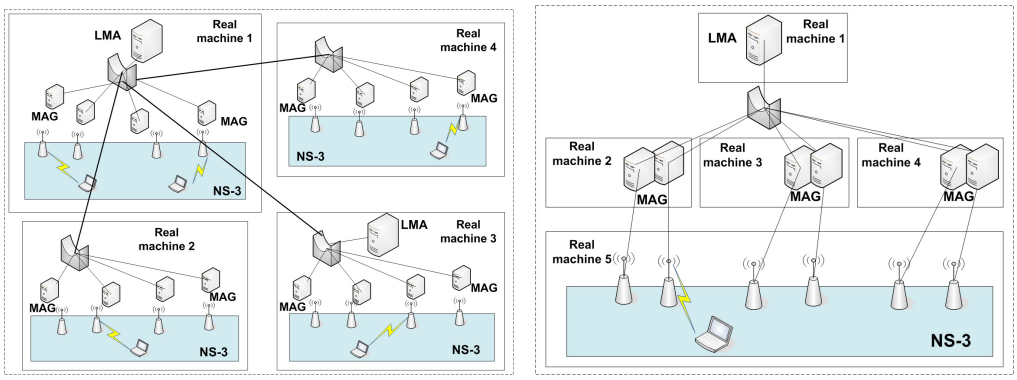
(a) (b)

Figure 3.5 – Resource usage: a) CPU, b) Memory.

The CPU and the memory consumption in the PMIP-NS3 are illustrated in Fig. 3.5a and Fig. 3.5b, respectively. As we can observe in Fig. 3.5b, the memory consumption in the

configuration 1 and the configuration 2 are almost the same. That means with the same number of virtual machines, increasing number of mobile nodes inside NS-3 does not add much more resources. On the contrary, the CPU consumption (see Fig. 3.5a,) is totally different. It is because the LMA and MAGs have to process PBU/PBA message from a lot of MNs. Also, the CPU required by NS-3 is increased. The same thing happens in case of the configuration 3 and the configuration 4.
In general, host memory/CPU is often the factor limiting the number of virtual machines that a host can support. Moreover, since many virtual machines are deployed in a single real machine, the host machine is easy to become overloaded. It influences the overall testbed especially in performance experiment. In our experiment, the memory and CPU consumption in the worst case is around 41 and 46 percent, respectively. These values seem not too high, however, it can be considered as a trade-off between the number of deployed nodes and the performance of the system (during peak period, it may consume up to 69.65% CPU, 80.07% memory).

3.3.6.4 Distributed Experiment Environment



(a) (b)

Figure 3.6 – An example of distribution technique.

In the experiment described in the previous subsection, the testbed can support up to 10 MAGs and 90MNs. While it is suitable for a medium scale experiment, it is not enough for a large scale one. The number of supported nodes is limited since the experiment environment is realized on a single machine which has limited resources. Some of them are consumed by the virtual machines, and some are by the simulator NS-3.
To overcome this limitation, the testbed can be deployed in a distributed manner among different physical machines. There are several methods to deploy the proposed testbed in a distributed way. The first method divides the network into several sub networks in which each sub network is deployed in a single host machine. For example, in Fig. 3.6a, a PMIPv6 domain deployed at the real machine 1 is extended by implementing the extra LMAs, MAGs in different real machines (machine 2, 3, 4).
To illustrate this method, we deployed a testbed in two different physical machines. A PMIPv6 domain has been deployed in the first real machine similar to in the previous section (testbed in a single machine). Some MAGs then have been installed in the second machine. As a result, we can deploy a network with two LMAs, 21 MAGs and 150 MNs. However, one limitation is that the PMIPv6 domain is divided into different *sub networks* (in different computers) in which the MN cannot move between sub networks. Some extra techniques should be applied to allow the MN to move between different real hosts such as

MPI for distributed simulation [157]. Another method addresses this limitation by putting the wireless environment in only one physical machine as described in Fig. 3.6b. In this case, the tunneling mechanism is required to connect multiple MAGs with their APs via only one interface. However, it raises some other issues as mentioned in [158].

3.4 Conclusion

This chapter at first gives the performance metrics which are crucial to evaluate a proposal for IP mobility management as well as IP mobile multicast. These metrics are then presented in details from a mathematical point of view. Next, we discuss different methods of experimentation for wireless mobile networks. We argue that, the most widely used method – simulation – sometimes lacks credibility in produced results, which is a critical issue for solution deployment. Furthermore, the use of real testbeds can obtain more reliable results, though they are much more costly and only built in a small scale. We then introduce a hybrid method which is a combination of virtualization and simulation. Through the study of a simple use-case showing mobility with PMIPv6, we demonstrate that our proposed method provides realistic results at a low cost. In other words, the near-to-real results can be achieved even with limited resources by using the proposed method. Additionally, this method can be deployed in a distributed manner for increased scalability.
As in our proposed testbed, the MNs are the NS-3 nodes, thus, it is suitable for the experiment that does not require any specific functions/components at the MNs. Vice versa, the extra effort is needed to deploy the additional components/functionality required in NS-3. As a result, for the experiment which does not require a lot of MNs and requires some extra functions at MNs, instead of deploying the MNs inside NS-3, we can deploy UML machines as MNs e.g., streaming source. This scenario is described in [25]. In addition, in some cases, real wireless/wired environment should be provided. A real machine can be used as an MN, while the network entities are deployed in another computer similar to in [17].
In order to validate a multicast solution in a mobile environment, the experimental results should be provided with high degree of confidence. In this context, our proposed testbed is basically suitable for measuring such performance metrics as multicast service disruption and packet loss, end-to-end delay and load balancing (scalability) when mathematical model is suitable for signaling and packet delivery cost, packet duplication and tunneling overhead.

Conclusion of Part I

In Part I of this thesis, we have given a brief introduction to IP multicast, IP mobility and identified the issues and challenges when considering multicast in a mobile environment as well as introduced the solutions for these issues mainly from the IETF point of view. We have presented the evaluation metrics to assess the performance of a mobile multicast solution and a near-to real testbed which allows achieve the realistic results at low cost.

In Chapter 2, we have discussed the basic concepts of IP multicast regarding the multicast address, the architecture, the models and possible applications. Two groups of protocol are needed for providing multicast service, namely multicast group management and multicast routing protocols. We concluded that these protocols, which are originally designed for a fixed network, may not suitable in a mobile/wireless environment. We have then presented various mobility management protocols ranging from the host-based to the network-based, from the centralized to the distributed approach. We focused on PMIPv6 as a typical example of the network-based and the centralized approach. DMM also was presented, mainly focusing on the network-based approach. Note that, from now on, only the network-based mobility management protocols are considered. Starting from the issues/challenges raising when considering IP multicast in MIPv6, we investigated, in details, the multicast-related issues in PMIPv6 from different aspects (general issues, the listener-specified, the source-specified and the deployment issues). We concluded that the mobility of the node has different impacts on the multicast service depending on such factors as the role of the node in the multicast session (source or listener), the considered multicast model (ASM or SSM), the multicast routing protocol, the multicast group management protocol and the mobility protocol in use as well as wireless access technology. In the scope of this thesis, we mainly focus on the service disruption and packet loss; tunnel convergence; sub-optimal routing and end-to-end delay; and leave latency and waste of resources.

In Chapter 3, the performance evaluation metrics to efficiently assess the performance of a mobile multicast solution has been introduced. We have then presented a near-to-real testbed which allows achieving the realistic results at low cost. The PMIPv6 testbed then can be used to evaluate the solutions in the next Parts.

Part II

IP Multicast Mobility in Proxy Mobile IPv6

Overview of Part II

In Part II, we consider different aspects of multicast mobility in a PMIPv6 domain. Starting with a basic issue - service disruption, this Part then discusses the multicast mobility-related issues in heterogeneous network. As multicast service is becoming popular, scalability and reliability issue should also be taken into account.

Chapter 4 focuses on the service disruption caused by the movement of a listener in a PMIPv6 domain. Since the base solution for the multicast listener in PMIPv6 does not address any specific optimization and performance issues, an effective method, which is based on the combination of the multicast context transfer and the explicit tracking function, will be proposed to minimize the service disruption. Another contribution of this chapter is that a near-to-real testbed for multicast mobility is provided. This testbed allows simulating the movement of multiple sources and listeners at the same time. A real implementation of both PMIPv6 and the multicast-related components (MLD proxy, multicast context transfer and explicit tracking function) are provided. A listener part of MLDv2 is also implemented in NS-3.

Chapter 5 discusses the scalability issue raised when considering a large number of mobile nodes together with their traffic demand. From the fact that multicast is the main service of the future internet and the mobile video content which is typically has much higher bit rates than the other content types, the multicast service should play a crucial load factor on the LMA. The consideration of multicast in the existing load balancing (LB) mechanisms can lead to several issues from both LB (efficiency degradation) and multicast service perspective (e.g., tunnel convergence problem and service disruption). Thus, a LB among LMAs taking multicast into account is proposed. The proposed solution helps better distribute the load among the LMAs (caused by the multicast flows) in runtime, thus, improving the efficiency of resource utilization. Moreover, the proposed solution does not influence the ongoing unicast/multicast sessions (except the selected session with which the multicast service disruption, in most cases, satisfies the requirements for the real-time services).

Chapter 6, via analyzing a use case of electric vehicle charging service (EVCS), discusses the issues and then proposes solution for a node moving in heterogeneous networks. Although the heterogeneous networks provide the possibility for greatly increasing capacity at a low cost, seamless mobility across different wireless access technologies e.g., WLAN, WiMAX and LTE needs to be taken into account. In the context of EVCS, a mobile node (an Electric Vehicle (EV)), can be connected with the infrastructure via different wireless/wired technologies in different steps: LTE while driving, WLAN while approaching a charging infrastructure, and PLC while being docked at a charging infrastructure. In the context of connecting vehicles which is gaining momentum, vehicle is a good example for considering the mobility in the heterogeneous networks. In addition, considering multicast in the EV is one step to enable the entertainment system in the EV, which is becoming more and more popular e.g., software update of the in-vehicle systems.

4
Optimizing Service Continuity in a Single PMIPv6 Domain

4.1 Introduction

As stated in Chapter 2, a base solution has been recently adopted for supporting multicast listener mobility in PMIPv6. This solution brings the multicast listener support into PMIPv6 by placing the multicast routing and the MLD proxy function at LMA and MAG, respectively. Nevertheless, it does not address any specific optimization and performance issues such as handover latency, tunnel overhead, and non-route optimization, etc. Specially, this chapter focuses on the handover performance in terms of service disruption time.

This chapter proposes a method based on the combination of the multicast context transfer and the explicit tracking function to minimize the service disruption time. Starting with the service disruption time analysis, experiments are then conducted to compare between different approaches relying on a testbed using the method described in Chapter 3. The numerical and experimental results show that through the utilization of multicast context transfer, the service disruption time can be reduced significantly. By tuning the behavior of the MLD for routers, we can also achieve a similar result, but make a dramatic increasing of multicast-related signaling. Especially, the problem will be more serious with a large number of multicast listeners. In addition, thanks to the multicast context transfer, the handover latency is minimized. Thus, this chapter mainly validates the effectiveness of the context transfer protocol compared to the other methods. In the next chapters, the context transfer protocol in general can be considered in the proposed solutions. Note that the implemented multicast context transfer and explicit tracking functions can be used in our testbed as well as in a real one. Our testbed can be served as a near-to-real one, which can provide realistic results at low cost for the multicast mobility experimentation in a PMIPv6 domain.

The rest of this chapter is organized as follows. Section 4.2 summarizes the proposals to reduce the multicast service disruption during handovers. Our solution is also presented in this section. Section 4.3 provides a performance analysis in terms of multicast service disruption time. In Section 4.4, the testbed implementation and the experimentation scenarios are introduced. The experimental results, the evaluation as well as the discussions on the impact of MLD traffic on the wireless link are presented in Section 4.5. Eventually, Section 4.6 concludes this chapter.

4.2 Multicast Listener Mobility and Service Continuity

In PMIPv6, when a listener performs a handover from the previous MAG (pMAG) to the new one (nMAG), several operations should be executed in order to allow the MN to continue receiving the multicast traffic from the nMAG: i) typical PMIPv6 operations; ii) acquisition of the MN's multicast subscription information at the nMAG; and iii) joining and getting multicast the first multicast packet at the nMAG. In the context of this chapter, the MAG always gets the multicast traffic from the corresponding LMA (following the tunnel-based approach), thus, the joining time depends on the delay between LMA and MAG. As a result, from the multicast service point of view, only the subscription acquisition time can be reduced to mitigate the total service disruption. Moreover, these operations can be done in parallel.

To decrease the service disruption time, the aim is to reduce the time needed by the nMAG to get knowledge of the MN's active multicast subscription information during handovers. So that the nMAG can subscribe to the on-going multicast flows (in advance) and forwards the multicast packets to the MN as soon as possible. To achieve that, there are two main strategies. The first one is based on the multicast context transfer exchanged between the pMAG/ LMA and the nMAG. The second one is still based on the normal MLD operations, however, tuning the MLD parameters to minimize the service disruption.

In more details, there are two different approaches in the first strategy. In the former, the nMAG gets the MN's subscription information from the LMA [116] while in the latter from the pMAG. The former case [116] is based on the idea that the multicast subscription of the listener is only critical during handover, neither after nor before. The active multicast membership information of the listener will be stored in the LMA (if necessary), and then the nMAG will interrogate the LMA to obtain this information (called M-LMA approach). Two modes of operation are then defined: the proactive and the reactive handover. In the proactive-handover, the listener firstly de-registers on the LMA by the pMAG before attaching to the nMAG. The de-registration message (PBU) will be extended to convey the listener's subscription information. The LMA stores the subscription information, and then sends it to the nMAG by using an extension of PBA message. On the contrary, the LMA receives the registration for the listener from the nMAG without the de-registration BU from the pMAG in the reactive-handover. Thus, upon receiving the PBU from the nMAG for the listener's registration, the LMA queries the listener's subscription information from the pMAG, and sends it to the nMAG using an extension of PBA. However, this solution does not mention clearly how the pMAG gets the active multicast subscription of the listener (e.g., by enabling explicit tracking function, extract membership status from forwarding states at node-specific point-to-point links, or normal MLD operation). In addition, the LMA commonly serves a huge amount of MNs, thus, the additional tasks like interrogation of pMAG for the subscription information and storage of the active multicast subscription may put additional load on the LMA. Also, this solution may introduce an additional delay for the unicast traffic.

The second approach (called M-FPMIP) [108] extends the PMIPv6 fast handover protocol [78] to support the multicast. Similarly, two possible handover modes are considered: the predictive and the reactive mode. In the predictive mode, after the detection of the up-coming movement of the listener, the multicast context transfer is exchanged between the pMAG and the new one. In this case, the acquisition of the listener's multicast subscription information is done by either using an MLD Query/Report mechanism or the explicit tracking function. The nMAG then can receive the active multicast groups from the pMAG. In the reactive mode, the nMAG relies on the normal MLD process to obtain the subscription information, thus, may lead to a significant service disruption. In both cases, the link-layer

information is required to obtain the address of the nMAG/pMAG. Therefore, this solution strongly depends on the access link-layer technology. Also, an additional support is required on the mobile node.
The second strategy [115] is tuning the behavior of the MLD for routers (namely M-MLD). By varying the Query Interval (QI) and Query Response Interval (QRI), the routers can tune the service activation time and join latency. Slow multicast service activation following a join may incur an additional delay in receiving multicast packets in the nMAG. By reducing the QI and QRI, the service disruption time can be lower but resulting in the increase of the multicast-related signaling. In addition, the departure of the MN without leaving the group in the pMAG may cause the network resources waste.
In order to minimize the modification required by the PMIPv6 protocol, we introduce a solution following the idea of using the context transfer from the pMAG to the current one (called M-CXT). Although the idea of using multicast context transfer is not new (can be found in several proposals [108, 123, 122]), however, instead of relying on the link-layer information to get the address of pMAG, we extend the PBA message to convey the pMAG's address. Thus, this solution is independent of layer 2 technologies and easier to deploy than the existing proposals. The multicast context transfer is also developed following the standard for the context transfer protocol [159]. Additionally, the proposed solution does not put any additional load on the LMA, which makes our solution better the M-LMA in terms of scalability. Based on the proposed solution, experiments are then will be conducted mainly to validate the advantage of the multicast context transfer compared to the strategy in which the tuning MLD parameters is required.

4.3 Multicast Service Disruption Time Analysis

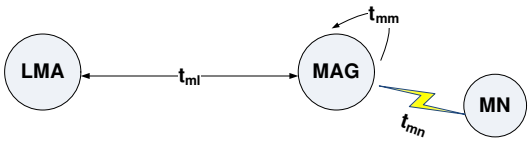


Figure 4.1 – Reference network topology.

Fig. 4.1 shows a reference topology for performance analysis. The delay factors consisting of total delay are defined as follows:

- t_{mm}: the delay between two MAGs.
- t_{ml}: the delay between MAG and LMA.
- t_{mn}: the delay between MAG and MN.
- t_{msa}: the multicast service activation time.
- t_{qrd} the query response delay.

The service disruption time for multicast service is defined as a period when a multicast listener cannot receive the multicast packets. Thus, as can be seen in Fig. 4.2, it can be split into three main contributions (as stated in Chapter 3): i) Layer 2 (L2) handover latency (t_{L2}); ii) Layer 3 (L3) handover duration (t_{L3}) caused by IP-related procedures. In PMIPv6, it includes the time for mobility management procedures (movement detection and location update procedures); and iii) The delay due to the multicast-related procedures, called $t_M(.)$.

Since in the proactive mode of M-LMA approach, it is not always feasible to the MN de-registers on the LMA by the previous MAG before attaching to the new one. Also, in the M-FPMIP approach, the under link radio access technology needs to support layer-2 triggers. Thus, in this section, the performance analysis will be done considering only the M-LMA (reactive-mode), the M-MLD and the M-CXT approaches.

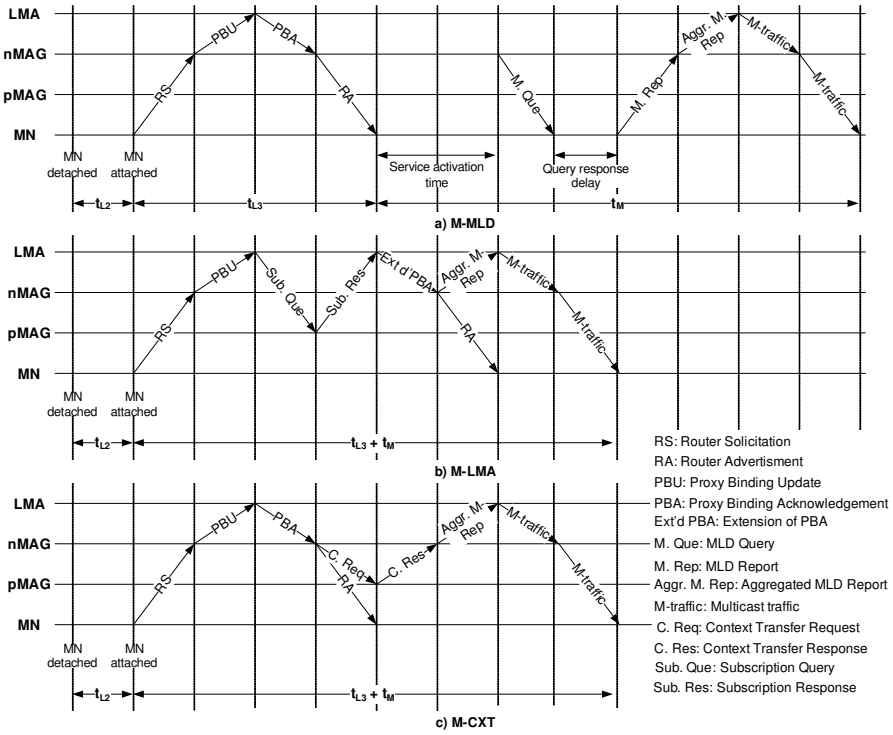


Figure 4.2 – Multicast-related signaling for handover: (a) M-MLD, (b) M-LMA, (c) M-CXT.

Let $t_{X,Y}$ denote the delay between node X and node Y. Then, the service disruption time is defined as

$$SD(.) = t_{L2} + t_{L3} + t_M(.), \tag{4.1}$$

where t_{L3} and $t_M(.)$ are given by

$$t_{L3} = 2t_{mn} + 2t_{ml}, \tag{4.2}$$

$$t_M(M - MLD) = t_{msa} + t_{qrd} + 3t_{mn} + 2t_{ml}, \tag{4.3}$$

$$t_M(M - LMA) = t_{mn} + 4t_{ml}, \tag{4.4}$$

$$t_M(M - CXT) = t_{mn} + 2t_{mm} + 2t_{ml}. \tag{4.5}$$

We suppose that MLD Queries are followed immediately the link-up event or the auto-configuration of IPv6 link-local address of an MN [119]. As a consequence, the multicast service activation time can be ignored ($t_{msa} = 0$). As such, the total disruption time in the M-MLD approach is

$$SD(M - MLD) = t_{L2} + t_{qrd} + 5t_{mn} + 4t_{ml}. \tag{4.6}$$

In case of M-LMA approach, the service disruption is calculated as

$$SD(M-LMA) = t_{L2} + 2t_{mn} + 6t_{ml}. \tag{4.7}$$

Using the multicast context transfer and the explicit tracking function, the context transfer function and layer 3 operations are executed in parallel as illustrated in Fig. 4.2 (c). Consequently, the service disruption time in the M-CXT approach is calculated as follows

$$SD(M-CXT) = t_{L2} + 2t_{mn} + 2t_{mm} + 4t_{ml}. \tag{4.8}$$

4.4 Experimentation Setup and Scenarios Description

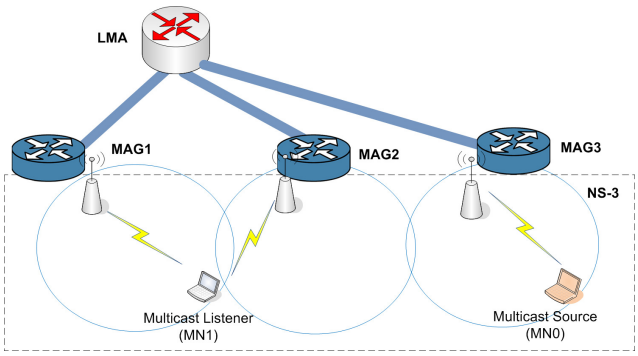


Figure 4.3 – Virtual PMIPv6 testbed.

A reference topology for multicast support in a PMIPv6 domain is illustrated in Fig. 4.3. The testbed - which consists of one LMA, three MAGs and two MNs, was developed based on the method described in Chapter 3. For a quick reminder of this method, the testbed is a combination of virtual machines and wireless environment provided by the network simulator NS-3. The PMIPv6 entities (LMA, MAG) are the virtual machines while the access points (AP) and mobile nodes (MN0 and MN1) are NS-3 nodes. MN0 plays the role of a multicast source while MN1 plays the role of a multicast listener. Acting as a multicast listener, MN1 is subscribed to the multicast channel which is being broadcasted by the source. To deploy a PMIPv6 domain, the open source PMIPv6 implementation, named OAI PMIP [155], is used. In OAI PMIPv6 implementation, the attachment/detachment phase for the MNs relies on SYSLOG [160] message exchanged between Client (at the AP) and Server SYSLOG (at the MAG). Thus, the Client SYSLOG function is implemented in NS-3 and deployed at the APs.
To enable the multicast support in a PMIPv6 domain, the MLD proxy function needs to be deployed at the MAG while the multicast routing function is provided at the LMA. There are two typical implementations of MLD proxy such as McProxy[1], ECMH[2]. Though the former is newer, it only supports MLDv1. That is why ECMH is selected. Yet, some functions need to be added into ECMH to support the multicast source mobility. On the other hand, the considered multicast routing protocols are PIM-SM/SSM [41]. There are two potential candidates providing PIM router functions: MRD6[3] and XORP[4]. The first one is chosen because of its simplicity of deployment and configuration under UML. We

[1]McProxy - Multicast Proxy for IGMP/MLD, Homepage: http://mcproxy.realmv6.org/
[2]ECMH - Easy Cast du Multi Hub, Homepage: http://unfix.org/projects/ecmh/
[3]MRD6, Homepage: http://fivebits.net/proj/mrd6/
[4]Xorp, Homepage: http://www.xorp.org/

also implemented the listener part of MLDv2 protocol under NS-3 to enable the multicast capability of NS-3 nodes.

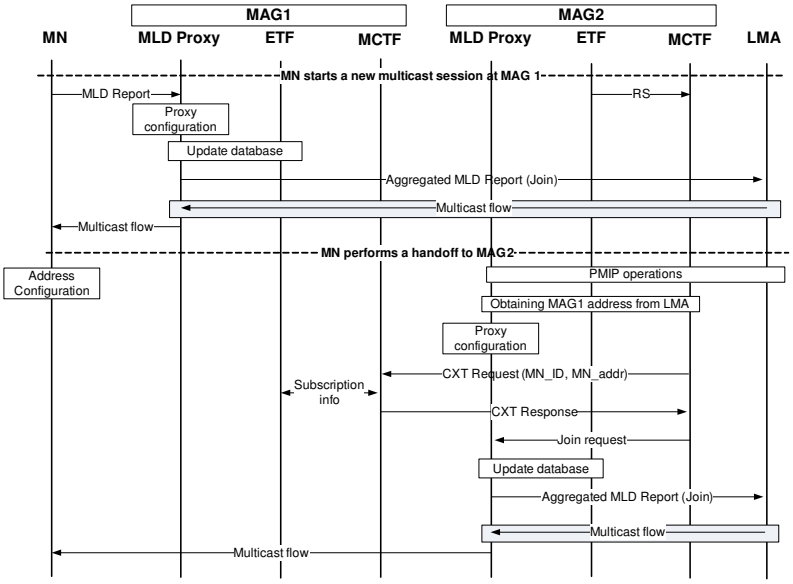


Figure 4.4 – Interaction between components of MUMO.

In general, we implemented a multicast mobility management module (MUMO, in C/C++), which takes responsibility for all actions related to the multicast mobility as described in [14, 15] at the MAG. The structure of this module is briefly described as follows: i) The proxy function performs the operation of the MLD proxy (based on ECMH); ii) The explicit tracking function (ETF) maintains the per-host multicast membership state (can be considered as an extension to MLD proxy); and iii) The multicast context transfer function (MCTF) is responsible for the multicast context transfer exchanging between MAGs to reduce the service disruption time. The interaction between the different components of this module is illustrated in Fig. 4.4. Note that the multicast context transfer function, which is developed as a separate sub-module, can be easily applied to the other solutions in PMIPv6 (e.g., direct-routing approach) as well as for the solutions in a DMM environment (see Chapter 8 for more details).
From the fact that the service disruption time in M-CXT would be the same as in the M-LMA approach (as can be seen in Fig. 4.2), for a sake of simplicity we do not consider the M-LMA approach in our measurements. In other words, the experimentation will be conducted regarding only the M-MLD and the M-CXT approaches corresponding to two simulation scenarios as follows:

- Scenario 1: tuning the behavior of the MLD for routers (corresponding to the M-MLD approach). In this scenario, the regular behavior of MLD protocol takes place while the QRI is varied to measure the service disruption time. Upon receiving an MLD Query at the new link, the listener (MN1) replies by a regular MLD Report. Then, the nMAG sends an aggregated MLD Report to the LMA to join the multicast group on behalf of the listener. Thus, the multicast traffic originated from the source is routed from LMA to listener via the new tunnel LMA-nMAG.

- Scenario 2: using the multicast context transfer (corresponding to the M-CXT approach). When the multicast context transfer is used, by detecting the presence of a

new listener, the multicast context transfer between nMAG and pMAG is executed, allowing nMAG to get the listener's active multicast subscriptions. As an MLD proxy, nMAG joins the multicast group on behalf of the listener, and forwards the multicast packets to the listener.

To make sure that the experimental results reflect exactly the impact of the two strategies, the parameter QRI will be varied in both scenarios. According to [35, 115], possible values of QRI using in the experimentation are 10, 5 and 2 seconds. Additionally, by now to simplify the experimentation, a simple mobility model is used: the listener moves between two MAGs with a fixed speed and a fixed direction. However, in the future, the mobility pattern will be applied to provide more flexible mobility of multicast listener. Also, the scenario in which many listeners are moving at the same time will be considered. To improve the credibility of the simulation results, we performed the experiment a large amount of times for each scenario. Based on the collected results, we calculate the average value and the standard deviation to improve the degree of confidence.

4.5 Results and Discussions

4.5.1 Results

Numerical Results In our analysis, t_{L2}, t_{ml}, t_{mm} and t_{mn} are assumed to be 50ms, 20ms, 10ms and 15ms, respectively, according to the literature [161]. Fig. 4.5 shows the numerical results. It is observed that the service disruption time in the M-MLD approach is definitely higher than that in the other approaches. On the other hand, the service disruption in case of M-CXT is a bit smaller than that in M-LMA (smaller is better). In other words, the M-CXT approach in general gives a similar performance in terms of service disruption as the M-LMA approach.

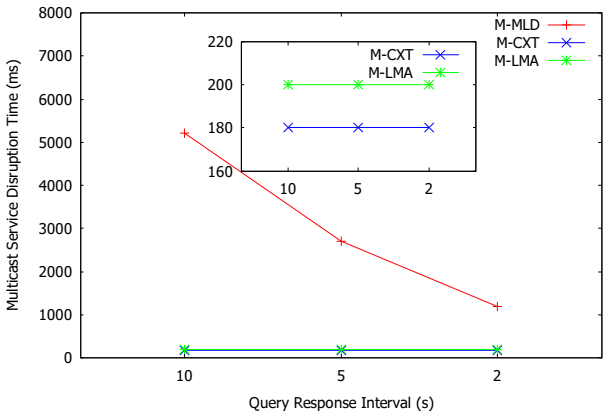


Figure 4.5 – Service disruption time: numerical results.

Experimental Results Fig. 4.6 describes the experimental results for the service disruption time in terms of mean ($< x >$) and standard deviation ($< \sigma_x >$). It appears clearly that the service disruption time in the M-MLD approach is absolutely higher than that in the M-CXT due to the value of t_{qrd}. As expected, the service disruption time in the former case decreases proportionally with the QRI, while almost keeping as a constant as the decreasing of QRI in the latter case. The average value of service disruption time in the

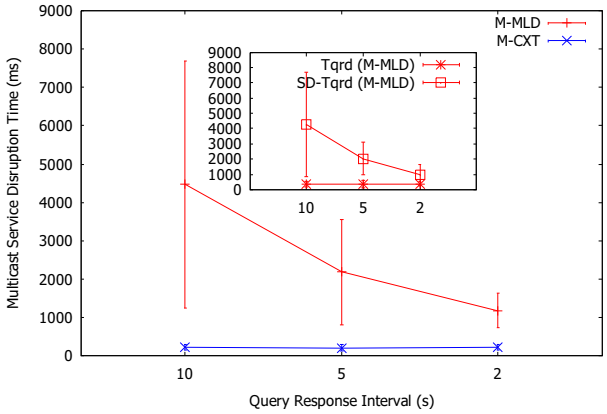


Figure 4.6 – Service disruption time: experimental results.

M-MLD is 1180ms (σ= 445.4ms) in the best case (when QRI is set to 2s), which still makes the impact of handover noticeable. If the multicast context transfer is used (M-CXT), in average, the service disruption time is around 220.53ms. Consequently, the handover impact on the quality of multicast stream is almost imperceptible. The variation of service disruption time in the M-MLD approach is clearly seen since it depends on several factors like scanning, association, authentication and t_{qrd}. Even t_{qrd} can spread out over the large interval [0, QRI], $< t_{qrd} >$ is definitely higher than that of other delay types (L2 and L3). Hence, t_{qrd} is the crucial factor in the service disruption time.

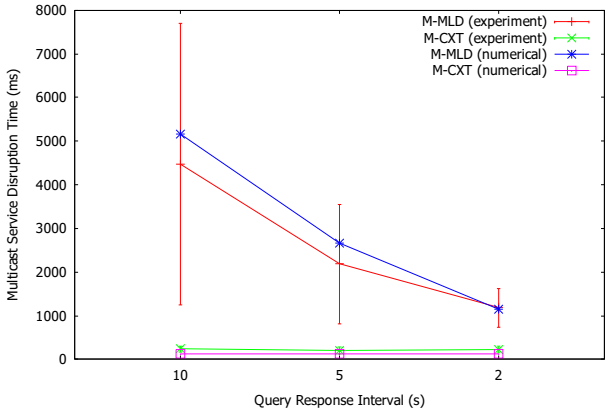


Figure 4.7 – Service disruption time: experimental vs. numerical results.

Numerical vs. Experimental Results Now the comparison between the numerical and the experimental results is investigated. For a fair comparison, we do not consider t_{L2}, since it depends on a specific wireless technology. Fig. 4.7 describes the numerical and experimental results. It is observed that the experimental results are, in general, in line with the theoretical analysis.

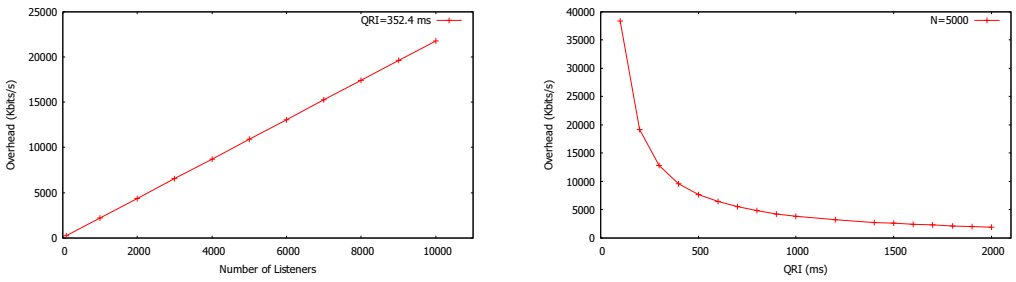
4.5.2 Discussions

Impact of QRI Reduction on the Wireless Link Condition If no multicast context transfer is used, the service disruption during handover can be clearly seen, even in the best

case (QRI=2s). To minimize the handover effect, the value of the query response delay (t_{qrd}) needs to be reduced. It is done by decreasing the QRI. This reduction facilitates to achieve a seamless handover but makes the traffic more bursty, leading to the signaling overhead over the air interface.
Following the MLDv2 protocol operation, after receiving an MLD query (periodical query or a query caused by a link-up event), the multicast listeners reply by an MLD Report at the interval selected randomly from the range [0, QRI]. As such, during the period [0, QRI] there are n MLD Report messages generated on the link (where n is the number of multicast nodes attached to MAG). The number of signaling messages is dramatically increased compared with those in case of the context transfer (only 2 messages are exchanged between MAGs via a wired link). The total air interface signaling overhead in the uplink direction is calculated as the size of MLD Report message multiplied by the number of MLD Report messages per second. Let s denote the average size of MLD Report message, which is 96 bytes [15]. Thus, the total overhead is expressed as

$$OH = \frac{n \cdot s}{QRI} \tag{4.9}$$

From the experimental results, $SD(M - CXT)$ in the worst case is 507.5ms. From Eq. (4.6), to achieve a similar delay without any context transfer, t_{qrd} must be less than or equal to a value of 352.4ms (when $t_{L2} = 0.1$ms). It is done by setting QRI to a value of 352.4ms. It was also proven by the simulation results in which the mean and standard deviation of service disruption time are 465.43 and 70.3 ms, respectively. With this value of QRI, Fig. 4.8 illustrates the air interface overhead. In more details, Fig. 4.8a shows the overhead as a function of the number of listeners attached to one MAG. As the number of listeners increases, the signaling overhead increases. For example, considering a typical PMIPv6 deployment in which a MAG severs approximately 5000 MNs [119], the signaling overhead is 10896 kbits/s ($\approx 10.8 Mbit/s$). It may cause a negative impact to the wireless network since the wireless link is a typically bandwidth limited. Fig .4.8b shows the signaling overhead when the value of QRI is varied over a range [100, 2000]ms. The overhead decreases when QRI increases. When QRI is small, the signaling overhead causes a noticeable impact to the wireless link. Thus, it is obvious that reducing the service disruption by using QRI should be carefully investigated at a cost of high signaling overhead and increase of power consumption at the mobile node.



(a) (b)

Figure 4.8 – Air Interface signaling overhead: (a) as a function of number of listeners (n), (b) as a function of QRI.

Waste of Resource (Leave Latency) Issue Due to mobility, the listener moves from the pMAG to the nMAG without explicitly sending an MLD message to leave the multicast

group at the pMAG. As a result, if the listener is the last member of this group, the pMAG still continues forwarding this flow until it updates the membership information. In more details, according to [35] the MLD proxy at pMAG has to wait to the source timer expires, then sends a source specific query and waits for a report during the time specified by the value of Last Listener Query Timer (LLQT) (during LLQT time, the pMAG should send Last Listener Query Count (LLQC) - 1 retransmissions of the query). The source timer at the beginning is set to the value of the Multicast Address Listening Interval (MALI). As a result, the total time needed for the pMAG to recognize that the last member has left its subnet is calculated as

$$LL = MALI - T_{leave} + LLQT, \tag{4.10}$$

where

$$MALI = RV \cdot QI + QRI, \tag{4.11}$$

$$LLQT = LLQI \cdot LLQC, \tag{4.12}$$

where LLQI is Last Listener Query Interval and RV is the Robustness Variable. T_{leave} is the interval time between the last source timer update and the moment where the listener leaves the pMAG. Thus, in average

$$T_{leave} = \frac{QI + QRI}{2} \tag{4.13}$$

Without the explicit tracking function, the default value of RV, QRI, QI, LLQI and LLQC is 2, 10s, 125s, 1s and 2, respectively. While in case of explicit tracking function, the value of RV can be set to 1 or 2 depending on the link condition [115]. Also, QRI may be set to 5, 10, and 20s. Thus, in the normal case, the leave latency is 194.5s, while in case of explicit tracking is 191s (in the best case, where RV and QRI are set to 1s and 5s, respectively). During this period, the pMAG continues forwarding the multicast traffic even though no listener is interested in this flow, leading to a significant waste of resource. Even with the explicit tracking function, the leave latency is slightly reduced. Taking benefit of the context transfer function, the nMAG can request the pMAG to stop forwarding the multicast flow by means of CXT Request message (see Fig. 4.4). Thanks to this mechanism, in our experiment the leave latency is 105.6ms (standard deviation = 45.2). Thus, the leave latency is negligible.

4.6 Conclusion

This chapter focused on the effect of using the multicast context transfer and tuning the behavior of the IGMP/MLD for routers on handover performance of multicast listener mobility. The numerical and experimental results showed that through the utilization of multicast context transfer, the service disruption time could be reduced significantly without increasing the multicast-related signaling. We also observed that by tuning the behavior of the IGMP/MLD for routers, we could achieve a similar result, but make a noticeable multicast-related signaling increase. Thus, the impact of the multicast-related signaling on the wireless link by the number of listeners and the value of QRI was studied. In addition, the solution based on the multicast context transfer helps minimizing the handover latency. This chapter also presented an enhanced version of the testbed described in Chapter 3 by introducing the multicast mobility support. We deployed a real implementation for the multicast context transfer and explicit tracking functions on our testbed. This implementation then can be directly applied in a real testbed. In more details, in the Medieval project,

the real multicast testbed [15, 161] has been deployed to validate the effective of multicast context transfer for PBS consumers over a DMM environment.

5
Load Balancing of Multicast Flows in PMIPv6 Networks

5.1 Introduction

The increasing penetration of the mobile devices, such as tablets and smart phones is generating a huge number of data traffic, especially video traffic over mobile networks [6, 1]. In this context, it is common to have a huge number of devices associated with the LMA in a PMIPv6 domain, thus, easily making the LMA a bottleneck and single point of failure. Consequently, the quality of the ongoing sessions could be degraded (e.g., longer queuing delay, and increased packet loss). In this context, mobile network operators may need to deploy multiple LMAs in a large PMIPv6 domain, so that the traffic can be distributed among the LMAs [76]. Yet, it is highly possible that some LMAs become overloaded while others are underutilized. Consequently, load balancing (LB) among the LMAs is needed.
From the fact that multicast is expected to be widely deployed in the near future to deal with a huge demand of multimedia traffic, as well as the mobile video content typically has much higher bit rates than the other content types, the multicast service should play a crucial factor in putting load on the LMA. However, its role has been neglected in all existing LB proposals. Therefore, the consideration of multicast in the existing LB mechanisms can lead to several issues from both LB (efficiency degradation) and multicast service perspective (e.g., tunnel convergence problem and service disruption).
For these reasons, a LB mechanism which takes the multicast service into account is needed. In this chapter, we will introduce such LB mechanism, the so-called multicast-based mechanism. The key idea is that by separating the multicast LB from the unicast LB, the proposed solution helps better distribute the load among the LMAs in runtime, thus, improving the efficiency of resource utilization. In details, when an LMA is overloaded, a multicast session will be selected to move to a less loaded one. The LB will also be executed when a listener starts a new multicast session to select the appropriate LMA to serve this session. As a result, the proposed solution does not influence the ongoing unicast/multicast sessions (except the selected session with which the multicast service disruption, in most cases, satisfies the requirements for the real-time services [162]). It is noted that this chapter mainly focuses on the multicast listener.
The rest of this chapter is organized as follows. Section 5.2 highlights the issues when considering multicast with the existing LB mechanisms. Section 5.3 introduces the multicast-based LB as well as the criteria for the LMA and multicast session selection. Section 5.4 presents the performance analysis regarding LMA load and multicast service disruption. Section 5.5 takes a look on the experiment testbed including the testbed description, the experiment scenarios and the collected results. Finally, Section 5.6 concludes this chapter.

5.2 Multicast Consideration in the Existing LB Mechanisms

There are two main approaches for LB among LMAs in PMIPv6, namely, proactive-MN and reactive-MN. In the proactive-MN approach [163, 164], the LB will be executed in the initial phase of an MN to select the least loaded LMA. This approach only takes the current load of the LMAs (neither unicast nor multicast service) into account. All mobility sessions of this MN then would be anchored at the assigned LMA during their lifetime in the domain. The main advantage of this approach is that it does not influence the ongoing sessions of the registered MNs. However, since it is executed in the initial phase of an MN, the varying session rate and data rate may cause the unfair load distribution among the LMAs. When an LMA is overloaded, it may drop the new sessions. It also causes several issues for the ongoing sessions such as service disruption and packet loss.

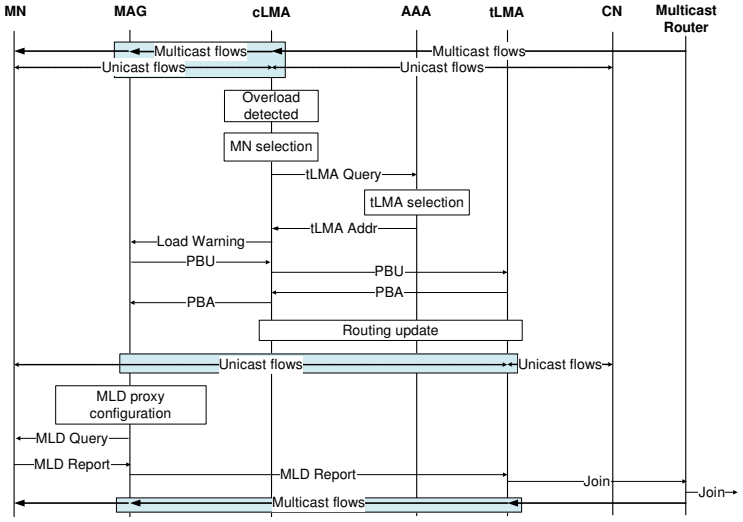


Figure 5.1 – Multicast considerations in the reactive-MN approach.

In the reactive-MN approach [165, 166], the LB will be triggered when the LMA load exceeds a specified threshold. The overloaded LMA will select one (or several) MN(s) to move to a less loaded LMA (called target LMA, or tLMA). The load information of all LMAs can be collected and managed at the authentication, authorization and accounting (AAA) server which then selects the tLMA among the LMAs in the domain. The PBU/PBA messages then are exchanged between the current LMA (cLMA) and the tLMA allowing the tLMA to serve as a new mobility anchor of the MN. This approach allows the network to adapt to the current situation. Thus, it may give a better performance e.g., distributing load among LMAs and increasing the reliability. Since the LMA plays the role of the mobility anchor for the MN, changing LMA during the mobility session could impact the selected MN's ongoing sessions. For this reason, this change is not recommended by the IETF [163, 164]. In addition, the existing proposals only consider the ongoing sessions as the unicast ones. How the LB works with the multicast is still an open question.
To support multicast in a PMIPv6 domain, the multicast router (MR) and the MLD proxy function need to be deployed at the LMA and the MAG, respectively [119]. In the base solution, a listener always receives the multicast traffic from its LMA via the LMA-MAG tunnel. As stated earlier, several procedures need to be executed in order to allow the MAG to continue receiving the traffic (from the tLMA). As a result, it experiences a noticeable

service disruption for the ongoing multicast channels. Additional mechanisms (e.g., MLD proxy peering function [118]) are required to reduce the service disruption time.
If there is more than one listener (including the selected one) associated with the cLMA and subscribing to the same multicast channel, the cLMA will continue forwarding this channel. Consequently, moving the MN cannot help significantly reduce the LMA load, especially when the load generated by this MN is mainly from this channel. The total load of all LMAs may also be increased since the tLMA may need to join the channel. In addition, as the LMA selection algorithm does not take multicast into account, the tLMA may not support the multicast capability. In other words, the multicast service cannot be guaranteed at the tLMA. Also, since many proxy instances are installed at MAG, it may cause the tunnel convergence problem.

5.3 Multicast-based Load Balancing Solution

In this section, at first, some criteria to select the appropriate LMA and multicast session for the LB purpose will be discussed. Two different approaches of the multicast-based solution i.e., the proactive-multicast (or MAG-initiated) and the reactive-multicast (or LMA-initiated) approach are then considered. In the former case, LB will be invoked when an MN starts a new multicast session to select a suitable LMA to serve this session. In the latter case, LB will be executed when an LMA is overloaded by selecting a multicast session to move to the less loaded one. It can be done thanks to an extension to MLD proxy to support multiple upstream interfaces [167]. In this case, only one proxy instance is deployed at MAG with multiple upstream interfaces being configured towards different LMAs. As a result, the MN can receive the multicast traffic from a less loaded LMA, while obtaining the unicast traffic from its LMA. Further information can be found in [24, 18].

Target LMA Selection Target LMA selection is first based on the channel policy which is defined by the operators (if exist). Otherwise, the LMA selection relies on the following policies (from high to low priority): i) The least loaded LMA among the (not overloaded) LMAs having the multicast forwarding state for this channel should be selected; and ii) The LMA with the lowest load in the domain should be selected. The selection policies come from the fact that if the channel is already available at the selected LMA (target LMA, or tLMA) with a negligible increase of load, the tLMA can forward this channel to the MAG [28]. To do so, a new logical entity, the so-called load balancing controller (LBC), has been introduced. This entity collects and manages the load state information of all LMAs in the domain. It is also responsible for the LMA selection. Upon the location of the LBC, three different schemes can be considered as below:

- Centralized LBC entity: The functionality of the LBC is responsible by a central entity, called C-LBC. This entity is similar to the notion of rfLMA as described in [163]. The LMAs periodically report their current load to the C-LBC by using an extension to the PBA/PBU message with the load information [163]. The C-LBC can be co-located with the AAA server.

- Distributed LBC function on the LMAs: The LBC function is executed in a distributed manner among the LMAs. Each LMA maintains a so-called Load Table which includes load information of all LMAs in the PMIPv6 domain. Each LMA periodically exchanges its load information with each other in the domain, for example, by setting a common multicast group for all LMAs.

- Distributed LBC function on the MAGs: In this case, the load of all LMAs is collected and stored at the MAGs. The MAG can obtain the current load of the associated LMA by using an extension of PBU/PBA messages or an extension of the Heartbeat message with the load information [168].

Without loss of generality, this chapter only considers the first scheme. As all LMAs periodically report their workload to the C-LBC, the frequency of the workload report should be carefully examined as the trade-off between the precision of the load state and the signaling/processing overhead. One possible solution is that the LMA only reports its workload when its load exceeds/is lower than a certain load level.

Multicast Session Selection The multicast session can be selected following some criteria: i) To reduce the potential impact on the ongoing session, the real-time and delay-sensitive session should not be selected. However, if all sessions are the real-time and delay-sensitive ones, the session with the highest data rate should be selected; and ii) The session requiring the highest data rate with the smallest number of subscribed listeners should be selected. It is noted that to better select LMA, the LMA selection algorithm should take the expected load of the selected multicast session into account.

5.3.1 Load Balancing in the Proactive-Multicast Approach

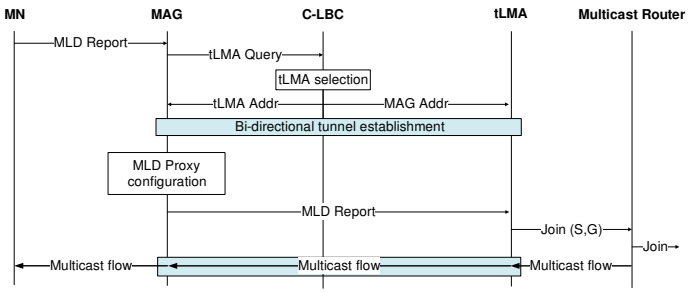


Figure 5.2 – Proactive-multicast approach.

The signaling procedure for the proactive-multicast (MAG-initiated) approach is illustrated in Fig. 5.2. When a registered MN wishes to subscribe to a multicast channel and this channel is available at the current MAG, the MAG will forward it directly to the MN. Otherwise, it will contact the C-LBC to get the address of an LMA (following the criteria as stated earlier), which can be served as the multicast anchor point for this session. After joining the channel via the tLMA, the MAG can receive the multicast packets and forwards them to the MN. Note that the communication between the MAG and the C-LBC can be done by extending the Remote Authentication Dial In User Service (RADIUS) protocol for PMIPv6 [169].

5.3.2 Load Balancing in the Reactive-Multicast Approach

Fig. 5.3 shows the signaling procedure for the reactive-multicast (LMA-initiated) approach. When an LMA (cLMA) is overloaded (its load exceeds a certain threshold), a multicast session will be selected to move from this LMA to a less loaded one (tLMA). After obtaining the tLMA address from the C-LBC, the cLMA sends the tLMA's address and the selected multicast session information to all related MAGs via a load-warning message (e.g., using an extension to the Update Notification message (UNP) [170]). The C-LBC also requests

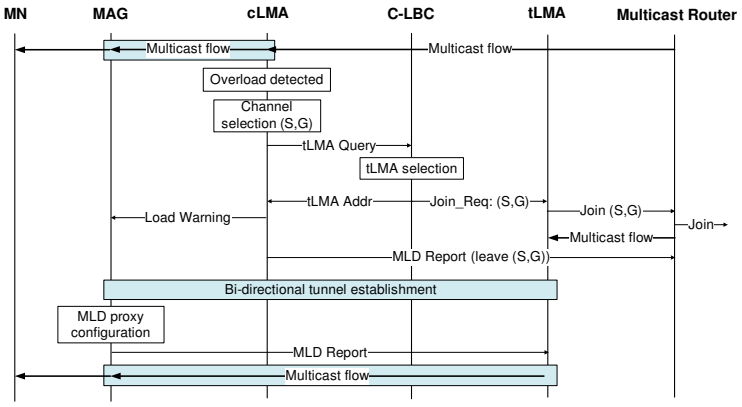


Figure 5.3 – Reactive-multicast approach.

the tLMA to join the channel in advance to reduce the multicast service disruption. The MAG then sends an MLD Report to the tLMA to join the channel. Afterwards, the MAG can receive the multicast packets from the tLMA instead from the cLMA. In the meantime, the cLMA can leave this channel in order to lower its load.

5.3.3 Handover Consideration

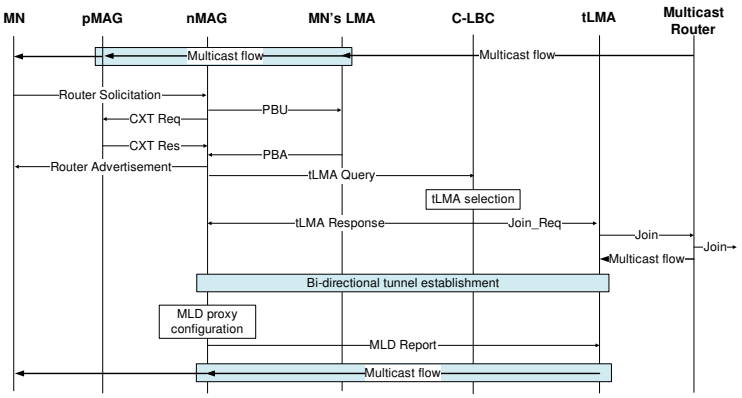


Figure 5.4 – Handover signaling with LB.

As can be seen in Fig. 5.4, if the MN performs a handover between two MAGs, the normal PMIP operation will be executed to update the routing information at the MN's LMA and the new MAG. Then, the similar process as for the new multicast session at the new MAG will be undertaken to select the appropriate LMAs to serve the ongoing multicast channels.

5.4 Performance Analysis

In this section, at first, we will highlight the different load factors imposed on the LMA. Based on that the comparison will be conducted between the reactive-MN and the reactive-multicast approach regarding their efficiency. The multicast service disruption time will also be considered.

5.4.1 Load Analysis

As stated previously, to support multicast in a PMIPv6 domain, the multicast router (MR) function and the MLD proxy function [119] need to be deployed at the LMA and the MAG, respectively. All multicast traffic passes through the MAG-LMA tunnel, accordingly. As such, the load of the LMA comes from two main parts: the load from the typical LMA's tasks (L_{lma}^{lma}) and the load from the MR's tasks (L_{lma}^{mr}). It is noted that a minor amount of load which is imposed by the background processes (e.g., system processes) is ignored in our analysis. Thus, we have

$$L_{lma}^{(.)} = L_{lma}^{lma} + L_{lma}^{mr}. \tag{5.1}$$

As a typical LMA, it performs three main logic functions: mobility routing (processing the unicast traffic from/to the associated MNs), location management (processing PBU/PBA, updating binding cache, maintaining tunnel, etc.) and home network prefix (HNP) allocation [76]. As a result, the L_{lma}^{lma} comes from three main parts L_{lma}^{mor}, L_{lma}^{lm}, and L_{lma}^{hal} corresponding to these logic functions. The L_{lma}^{mor} and L_{lma}^{hal} depend on all the unicast sessions of the registered MNs, and the new MN arrival rate (λ_n), respectively. While L_{lma}^{lm} depends on the number of registered MNs (n) and the new MN arrival rate (λ_n). Hence, they are given by

$$L_{lma}^{mor} = \sum_{i=1}^{n}\sum_{j=1}^{u_i} L_{mn_i}^{j}, \tag{5.2}$$

$$L_{lma}^{hal} = \lambda_n L_{hal}, \tag{5.3}$$

$$L_{lma}^{lm} = (n+\lambda_n) L_{lm}, \tag{5.4}$$

where $L_{mn_i}^{j}$ is the load offered by the unicast flow j of the MN$_i$; L_{lm} and L_{hal} are the unit load generated when the LMA performs the location management and HNP allocation for an MN.

Regarding the multicast router role, the L_{lma}^{mr} can be split into three main contributions corresponding to three functions: packet replication (L_{mr}^{pr}), reverse path forwarding (RPF) recalculation (L_{mr}^{rpf},) and state maintenance function (L_{mr}^{sm}) [28]. The L_{mr}^{pr} is the total load from all the multicast channels which are available at the LMA, and defined as

$$L_{mr}^{pr} = \sum_{i=1}^{m} L_{mc_i}, \tag{5.5}$$

where L_{mc_i} is the load of channel MC_i. Note that the multicast router can replicate the data for multiple outgoing interfaces with almost the same level of load compared to that for one interface (or the unicast traffic with the same characteristics e.g., packet size and data rate) [28].

Let us now consider the different load factors which can be used as the parameters to select the appropriate LMA such as: processor capacity (CPU), number of supported sessions, number of registered MNs, and bandwidth. Accordingly, we assign each factor with a weighting variable which reflects the selected load factors. We then obtain

$$L_{lma}^{(.)} = \alpha\,(n+\lambda_n)\,L_{lm} + \beta\lambda_n L_{hal} + \gamma\sum_{i=1}^{n}\sum_{j=1}^{u_i} L_{mn_i}^{j} + \delta L_{mr}^{rpf} + \theta L_{mr}^{sm} + \rho\sum_{i=1}^{m} L_{mc_i}. \tag{5.6}$$

where $\alpha, \beta, \gamma, \delta, \theta$, and ρ are weighting factors (in the interval [0,1]). For example, if the load is defined as the number of registered MNs, only two factors L_{lma}^{lm} and L_{lma}^{hal} are taken

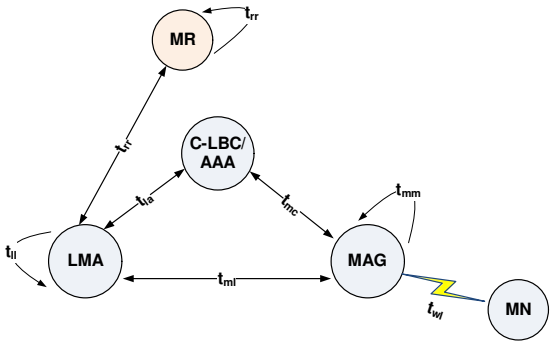


Figure 5.5 – Reference network topology.

into account. In this case, the values of $\gamma, \delta, \theta, \rho$ should be set to 0. LMA load is given as

$$L_{lma}^{(.)} = \alpha\,(n + \lambda_n)\,L_{lm} + \beta\lambda_n L_{hal}. \tag{5.7}$$

As a result, the impact of the number of sessions as well as the session's data rates on the LMA load are ignored. Similarly, if the load is considered as the number of sessions, the L_{lma}^{mor} and L_{mr}^{pr} are taken into consideration, in which the load of each session is identical. Thus, α, β, δ, and θ should be set to 0. Eg. (5.6) becomes

$$L_{lma}^{(.)} = \gamma \sum_{i=1}^{n} \sum_{j=1}^{u_i} L_{mn_i}^{j} + \rho \sum_{i=1}^{m} L_{mc_i}. \tag{5.8}$$

Again, the impact of the session's data rate is ignored. However, it is obvious that a high data rate session puts much more load on the LMA than the low data rate one. Therefore, they cannot be treated equally. In this chapter, we consider the sessions with different characteristics have different impact on the load.
In order to evaluate the load distribution among LMAs in different approaches, we use Jain's Fairness Index [171]. Let L denote the set of LMAs in the domain: $L = \{LMA_1, .., LMA_l\}$, where l is the number of LMAs. According to [171], the fairness index can be computed by

$$FI = \frac{(\sum_{i=1}^{l} L_{lma}^{(i)})^2}{l \cdot \sum_{i=1}^{l} (L_{lma}^{(i)})^2}, \tag{5.9}$$

where $L_{lma}^{(i)}$ is the load of the LMA_i (i=1,..,l). The fairness index ranges from $\frac{1}{l}$ to 1, in which the higher index indicates more fair situation. Ideally, when the load is equally distributed among LMAs, the fairness index is 1.

5.4.2 Multicast Service Disruption Consideration

In the reactive-MN and the reactive-multicast approach, the changing LMA of an MN (listener) may cause the service disruption of the ongoing multicast sessions. The multicast service disruption time is defined as a period when a listener cannot receive the multicast packets. Fig. 5.5 shows a reference topology for performance analysis. The delay factors consisting of the total delay are defined as follows:

- t_{mm}: the delay between two MAGs.
- t_{ml}: the delay between MAG and LMA.
- t_{mc}: the delay between MAG and C-LBC.

- t_{la}: the delay between LMA and AAA/C-LBC.
- t_{ll}: the delay between two LMAs.
- t_{rr}: the delay between two MRs (between LMA and MR).
- t_{wl}: the delay between MAG and listener (MN) (wireless connection).
- t_{join}: the delay time an MR needs to join a multicast channel (including processing time and PIM Join transmission time).
- t_{qrd}: the query response delay which is the interval between the moment when the MN receives an MLD Query and replies with an MLD Report [35].
- t_{cv}: the routing convergence time which reflects the time to update the new anchor location of the selected MN's prefix.

In the reactive-MN approach, as can be seen in Fig. 5.1, the service disruption time (SD) can be calculated from the moment when the cLMA sends a PBU to the tLMA until the moment when the MN receives the first multicast packet from the tLMA. Let d_{join} and $d_{delivery}$ denote the time needed for the tLMA to join and get the first multicast packet for this channel (from a router which already had the multicast forwarding state for this group, namely intersection MR or IMR), respectively. Assuming that n_{mr} is the average number of hops between tLMA and IMR, we have

$$d_{join} = n_{mr} t_{join}, \tag{5.10}$$

$$d_{delivery} = n_{mr} t_{rr}. \tag{5.11}$$

Thus, the service disruption time in the reactive-MN approach is given by

$$SD_{R\_MN} = 2t_{ll} + 3t_{ml} + 3t_{wl} + t_{qrd} + n_{mr} t_{join} + n_{mr} t_{rr} + t_{cv}. \tag{5.12}$$

Via the utilization of the peering function (PF) in the reactive-MN approach, the time needed for the MLD proxy instance at the MAG to obtain the multicast subscription information can be ignored. Consequently, the service disruption can be calculated as

$$SD_{R\_MN\_PF} = 2t_{ll} + 3t_{ml} + t_{wl} + n_{mr} t_{join} + n_{mr} t_{rr} + t_{cv}. \tag{5.13}$$

Similarly, the service disruption time in the reactive-multicast approach is computed from the moment when the cLMA sends a load warning message to the MAG until the moment when the MN receives the multicast traffic (see Fig. 5.3).

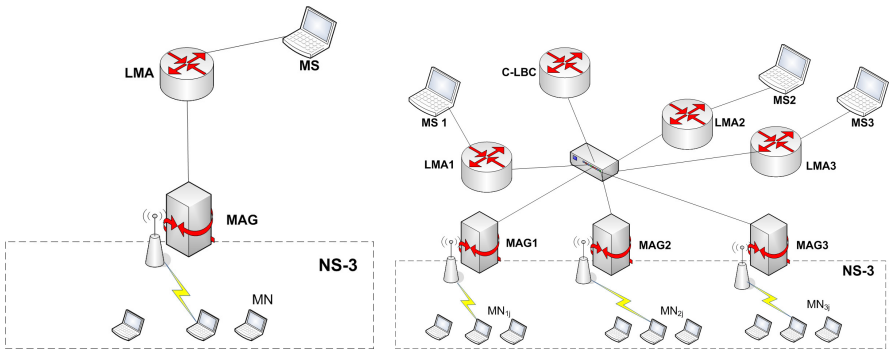
$$SD_{R\_M} = max\{2t_{ml}, n_{mr} t_{join} + n_{mr} t_{rr}\} + t_{ml} + t_{wl}. \tag{5.14}$$

Also, as seen in Fig. 5.4, the service disruption during handover (multicast handover latency) when applying the multicast-based LB mechanism is expressed as

$$\begin{aligned} SD_{HO} = D_{L2} + 2t_{wl} + max\{2t_{ml}, 2t_{mm}\} + t_{mc} \\ + max\{t_{mc} + t_{ml}, t_{la} + n_{mr} t_{join} + n_{mr} t_{rr}\} + t_{ml}. \end{aligned} \tag{5.15}$$

5.5 Experimentation

From the LB perspective, this section will present two separate experiments. At first, we will show in general how the different factors affect the load of an LMA. We will then evaluate the performance of the multicast-based solution in comparison with the MN-based solution and the pure-PMIP environment (without any load balancing mechanism) by using



(a) (b)

Figure 5.6 – Testbeds: (a) Experiment 1, (b) Experiment 2

a near-to-real testbed. It is noted that, at this stage, we only focus on the case where the traffic is dominated by the multicast traffic. In addition, the load is defined as the CPU utilization rate and the performance metric is the load distribution among the LMAs. From the multicast perspective, this section will present the numerical results for the service disruption time analysis given in the previous section.

5.5.1 Experimentation Setup and Scenarios Description

As illustrated in Fig. 5.6, the testbed is deployed as similar as in Chapter 4. The PMIP entities (LMA, MAG) and the multicast sources (MSs) are the virtual machines while the access points (APs) and MNs, which play the role of a multicast listener, are NS-3 nodes. During the experimentation, the LMA load is collected by using a performance measurement tool e.g., *mpstat*[1]. To improve the credibility of the experiment results, the LMA load was collected every one second during 360 seconds in each experiment.
To generate the multicast traffic, several tools can be used e.g., *Iperf* [172] and *MINT* [173] (and *mcfirst*[2]). For example, in case of *Iperf*, the following Linux commands can be used:
Source# Iperf -s -u -B ff08::1 -V -i 1
Listener# Iperf -c ff08::1 -V -u -T 32 -t 100 -i 1 -l 67B -p 12345
In case of using *MINT* and *mcfirst*:
Source# ./mint -s -p 1234 -n 1000 -6 -t 12 ff08::2
Listener# mcfirst -6 -I eth0 ff08::1 1234

5.5.1.1 Impact of Different Load Factors

To show the impact of different factors on the LMA load, the first experiment used a testbed composing of one LMA, one MAG (and one AP), and one MS, as described in Fig. 5.6a. Then two experiment scenarios are defined. The scenario 1 aims at demonstrating the case when the load takes into account only the number of MNs. The number of MNs associated with the LMA will be varied from 1 to 150 (Due to the limitation of the testbed, it can only support upto 150 MNs). The binding registration signaling for these MNs occurred within a small interval (50s) which almost represents the worst case scenario. The scenario 2 shows the impact of unicast/multicast flow with different data rates on the LMA load. Thus, only one MN is required. At first, the MN subscribes to a multicast channel broadcasting by the MS. The LMA load will be measured when the flow's data rate is varied from 100 Kbps to 15 Mbps. Note that a standard definition video streaming typically runs at 3.75

[1]http://linuxcommand.org/man_pages/mpstat1.html
[2]mcfirst command: http://manpages.ubuntu.com/manpages/precise/man1/mcfirst.1.html

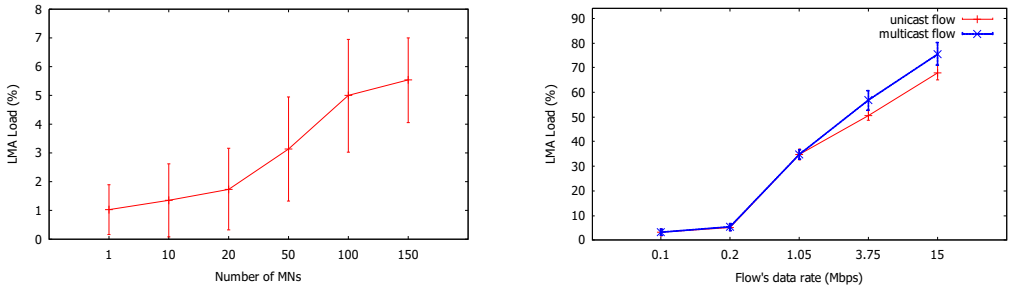
Mbps while the high definition at 15 Mbps [174]. The multicast flow is then replaced by the unicast one with the same data rate. The datagram size in both cases is kept constant at 67 bytes.

5.5.1.2 Evaluation of the Multicast-based LB Mechanism

The second experiment aims at evaluating the performance of the multicast-based solution in comparison with the MN-based and the pure-PMIP environment. At this stage, the experiment focuses on the case where the traffic is dominated by the multicast traffic. The performance evaluation metric is the load distribution among LMAs. This metric is selected since we could not achieve high system performance without fairly and efficiently utilizing the available network resources. The other metrics such as queuing delay and packet dropping probability will be left for future works.
As illustrated in Fig. 5.6b, the testbed is composed of one LBC, three LMAs, three MAGs (and three APs), three MSs, and 18 MNs. The C-LBC functionality is implemented by extending the LMA functionality. At the beginning, each multicast source MS_i (i=1,2,3) broadcasts six multicast channels C_{ij} (j=1,..,6) with identical traffic characteristics (400 Kbps). In the experiment, we use the same threshold value for all LMAs, for example, 85 percent of the CPU utilization rate. At first, the MN_{ij} attaches to the MAG_i and the LMA_i, respectively. The unicast flow is also created between each MN and the corresponding MS (100 Kbps). Two scenarios are then defined to evaluate the proactive-multicast and the reactive-multicast approach.
In the scenario 1, six MN_{1j} (j=1,..,6) join six multicast channels C_{1j} (via LMA_1); MN_{21} joins C_{21} (via LMA_2); MN_{31} and MN_{32} join C_{31}, C_{32} (via LMA_3), respectively. Three approaches are considered: the pure-PMIP, the proactive-MN and the proactive-multicast. In the scenario 2, six MN_{ij} (j=1,..,6) join three multicast channels (say C_{i1}, C_{i2}, C_{i3}) at the LMA_i (i=1,2,3) (two MNs per channel, three channels at each LMA). Then the data rate of the existing multicast sessions as well as the number of sessions are varied to make the LMA load changes. For instance, at the LMA_1 the data rate of the channel C_{11} and C_{12} is increased with 800 Kbps and 1.2 Mbps, respectively. The channel C_{21} (at LMA_2) and the channels C_{31}, C_{32} (at LMA_3) are terminated. The results then are collected when the pure-PMIP, the reactive-multicast and the reactive-MN approach are applied.

5.5.2 Experimental Results

5.5.2.1 Load Factors Measurement



(a) (b)

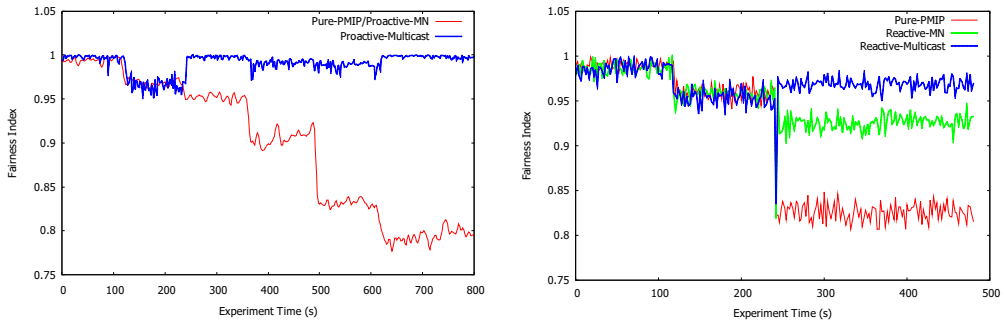
Figure 5.7 – Experiment 1: (a) load .vs number of MNs, (b) unicast .vs multicast flow.

Fig. 5.7a reports the average and standard deviation values of LMA load as a function of

the number of MNs (scenario 1). In this case, the load is calculated according to Eq. (5.7). We also measure the load from background processes: (average, standard deviation) = (1.001%, 0.888%). We can observe that the load slightly increases when the number of MNs increases. Fig. 5.7b illustrates the LMA load when the data rate of the multicast and unicast flow is varied (scenario 2). When the flow's data rate is low, the load imposed by the multicast and unicast flow is almost the same. As the flow rate increases, the load offered by the multicast flow is higher than that by the unicast flow. As the experiment was conducted by using a very limited capacity machine, it requires about 75% load to treat a high definition video flow (15 Mbps). It also could be observed that the load offered from a typical LMA's task with 150 MNs is similar to that from a low rate multicast flow (about 200 Kbps). Thus, it is obvious that the multicast/unicast flow is a crucial factor in terms of load put on the LMA. In other words, in a multicast-dominated domain, moving an MN from the overloaded LMA could not help reduce its load significantly.

5.5.2.2 Evaluation of the Multicast-based Load Balancing Solution

Fig. 5.8a shows the FI value in the scenario 1. At the beginning, the load of all LMAs is almost the same. As a result, the FI value is very close to 1 (indicating that the load is almost shared among the LMAs). From the time the MNs subscribed to the multicast channels (at about 120s), the FI value is decreased rapidly in the pure-PMIP environment since the load is concentrated on the LMA_1. For instance, the LMA_1 becomes overloaded while the LMA_2 and LMA_3 are at low load. Since the LMA assignment is already done for the MNs, the FI value in the pure-PMIP can also be considered as that in the proactive-MN. We observed that the FI value in the multicast-based approach is always greater than that in the other cases. Also, the FI value is close to 1. It demonstrates that the multicast-based approach achieves a better load distribution among the LMAs. The reason is the proactive-multicast approach dynamically assigns the channel to the least loaded LMA at the time when the channel is started.

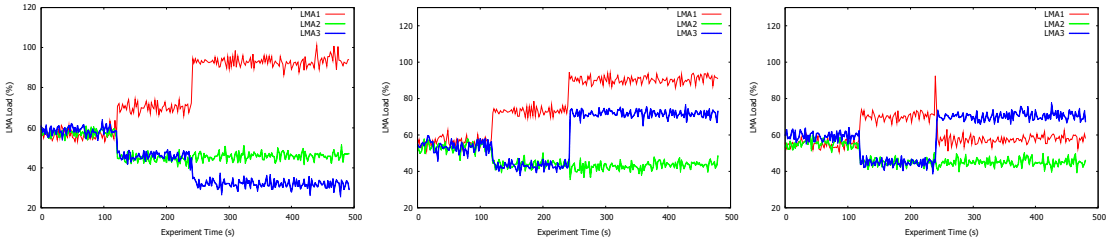


(a) (b)

Figure 5.8 – FI value in the experiment 2: (a) Scenario 1, (b) Scenario 2.

Fig. 5.8b plots the FI value in the scenario 2. At the beginning (from 0 to 120 ms), when each LMA has to serve three identical channels, the LMAs' load is nearly equal. As a result, the FI value in three approaches is almost the same and very close to 1. As the data rate of the existing multicast flow in LMA_1 is increased (C_{11}'s data rate is increased from 400 Kbps to 800 Kbps), LMA_1 load is increased accordingly. Meanwhile, the load of LMA_2 and LMA_3 is decreased (channel C_{21} at LMA_2 and C_{31} at LMA_3 are terminated). Consequently, the FI value is decreased. Since the reactive LB mechanism is only evolved when the LMA load exceeds the threshold value (85%), the FI values in three approaches are kept the same when

the LMAs are running under a heavy load. When LMA_1 is overloaded (at about 240s, as C_{22}'s data rate is increased from 400 Kbps to 1.2 Mbps), the LB mechanism is involved. As a result, the FI value in the reactive-MN and reactive-multicast is clearly greater than that in the pure-PMIP environment. That means the load is better shared between the LMAs. Moreover, the reactive-multicast approach gives a better performance than the MN-based (FI value is greater). In more details, the multicast channel with the highest data rate (C_{12} with 1.2 Mbps) is moved from LMA_1 to LMA_3 in the reactive-multicast approach, while one MN (among two) subscribed to this channel is moved to LMA_3 in the reactive-MN approach. The detail of load distribution of different approaches is plotted in Fig. 5.9.



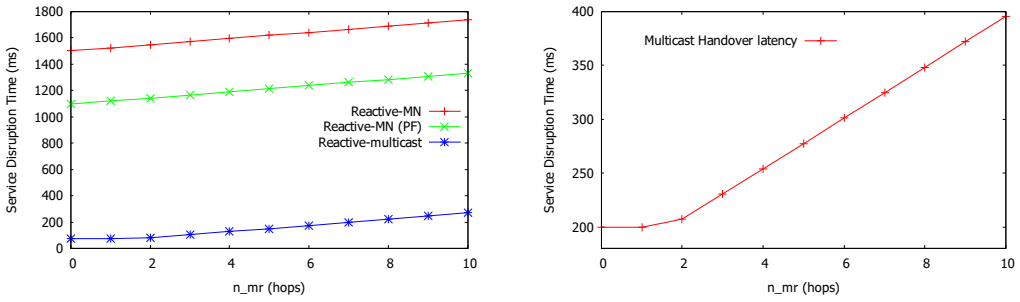
(a) (b) (c)

Figure 5.9 – LMA load in the scenario 2 (experiment 2): (a) pure-PMIP , b) reactive-MN approach, (b) reactive-multicast approach.

The reactive-multicast helps avoid LMA_1 from being overloaded. Meanwhile, the overload status cannot be resolved in the reactive-MN approach (LMA_1 is still overloaded, while LMA_{13} load is greatly increased). As a result, the total load of all LMAs is significantly increased compared to that in the pure-PMIP and reactive-multicast approach. It is due to the fact that the LMA_3 has to join the channel C_{12} while LMA_1 continues forwarding this channel. In this case, more than 31% of the LMA capacity is wasted.

5.5.3 Multicast Service Disruption Time

In this subsection, the following parameter values are used: $t_{mm} = t_{ll} = t_{la} = t_{rr} = 10$ ms, $t_{ml} = t_{mc}$ =20 ms, t_{wl}=15 ms, t_{join} =13.5 ms, $D_{L2} = 50$ ms, and $t_{qrd} = 374.2$ ms. t_{cv} is typically in seconds (for example, the default value in case of OSPF is 10 seconds) [175, 176]. In this subsection, it is set to 1s. The value of n_{mr} is varied over a range [0, 10] hops. It is noted that most parameters used in this evaluation are set to the typical values found in [16] and [177].



(a) (b)

Figure 5.10 – Service disruption time as a function of n_{mr}: (a) caused by LB mechanisms, (b) by handover.

Fig. 5.10a shows the multicast service disruption time as a function of n_{mr}. It appears clearly that the service disruption in the reactive-MN (D_{R_MN} and $D_{R\_MN\_PF}$) is definitely higher than the maximum tolerant interruption time for normal services, as specified in [162] is 500ms. Thus, it causes a noticeable service disruption. On the other hand, the service disruption in the reactive-multicast is kept below the value of 300ms, thus, satisfying the requirements for the real-time services. In other words, the reactive-multicast approach helps greatly reduce the service disruption compared to the reactive-MN solution. Moreover, in the reactive-multicast approach, if there exist the LMA which already had the forwarding state for this channel and is not overloaded, it should be chosen as the tLMA. As a result, it is high probably that the d_{join} and $d_{deliver}$ are ignored. That means in most cases D_{R_M} is 75 ms.
Fig. 5.10b shows the service disruption time during handover as a function of n_{mr}. We could observe that when $n_{mr} < 6$, the handover latency is below the value of 300 ms. Moreover, in most cases the multicast traffic is already available at the tLMA, thus, the service disruption during handover is 200 ms. Consequently, the handover impact on the quality of multicast flow is almost imperceptible.

5.6 Conclusion

As the multicast is expected to be widely used in the future networks, degrading the role of the multicast in the available LB mechanism can cause some issues not only from LB perspective (degradation of efficiency) but also from multicast perspective (tunnel convergence problem and service disruption). To overcome these issues, a multicast-based solution has been proposed. The benefit of the solution is that it does not influence the other ongoing unicast/multicast sessions. It can also co-operate with the existing LB proposals to improve the performance of the network.
Via a near-to-real testbed, the experiment results show that the proposed solution helps better distribute the load imposed by the multicast service among LMAs. Additionally, it helps greatly reduce the multicast service disruption time caused by a changed LMA for LB purpose compared to the existing proposals, even satisfying the service disruption requirement for the real-time services.
However, from the performance analysis and the experiment result, we conclude that none of the two solutions is complete. The multicast-based solution in general works well in the domain where the mobile data traffic is dominated by the multicast traffic; the unicast-based solution, in contrast, works well with the unicast-dominated domain. For instance, the multicast-based solution may be the most convenient for distributing load among the multicast tree mobility anchors (MTMA) which work as a topological anchor point for the multicast traffic in a PMIPv6 domain [178]. It comes from the fact that the MTMA only serves the multicast traffic. As a result, the multicast-based should co-operate with the MN-based solution to enhance the reliability and scalability of the network. For example, the proactive-MN can be applied when an MN enters the PMIPv6 domain, while the proactive-multicast is evolved when a multicast session is initiated. Besides, the reactive-multicast can be followed by the reactive-MN approach. At this stage, if any multicast session is not a real-time and delay sensitive one, the reactive-multicast approach will be performed. Otherwise, the reactive-MN will be executed. The main idea is that we try to distribute load among LMAs by using the multicast-based solution before applying the reactive-MN solution to avoid the influence on the ongoing sessions. Therefore, the blocking probability of a new MN (session) and the dropping probability of the existing MNs (sessions) are obviously lower than the existing LB mechanisms (lower is better).

6
Mobility in Heterogeneous Networks: Electric Vehicle Charging Service Use-Case

In this chapter, the mobility in heterogeneous networks will be illustrated via a use case: Electric Vehicle Charging Service (EVCS). There are several reasons for selecting this use case. Firstly, the electric vehicle (EV) is a promising choice for personal transportation in the near future. Secondly, the idea of connecting vehicles is gaining momentum. In addition, a mobile node, an EV in this context, can be connected with the infrastructure via different wireless/wired technologies in different steps (LTE while driving, WLAN while approaching a charging infrastructure, PLC while being docked at a charging infrastructure). Thus, considering multicast in the EV is one step to enable the entertainment system in the EV, which is becoming more and more popular. Moreover, IP multicast can also be used to update the software of the in-vehicle systems.
According to Cisco Internet Business Solutions Group (IBSG) [179], connecting vehicles creates such significant benefits as traffic safety, environmental eco-friendly, easing traffic congestion, and enhancing driver/passenger experience (in-vehicle infotainment systems). Four key capabilities in the connected vehicle are connection within the car, connection to personal devices, connection *around* the car and connection to the cloud (or infrastructure). These capabilities make a vehicle as a *personal digital assistant on wheels* [180] keeping peoples connected to the Internet of Things. Thus, they make our travel experience safer and more convenient as well as enhance the in-vehicle experience [180]. In line with this trend, the EVCS gains the benefits of connecting vehicles to provide a smart charging service from both user and electricity operator perspective.

6.1 Introduction

The number of vehicles in use is set to increase exponentially in recent years (1.015 billion in 2010 [181]). This trend causes some serious issues regarding energy sources like increasing in fuel demand and costs [182], environmental concerns [183] and air quality. On one hand, it encourages the production and use of clean and efficient energy vehicles in which the electric vehicles (including full electric and plug-in hybrid electric vehicles, in common, EVs) belong to. On the other hand, the evolution of battery technology allows increasing the battery capacity while decreasing the weight/size of battery pack and reducing the costs. This context makes the EV a promising choice particularly for individual mobility in the cities.

In order to gain the customer acceptance of the EV, the charging infrastructure needs to be deployed at least as numerous and widespread as the fueling stations. Yet, unlike the fueling station, the various available charging strategies requires unprecedented interactions between drivers and the Grid operators. Secondly, the type of charging stations will range from the commercial stations to the single plugs operated in parking lots or in residential areas. Altogether, this will lead to a segmentation of Electric Vehicle Charging Services (EVCS), with a complex tracing of charging contexts and payment, which would make the charging process difficult and charging capacity/need unforecastable for Grid operators, adding anxiety to users and Grid operators. One solution to mitigate such situation is to make heterogeneous charging strategies and stations, as well as and the natural mobility of EVs transparent to the EVCS.
As stated in [184], the critical requirement to get energical and economical benefits from Smart-grid and EVs is to reach an optimal scheduling of charging EVs and storing electricity by EV. Uncoordinated burst of EV charging may cause a huge energy demand that can result in the electrical grid congestion, while storing electricity by EVs may be inefficient if required immediately elsewhere. Thus, it is important for Grid operators to monitor the necessary data (like energy consumption and demand) and to assign and route vehicles to the appropriate charging stations supporting their required charging policies. Such negotiation cannot be conducted at the charging station but must be conducted while driving. The EV therefore needs to communicate with the charging infrastructure [185]. In this context, several access technologies (e.g., WLAN, LTE and Power Line Communication (PLC) [186][187]) must be used at different phases of the EVCS, such as LTE while driving, WLAN while approaching a charging station, and PLC while being docked at a charging station. Such heterogeneous communication technologies should be transparent to the user, the Grid operator and to the EVCS in order to maintain the service context.
In this chapter, we propose an EVCS solution from both user and Grid operator point of view. For the user, it provides a ubiquitous and transparent charging service at different scenarios (at home, at a charging station and at a parking), making charging an EV as simple as possible. It also helps the Grid operator to efficiently manage the user consumption/demand to control the load on the grid especially when a large number of EVs is considered. From the centralized nature of Smart-grid services, a network-based IP mobility management solution, Proxy Mobile IPv6 (PMIPv6) [76], is most appropriate to federate segmented charging services and make the charging experience transparent to EVs mobility as well as the communication technology used by each phase of the EVCS. By using PMIPv6, the service takes care of the EV mobility, handling vertical and horizontal handovers between different communication technologies (e.g., WLAN, LTE and PLC). Yet, IPv6 address preservation in PMIPv6 remains an issue in such context, and we provide a solution by relying on a logical interface approach to hide the change of interface to the IPv6 stack. Finally, we will validate the EVCS concept and the performance of PMIPv6 for the EVCS against benchmark from IEEE 1646. The mobile multicast in heterogeneous networks is also taken into consideration. A near-to-real testbed, which is a combination of real and virtual machines, has been deployed to reduce the hardware cost and to provide more flexible experiment. A real PLC connection provided by partners from the VELCRI project is used to obtain realistic results.

In the context of this thesis, this chapter discusses the mobility of the nodes in heterogeneous networks, mainly from a mobile node point of view. In other words, the MN will move in a PMIPv6 domain using different access technologies e.g., WLAN, LTE and PLC. Thus, both vertical and horizontal handover will be considered. A vertical handover is executed when the mobile node changes the type of technology it uses to access the network, while a

horizontal handover is performed between two layer 3 point of attachment using the same technology. Also, IP multicast will be taken into account. From a mobile node point of view, to obtain the same IPv6 address when switching between different interfaces, logical interface mechanism is used. Moreover, it helps to hide the changing of the interfaces from multicast application point of view. Also, the IEEE, through its 802.21 work group[1], has developed a standard that allows a MN to seamlessly roam across different types of 802 network access technologies e.g., WLAN, WiMAX and LTE. The solution based on the Media Independent Handover (MIH) Services has been deployed in the Medieval project [188]. Thus, we do not mention MIH-based solution in this chapter.
The structure of this chapter is as follows. Section 6.2 describes a solution for EVCS regarding different charging use cases, design principles, and operations. Section 6.3 briefly introduces PMIPv6 in the context of EVCS and considers multicast in the context of EVCS and heterogeneous networks. While section 6.4 describes the testbed, experiment scenarios and the experiment results. Finally, conclusions are presented in the last section.

6.2 Electric Vehicle Charging Service

In this section, starting from the deployment scenarios for EVCS, the usage scenarios, the design principles as well as the operations of the EVCS are briefly provided. Further discussions on EVCS can be found in [17, 189]. This section also makes an early highlight on the reasons why PMIPv6 is a good choice in the context of EVCS.

6.2.1 Electric Vehicle Charging Deployment

In the context of VELCRI project, there are three types of charging strategies, namely standard, rapid and ultra-rapid. The standard charge may take from 4 to 8 hours to provide a full charge upon the initial state of battery, while the rapid and the ultra-rapid charge need about 30 minutes and 5 minutes, respectively. The location of the charging pods may vary, however, three typical places with the corresponding characteristics are considered:

- Charge at home: long charging time at low power;
- Charge at a station: short charging time related to average fueling time; requires a high peak power level, which limits the simultaneously charging pods at stations;
- Charge at a parking: charging time related to the time spent in the parking, reduced peak power but large amount of charging pods, which requires flexible charge scheduling.

From the characteristics of different types of charge and locations, Table. 6.1 shows the possible deployment scenarios of charging system. It is worth noting that the scenarios marked *possible* are not considered in this chapter.

Table 6.1 – Charging System Deployment: Type and Location

Charge Type \ Location	**Home**	**Station**	**Parking**
Standard charge	√	-	(possible)
Rapid charge	-	(possible)	√
Ultra-rapid charge	-	√	(possible)

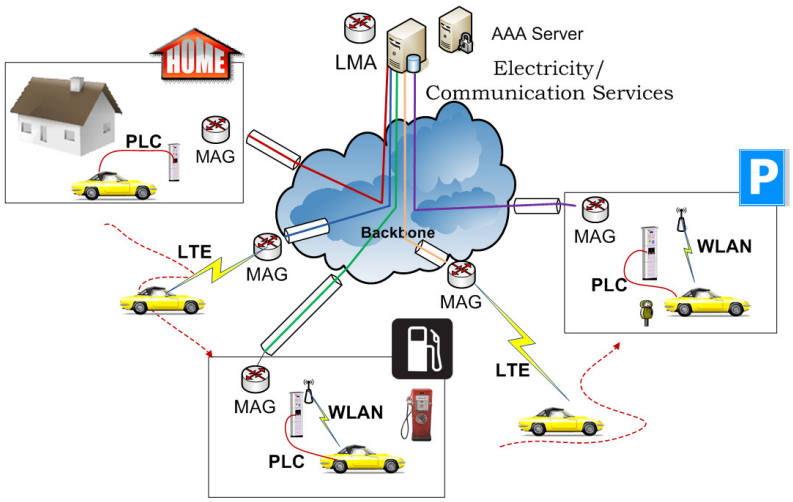


Figure 6.1 – General use cases of EVCS.

6.2.2 General Use Cases for Electric Vehicle Charging Service

Based on the charging deployment scenario, four general use cases for the EVCS are considered (see Fig. 6.1): (a) charging at home, (b) charging at a station, (c) charging at a parking, and (d) moving between the stations/parkings.

Charging at Home The network at home can be considered as home network of the EV. The EV is typically charged in the evening (period of high energy demands and high cost) when the EV owners return home. Thus, the EV needs to be charged intelligently. It can be done thanks to the intelligent charging management which is responsible for the automatic charge/discharge of the EV in order to lower cost and effectively control/optimize the load on the grid.

Charging at a Station The EV, at first, communicates with the infrastructures via the wireless access technologies e.g., WLAN and LTE to assign and route vehicles to the appropriate stations. At the station, the EV will be plugged into an electrical outlet (using PLC connection) to charge. A vertical handover between WLAN/LTE and PLC will be performed that allows the EV to continue communicating with the charging station. Again, the charging process will be taken care by the intelligent charging management. The EV can also use additional services during the charging process. After the charging is done, the EV may receive a bill including the charging-related information (time and cost), the EV profile and operator's information.

Charging at a Parking The steps prior to parking are similar to those in the previous case (charging at a station). The charging schedule can also be negotiated. Because of the difference between station and parking, localized service can be provided to route vehicles to the appropriate charger.

Moving between the Parkings In some cases, the charging process is interrupted. The context related to this EV will be stored at a database. After connecting to another parking, the EV can make an attempt to keep the same negotiation or fall back to a renegotiation

[1]IEEE 802.21 Working Group, http://www.ieee802.org/21/index.html

in case the parking fails to support the requirements. In the first case, the context will be restored (preservation of the context) at the current parking.

6.2.3 Design Principles

To deal with different usage scenarios of EVCS, we proposed a solution guided by a set of design principles as follows:

- Transparency: transparent mobility of the user to the service. It allows EVs to use the charging system as similar as at home (e.g., context preservation and under only one contract);
- Pre-negotiation: negotiation with the charging infrastructure before deciding to go to a specific station/parking to charge (pre-negotiation);
- (Intelligent) Charging management: cost minimizing (for user) while maximizing system reliability and stability (for Grid operator);

Moreover, the EVCS should provide an easy-to-use service and secured transactions (from user perspective), as well as an effective way to manage the user information (energy demand, consumption, and location) to better control the load on the grid (from Grid operator perspective).
Therefore, the charging service can be divided into the basic modules which are mapped to the design principles as described in Fig. 6.2.

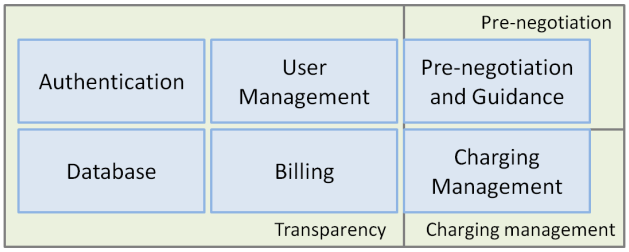


Figure 6.2 – EVCS modules reflect the design principles.

6.2.4 EVCS: Operations and Functionalities

Following its design principles, the EVCS is proposed with the main operations as briefly described as follows (further information can be found at [189]):

Session initiation (via WLAN/LTE/PLC) It is executed when an EV is connected to the charging infrastructure for authenticating/authorizing and obtaining the EV profile (context establishment). PLC is used for the session initiation only in case of charging at home.

Session negotiation and guidance (via WLAN/LTE) This operation allows the EV to negotiate with one or multiple charging infrastructures to find the most appropriate one based on such metrics as charging time, cost (for user), charging type, required capacity and slots availability (for Grid operator). It is noted that this step is executed before reaching a charging station/parking thanks to the wireless access technology (WLAN/LTE). Also, additional information of the station/parking can be provided like discounts and bonuses.

Charging management (via PLC) Charging process does not start as soon as the EV is plugged, but is rather scheduled according to the capacity of the grid and the demand of the user established during the negotiation phase. Accordingly, an intelligent charging management unit coordinates the charging process on bi-directional communication link between the infrastructure and the EV while being plugged. In other words, the EV can be charged when the demand is low, otherwise it can be considered as a distributed energy source when the demand is high.

Session termination (Billing, via WLAN/LTE/PLC) When a session is terminated, electricity used or sold as well as related statistics (price, charging time and charging type, etc.) will be logged to the service provider and the cost charged on the user account as if the user was at home.

6.3 PMIPv6 for Electric Vehicle Charging Service

In the context of EVCS, since an EV can be charged at different places as similar as at home, PMIPv6 is a good choice. It is because it makes heterogeneous communication technologies transparent to the EVCS and hides the mobility of the EVs to the service.

As we can see in Fig. 6.1, using PMIPv6 offers some benefits in the context of EVCS: (1) Network-based mobility management and Address preservation: The MAG where the EV is currently connected simulates the EV's home network. Therefore, the EV uses the same IPv6 address when moving in a PMIPv6 domain. So, the EV is not aware of the mobility; (2) Context preservation: This feature facilitates the charging process of the EV in case of mobility; (3) Location management; (4) Easy-to-integrate with Authentication, Authorization and Accounting (AAA) mechanism; and (5) EV-Grid interaction: The PMIP messages can be extended for collecting the EV-related information. Thanks to the advantages of PMIPv6, the energy and utility suppliers can provide an easy way but flexible to access their services.

Although PMIPv6 can bring benefits to the EVCS, it has several limitations. Thus, improvements are needed to make PMIPv6 suitable for the EVCS.

Handover across heterogeneous access technologies (WLAN, LTE and PLC) - IPv6 Address Preservation Considering handover across different access technologies (vertical handover), there are several mechanisms which allow the EV to obtain the same IPv6 address after handover. The first one is based on the auto-configuration mechanism by using a common identification for both PLC and WLAN interface (like Network Access Identifier). The second one uses the Dynamic Host Configuration Protocol (DHCP) mechanism in which two interfaces must be set with the same client identifier. However, the major limitation of these two approaches is that two interfaces cannot be active at the same time. As the result, it may cause a significant service disruption and packet loss.

The third mechanism uses the logical interface technique [190] which allows to hide the different access technologies (e.g., using Linux bridge mechanism). Thus, the changing of interface is transparent to the IP stack. Moreover, two interfaces can be active at the same time. For this reason, this mechanism is more suitable than the others to facilitate the vertical handover in terms of handover latency. Note that in the context of electric vehicle, with a huge power, the impact of power consumption caused by turning on both of the interfaces is negligible.

Context Preservation To support the context preservation characteristic, the MN's context needs to be stored in a database/policy profile. One possible solution is that the AAA server is extended to store this type of information.

6.3.1 Multicast Considerations

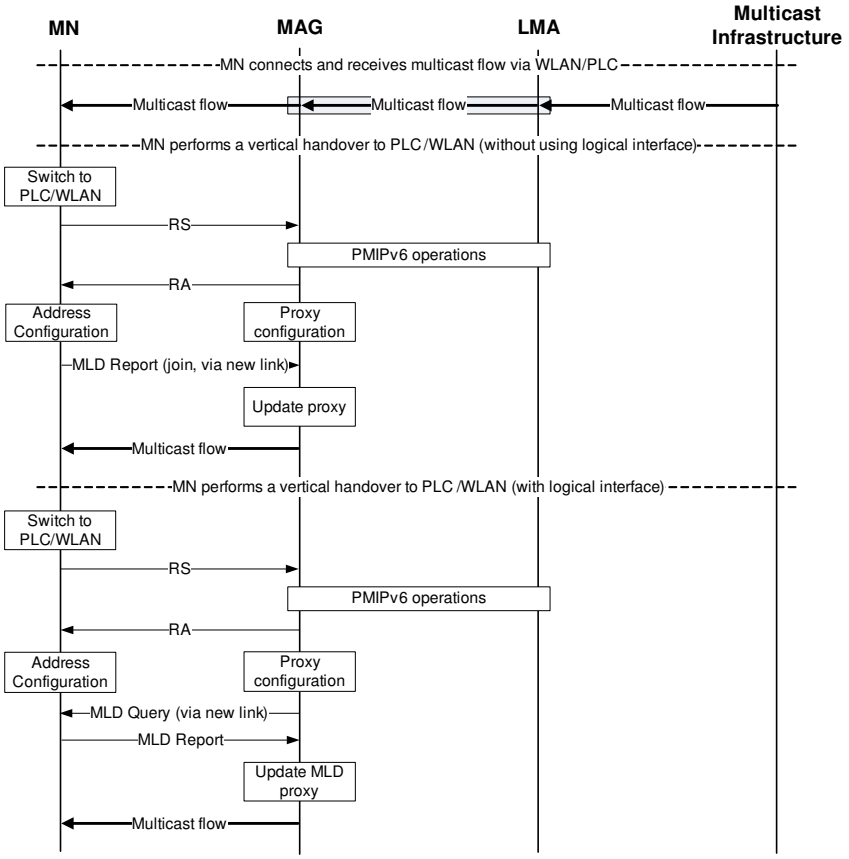


Figure 6.3 – Handover signaling regarding multicast.

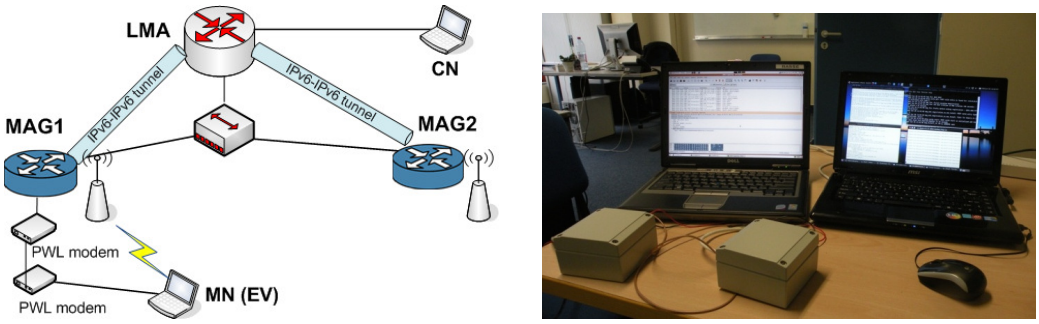
When an MN (a listener) performs a vertical handover between two interfaces while connecting to the same MAG, the normal PMIPv6 will be executed to allocate a HNP for the new interface. Depending on the PMIPv6 implementation, the MN can obtain the same HNP as for the previous interface or a new HNP. It then configures its IPv6 address based on the prefix allocated. As a normal proxy operation, the MLD proxy at MAG will add the MN to a downstream interface. Moreover, from a listener point of view, the listener should join the on-going multicast flows at the new interface. Thus, the requirement in terms of mobility transparency cannot be guaranteed. Thanks to the logical interface mechanism, the listener does not need to re-join the on-going flows, since the logical interface has already joined them. As a result, the listener is unaware of mobility from the multicast service point of view (see Fig. 6.3). However, even with logical interface, if the on-going flows are not present at this downstream interface, the MN has to wait to receive an MLD Query message to express its active multicast flows by mean of MLD Current State. As stated in the previous section, it may experience a noticeable service disruption (see Fig. 6.3). Thus, the MAG will inform the MLD proxy so that the proxy can update its membership state to

forward the on-going multicast flows in the new downstream interface as soon as possible. It can be considered as an extension to MLD proxy. In case of a vertical handover between two different MAGs, the context transfer is needed to reduce the service disruption time as discussed in Chapter 4. Again, by applying the logical interface mechanism, the mobility is transparent to the listener.
When the MN performs a horizontal handover between two MAGs, similarly, the context transfer between these MAGs is required in order to avoid a large service disruption and packet loss. Further information on the handover signaling and operation can be found in Chapter 4.

6.4 Experimentation

6.4.1 Experimentation Setup and Scenarios Description

In order to validate the proposed solution, a near-to-real testbed has been deployed. In this section, the testbed and the experiment scenarios are presented.



(a) (b)

Figure 6.4 – Testbed: a) architecture; b) actual image.

Description of the Testbed The testbed, as indicated in Fig. 6.4a, is composed of one LMA, two MAGs, one CN and one MN playing the role of an EV. It is noted that the CN represents an entity in the Smart Grid. The testbed is based on the User-mode Linux (UML) to create the virtual machines. The LMA, the MAGs and the CN are the virtual machines (UML) running on a host machine. Another real machine is used as an EV that connects with the MAG via a WLAN or a PLC connection. To connect the virtual machines, the virtual Ethernet connection is simulated by using a combination of Linux Bridge and TAP interface (for more details, see Chapter 3). In case of PLC connection, two PLC modems are connected via coaxial cable and to the MN and to the MAG, respectively. Thanks to VELCRI project, a real PLC connection is used in the testbed. The PMIP functionality and multicast support can be deployed similar to in the Chapter 4. The actual image of the testbed is described in Fig. 6.4b. In addition, the mapping between the actual image and the logical components of the testbed is illustrated in Fig. 6.5.
During the experiments, a network analyzer tool (e.g., Wireshark) is used to capture the packets exchanged between the entities while a network testing tool (like Iperf) to measure the throughput of WLAN/PLC connection. The Ping application plays the role of a simple service running on EV and CN. When considering multicast, the CN also plays the role of a multicast source broadcasting a multicast flow which is subscribed by the EV (playing the role of a listener).

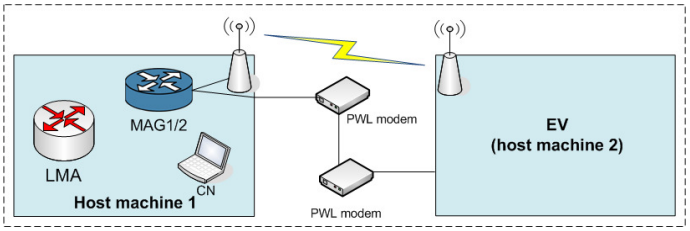


Figure 6.5 – Mapping between the actual image and the testbed components.

Logical Interface Mechanism in Linux Logical interface mechanism is applied on the MN using the bridge-utils (bridging)[2] and TUN/TAP device for Linux systems as specified in Fig. 6.6. The TAP device works at the Ethernet frame level while the TUN device acts as a network layer device. We then use the *ebtables* tool[3](or *iptables*[4]), which is a filtering tool for a Linux-based bridging firewall, to switch between the interfaces.

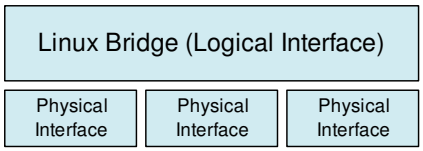


Figure 6.6 – Logical interface mechanism under Linux.

Experiment Scenarios We define four experiment scenarios based on the use cases given in the previous section as follows:

- Scenario 1: Authentication and context establishment. This scenario aims at demonstrating that PMIPv6 can work correctly with PLC.
- Scenario 2: Vertical handover between WLAN and PLC at one MAG. This scenario describes the transition between the negotiation, the charging management and the termination step.
- Scenario 3: (Horizontal) Handover/roaming between two MAGs. From the EVCS point of view, this scenario represents the mobility of the EV between the parkings. It is noted that the horizontal handover in some cases can be replaced by successive vertical/horizontal handovers. Without loss of generality, only a horizontal handover using WLAN is considered.
- Scenario 4: Multicast considerations in the scenario 2 and 3. In this case, the CN plays the role of a multicast source broadcasting a multicast flow while the EV plays the role of a multicast listener. Further information about how to generate the multicast traffic in this testbed can be found in Chapter 5. In case of handover between two MAGs, the multicast context transfer and the explicit tracking functions are enabled at MAG to reduce the service disruption time as similar in Chapter 4.

6.4.2 Experiment Results and Discussions

At this step, the experiment focuses on the validation of the concept of EVCS, the performance of PMIPv6 for the future EVCS as well as multicast mobility with heterogeneous

[2]Linux Bridge: http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge
[3]ebtables – Linux Ethernet bridge firewalling: http://ebtables.sourceforge.net
[4]iptables: http://ipset.netfilter.org/iptables.man.html

communication technologies e.g., WLAN, LTE and PLC. Thus, two evaluation metrics are concentrated, i.e., PMIP functionality and performance metrics which are translated into the corresponding EVCS ones. The first metric aims at validating the functionality of the EVCS regarding the authentication, the context establishment, the address preservation and the service continuity in case of handover. The second metric takes into account the response time (Round-Trip Time (RTT) between the EV and the CN), handover latency, throughput and packet loss in case of unicast traffic; while handover latency, packet loss in case of multicast traffic. From the EVCS point of view, the response time is the time needed for exchanging information between EV and charging infrastructure (stations and Smart Grid) for controlling and monitoring purpose. Handover latency is translated into the time needed to acquisition of the context (IPv6 address) when switching between the operations (negotiation/charging management/termination) in the scenario 2 and when performing handover/roaming between stations in the scenario 3. From multicast service point of view, the multicast service disruption time and packet loss are considered metrics.

Functionality Metric When an EV was connected to a MAG via the PLC connection, the regular PMIPv6 procedures were executed (performing AAA procedures, exchanging PBU/PBA messages, updating binding state at LMA/MAG) to allocate a HNP (2001:100:7777::/64) to the EV. Based on this HNP, the EV configured its IPv6 address (2001:100:7777:021f:3cff:fe59:95a4/64) and used this address to communicate with the CN (scenario 1).
When the EV performed a vertical and a horizontal handover, the EV got the same prefix and kept using the same IPv6 address. By analyzing the packet exchanged between the entities, we can observe that after handover, the EV/CN continues to receive the Echo Request/Reply messages from the CN/EV. From the service point of view, that means the service continues to run after handover.

Performance Metric The average RTT between the EV and the CN via WLAN connection is 1.98ms (standard deviation (σ) = 1.47) while via PLC is 3.34ms (σ = 0.47). Thus, the values satisfy the timing requirement for monitoring and control information by IEEE 1646 (16ms) [191]. We can see that although the average RTT in case of WLAN is smaller than that of PLC, the standard deviation in case of WLAN is much higher than the case of PLC. That means the PLC, as a wired link, can provide more reliable connection than the WLAN. Concerning the throughput, it is about 4.6Mpbs by using PLC. This value is adequate for the normal traffic services.
Regarding handover latency in the scenario 2, since the PLC and WLAN interfaces are activated at the same time, the handover delay is slightly increased compared to the time needed to update the EV location (between the RS and RA message). This value in the experiment is 30ms (σ = 10.7) for the handover from PLC to WLAN and 42ms (σ=12.4) for the handover from WLAN to PLC. In both cases, there is no packet loss.
In the scenario 3, handover latency is about 2030ms (σ = 229.1). This value is much greater than that in the scenario 2. It is due to the time needed to change the mapping of the WLAN interface of the real machine 1 from MAG1 to MAG2 and the time for the tunnel establishment between MAG2 and LMA. This duration in our experiment is quite large (1977ms and σ = 242.4).
Based on the handover latency, a threshold value can be defined (e.g., 500 ms) to help the system make an appropriate behavior. For instance, if the handover latency is less than the threshold value, it can be considered as a vertical handover between two interfaces at the same MAG (scenario 2). Vice versa, it can be considered as a handover between MAGs. In

the latter case, the session information needs to be stored into the profile server. Yet, some experiments are required to select the most appropriate threshold value.

Multicast Considerations When the EV performs a vertical handover from PLC to WLAN at one MAG, the multicast service disruption duration is 53.2ms (σ = 23.4). In case of handover from WLAN to PLC, the multicast service disruption time is 70.4ms (σ = 21.3). This time consists of the time needed for the typical PMIPv6 operations, the MLD proxy update time and the time for the first multicast packet reaches the MN after handover.
Similarly, the multicast service disruption time in case of horizontal handover between MAG1 and MAG2 using WLAN is 2038.2ms (σ = 332.3). Again, this value is high since the time needed for the switching interface process between MAG1 and MAG2 is large. In this context, we focus on the duration, which mainly consists of the time for the layer 2 handover, the typical PMIPv6 operations, and the multicast-related procedures, which is 176.3ms (σ = 63.2). With this value, the handover impact on the quality of multicast stream is almost imperceptible.

6.5 Conclusion

Using EVCS as a use-case, this chapter discusses the mobility in heterogeneous networks. The consideration of EV's mobility as well as IP multicast in heterogeneous network can be seen as a step towards the era of connecting vehicles. From the EVCS point of view, this chapter proposes a solution taking into account different use case scenarios. A centralized IP mobility management solution, PMIPv6, is used to deal with the natural mobility characteristics of the EV. PMIPv6 can facilitate the usage of charging service by keeping the mobility transparent to the user and the Grid operator. Moreover, from a Grid operator perspective PMIPv6 helps to effectively manage a huge number of EVs and to collect the required information of the EV for the Vehicle-to-Grid (V2G) and Grid-to-Vehicle (G2V) purpose. From the multicast service point of view, this chapter investigates the mobility of a listener in heterogeneous networks. Different access technologies are considered as WLAN, LTE and PLC. Both vertical and horizontal handover are taken into consideration. The logical interface mechanism helps to hide the handover between different interfaces as well as to avoid packet loss. Also, the listener remains unaware of mobility from the multicast application point of view, thanks to this mechanism.
A testbed has been deployed based on the virtual mechanism that allows achieving the near-to-real results at a low cost. In addition, a real PLC connection is used in the experimentation to obtain the realistic results. At this step, from service perspective, the experiment results validated the solution in terms of functionality as well as performance.
As future work, the EVCS modules will be developed. The (complete) service then will be evaluated in terms of its operations, functionality and performance with different use case scenarios. In addition, we will study the benefits of EVCS in a DMM environment.

Conclusion of Part II

In Part II of this thesis, we have discussed different aspects of multicast mobility in a PMIPv6 domain and proposed the corresponding solutions. Starting with a basic issue - service disruption, this Part then considered the multicast mobility-related issues in the heterogeneous network as well as the scalability issue from a load-balancing point of view.

Chapter 4 has focused on the service disruption caused by the movement of a listener in a PMIPv6 domain. A simple but effective solution has been proposed to mitigate the service disruption and the handover latency. This solution is based on the combination of the multicast context transfer and explicit tracking function. We have presented a near-to-real testbed for the multicast mobility which allows simulating the movement of multiple sources and listeners at the same time. Also, a real implementation of both PMIPv6 and the multicast-related components (MLD proxy, multicast context transfer and explicit tracking function) have been developed. A listener part of MLDv2 was also implemented in NS-3.

Chapter 5 discusses the scalability issue raised when considering a large number of mobile nodes and their traffic demand. From the fact that multicast is the main service of the future internet, the multicast service should play a crucial factor in putting load on the LMA. The consideration of multicast in the existing LB mechanisms can lead to several issues from both LB (efficiency degradation) and multicast service perspective (e.g., tunnel convergence problem and service disruption). Thus, a LB among LMAs taking multicast into account was proposed. The proposed solution helps better distribute the load among the LMAs in runtime, thus, improving the efficiency of resource utilization. Moreover, the proposed solution does not influence the ongoing unicast/multicast sessions (except the selected session with which the multicast service disruption, in most cases, satisfies the requirements for the real-time services [162]). Our solution can co-operate with the existing ones to improve the performance of the system. This chapter also showed an example of the performance of the near-to-real testbed when considering the real traffic.

Chapter 6, via analyzing a use case of electric vehicle charging services, has discussed the issues as well as proposed solution for a node moving in heterogeneous networks. In the context of EVCS, a mobile node (an EV), can be connected with the infrastructure via different wireless/wired technologies in different steps: LTE while driving, WLAN while approaching a charging infrastructure, and PLC while being docked at a charging infrastructure. Thus, both vertical and horizontal handovers between different access technologies have been considered. The logical interface has been used to hide the different access technology to the IP and the application layer.

In the next Part, we will consider the inter-domain mobility as a step towards DMM before investigating solution for DMM environment.

Part III

IP Multicast Mobility in DMM

Overview of Part III

In this Part, we will first propose an inter-domain mobility for PMIPv6 based on DMM concept. The inter-domain PMIPv6 can be considered as one step towards DMM. The multicast mobility support then will be considered in both the inter-domain and DMM environments.

In Chapter 7, a solution for inter-domain mobility for PMIPv6 will be presented. As DMM is still under discussion, and has not been standardized, it will not be deployed soon. In addition, since PMIP is widely accepted, inter-domain PMIPv6 which is based on DMM concept can be considered as a step towards a *pure DMM* deployment. The proposed solution allows the data packets to be routed via a near-optimal way by bringing the mobility anchors closer to the MN while the control management can be placed anywhere in the network. A basic support for the multicast listener mobility in an inter-domain environment then will be provided.

In Chapter 8, a dynamic multicast mobility anchor selection will be proposed in DMM. It enables a per-flow multicast support. From a multicast service perspective, it helps satisfy the strict requirements in terms of service disruption and delay. Additionally, the packet duplication as well as waste of resources (or leave latency) issues can be reduced. It also provides a mechanism to better distribute the load among the MARs.

7
Inter-domain Mobility for PMIPv6: From the DMM's Perspective

7.1 Introduction

Recently, Proxy Mobile IPv6 (PMIPv6) [76] has been standardized by the IETF, and widely adopted in 3GPP and WiMAX architecture. Taking advantage of the network-based mobility management, PMIPv6 enables IP mobility for moving hosts without their involvement. PMIPv6 brings several benefits compared to the host-based mobility management (e.g., MIPv6 [70]) (see Chapter 2). However, PMIPv6 fails to support the inter-domain mobility. That means, even when an MN moves to another PMIPv6 domain, session continuity cannot be maintained.

In order to support the inter-domain mobility, several solutions have been proposed e.g., integration of MIPv6 and PMIPv6 (H-PMIP) [192]; and I-PMIP [193]. Yet, they have limitations such as sub-optimal routing, signaling overhead and handover latency. Especially, due to the lack of granularity on the mobility management service, the mobility service is always provided even for the sessions that do not require mobility management support e.g., the sessions launch and complete while the mobile node connected to the same domain.

In this chapter, we propose inter-domain mobility solutions for PMIPv6 (called D-PMIP) based on the DMM concept. Following the DMM requirement (REQ4) in terms of reusing/extending the existing IETF IP mobility protocols (i.e., MIPv6 and PMIPv6), the proposed solutions apply the DMM concept into the existing PMIPv6 networks to support inter-domain mobility. The solutions may be fully or partially distributed. Thus, they allow data packets to be routed via a near-optimal way by bringing the mobility anchors closer to the MN while the control management can be placed anywhere in the network. The numerical results show that the partially distributed solution (DP-PMIP) gives better performance than the existing inter-domain handover solutions e.g., MIPv6, H-PMIP and I-PMIP in terms of handover latency, signaling cost and tunnel usage.

The rest of this chapter is organized as follows. Section 7.2 describes related work on the inter-domain mobility support. In section 7.3, the two different proposals are presented with respect to its architecture and operations. We also present a basic support for the multicast listener mobility in the proposed solution. Section 7.4 provides performance analysis in terms of signaling cost, handover latency and tunnel usage. Section 7.5 shows the numerical results taking into account the impact of different factors. Eventually, Section 7.6 concludes this chapter.

7.2 Inter-domain Mobility Support

Several solutions have been proposed for inter-domain mobility support for PMIPv6. The common idea is using a global mobility anchor to keep the MN reachable when it moves to a visited PMIPv6 domain. In [192], the authors introduce a scenario in which PMIPv6 is used as an intra-domain mobility management whereas MIPv6 as a global mobility management (named H-PMIP). As a result, the complexity of the hosts is increasing since they have to support both the network-based and the client-based protocol stacks. Another scenario is also considered, where PMIPv6 and MIPv6 are co-located at LMA/HA. Yet, there exist some problems due to the natural difference between the two protocols [192].
In [193], an extension to PMIPv6 (called I-PMIP) is proposed for the inter-domain mobility support by reusing the local mobility anchor as a global anchor point when the MN is away from home. Then the traffic is forwarded from/to the anchor, which is called Session Mobility Anchor (SMA), to/from the current serving Local Mobility Anchor (S-LMA) where the MN is currently attached. Thus, two scenarios are suggested to find the corresponding SMA:

- Direct location: A common database is introduced to store information about the established MN-SMA bindings from all domains.

- Indirect location: This scenario is based on the fact that the SMA is a topological anchor point of the MN. So, after inferring the MN's IPv6 address, the S-LMA sends a PBU to this address. This PBU will obviously reach the SMA. However, this approach requires each SMA to analyze all of its incoming traffic to recognize the corresponding PBU. As a result, the complexity of the LMA is increasing, particularly when a lot of traffic passes the LMA.

One critical problem of this solution is that the mobility service is provided on a per user basis. Thus, the mobility service is always provided even for the sessions that do not require a mobility support (e.g., when the MN remains attached to the same domain during the lifetime of the sessions). Also, when the MN starts a new session at a new domain, it still has to use the SMA as the anchor point, which may cause the sub-optimal routing and tunneling overhead problems.
Another proposal [194] is based on the idea that the home address (HoA) and Care-of-Address (CoA) are not only used for the MN, but also for the specific session. Every PMIPv6 entity maintains two Binding Cache Entries (BCE) for each registered MN. One is Inner-domain BCE as normal BCE in the PMIPv6 domain, and the other is Inter-domain BCE which maintains the binding between HoA and CoA of the Corresponding Node (CN). When an MN moves to another PMIPv6 domain, the S-LMA needs to communicate with the previous one to get the HoA of CN. It also interacts with the CN's home LMA to update the current location of the MN. The same process is executed when CN changes its PMIPv6 domain. Though the traffic is routed via a near-optimal way (directly from the CN to the current location of the MN), this solution becomes too complex especially when the MN communicates with many CNs at the same time. Moreover, this proposal can be applied only in the case where both the MN and the CN are attached to PMIPv6 domains.

7.3 Description of the Solution

Based on the DMM concept, we introduce an inter-domain mobility support, called D-PMIP. Thus, this proposal brings some benefits: (i) the mobility anchors are placed very

close towards the MN; and (ii) the mobility service is only provided for the sessions that really require the service continuity.

Once the MN enters its PMIPv6 domain, it gets a set of prefixes. For simplicity, it is assumed that only one prefix will be allocated for each MN. Based on the prefix allocated, the MN configures its IPv6 address. The MN then can use this address to initiate and maintain the sessions in a standard way while it remains attached to this domain. When the MN changes its domain, it gets another prefix and configures its address based on this prefix. This address can be used to set up the new sessions. Until the previous sessions are not closed, the old address should be kept. Thus, a tunnel is built between the anchor LMA (A-LMA) and the current one to redirect packets between two LMAs using the old prefix.

To enable the inter-domain mobility support, the BCE in the LMA is needed to extend with a field, called I-LMA which contains a list of the MN's prefixes and the previous/current LMA's address. Based on the DMM concept, two possible solutions for inter-domain mobility support are considered, namely the partially (DP-PMIP) and fully distributed (DF-PMIP) solution. The former solution relies on a common database for control plane, while in the latter one the mobility function is distributed in both data and control plane.

7.3.1 Partially Distributed Solution (DP-PMIP)

Similar to I-PMIP, this solution relies on the existing of a central entity called Inter-domain Central Mobility Database (ICMD) which stores information of mobility sessions of all PMIPv6 domains. This common database can be established by service level agreements between the operators of PMIP domains. Unlike I-PMIP, the MN's prefix is used to distinguish between ICMD entries. In addition, the ICMD can play the role of the LMA and the MAG to handle the PBU/ PBA messages.

7.3.1.1 Initial Registration

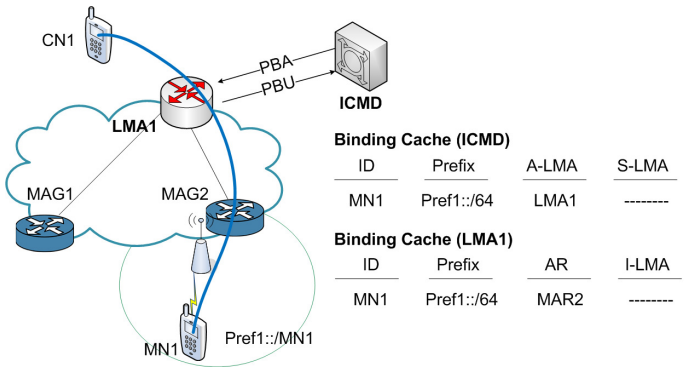


Figure 7.1 – Initial registration signaling in the partially distributed approach (DP-PMIP).

When an MN is attached to a PMIPv6 domain, the standard PMIPv6 operations are executed. The LMA (LMA1) then sends a PBU to the ICMD. This PBU includes the Mobile Node Identifier and Home Network Prefix (HNP) option which are set to the MN's identifier (MN-ID) and the MN's prefix (Pref1), respectively. Since the session is new, the ICMD creates an entry which consists of the MN-ID, the Pref1 and the address of LMA1 in its BCE. The signaling process and the BCE of the ICMD are described in Fig. 7.1.

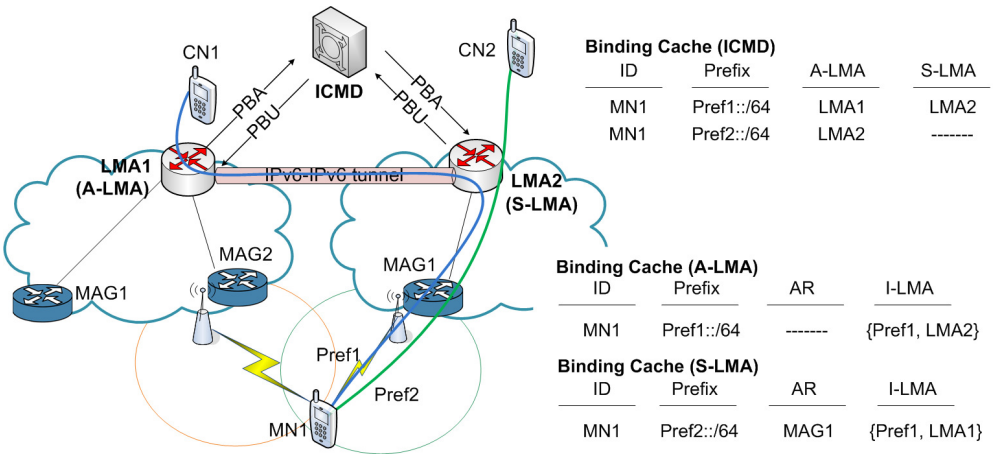


Figure 7.2 – Handover signaling in the partially distributed approach (DP-PMIP).

7.3.1.2 Inter-domain Operations

The signaling procedure of DP-PMIP in case of handover is illustrated in Fig. 7.2. When the MN moves to another domain, the current LMA (LMA2 or S-LMA) allocates another prefix (Pref2) to the MN. Then, the S-LMA sends a PBU to the ICMD for the new prefix registration. Upon receiving the PBU and searching the BCE table, the ICMD updates the current location to the existing entries for the MN. It also creates a new entry corresponding to the MN-ID and the new prefix. The ICMD then sends a PBU including the S-LMA's address to the A-LMA (LMA1) to update the current location of the MN. After receiving the PBU, the A-LMA sets up its endpoint for bi-directional tunnel to the S-LMA, updates its BCE and routing for Pref1. In parallel, the ICMD indicates the address of A-LMA to S-LMA (by means of PBA message), which performs the same process as that of A-LMA. Afterwards, a bi-directional tunnel is established between the S-LMA and A-LMA to carry the traffic from/to MN using Pref1.
As a global anchor point of Pref1, the A-LMA, after receiving the packets destined to this prefix, forwards them through the bi-directional tunnel to the corresponding S-LMA. The packets then reach the MN at the current PMIPv6 domain.
When the MN transmits packets using Pref1 as source, the S-LMA, after receiving the packets, firstly checks their source address in the BCE. The S-LMA then forwards them through the tunnel to the corresponding A-LMA which routes them towards the destination. On the contrary, the packets using Pref2 as source are routed as a regular PMIPv6 routing.

7.3.2 Fully Distributed Solution (DF-PMIP)

In this solution, the central database for inter-domain is removed from the architecture. Thus the complexity of the handover procedures is increased as a result of the trade-off between the elimination of the central database and the signaling cost. Since the S-LMA does not have knowledge of the LMAs in the other PMIPv6 domain, finding the A-LMA's address of the MN's prefix becomes a key challenge. There are several methods to solve this issue:

- using a Layer 2 handover infrastructure e.g., IEEE 802.21 [195];
- using a distributed LMA-discovery mechanism [164];
- relying on a distributed infrastructure that allows the communication between the domains.

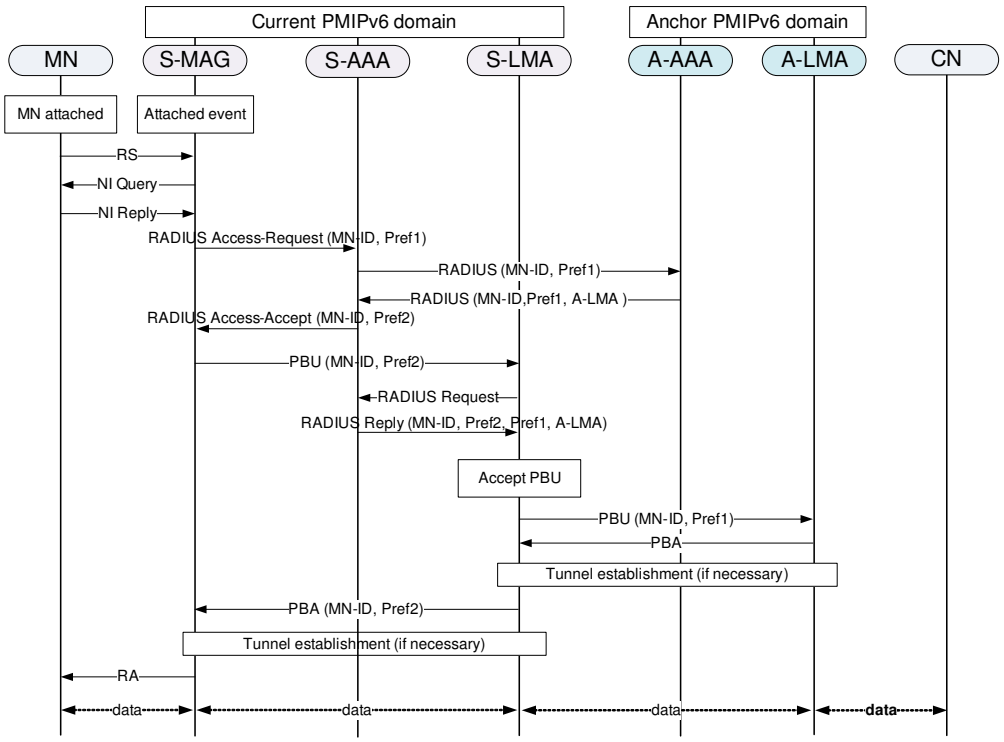


Figure 7.3 – Fully distributed approach (DF-PMIP).

In this chapter, we introduce an example to illustrate how this approach works by using a distributed Authentication, Authorization, and Accounting (AAA) infrastructure [196] and Remote Authentication Dial In User Service (RADIUS) protocol for PMIPv6 [169]. The protocol operations can be briefly explained as follows (see Fig. 7.3).
After detecting the presence of a new MN, the current serving MAG (S-MAG) obtains the information of the MN (MN's IPv6 address) by exchanging Node Information (NI) Query/NI Reply messages [197]. If the MN's IPv6 address is not available, then the normal process is executed. Vice versa, the S-MAG, after extracting the prefix from MN's address, sends a RADIUS Access-Request message with PMIPv6-Home-HN-Prefix (Pref1) and Mobile-Node-Identifier (MN-ID) options, to the AAA server (S-AAA) to retrieve the MN's policy profile. If this prefix belongs to its domain, the S-AAA then continues with its regular operations. Otherwise, acting as a RADIUS client, the S-AAA sends a RADIUS message (including MN-ID and Pref1) to the AAA in the anchor domain (A-AAA), to get A-LMA's address. Upon the reception of the RADIUS reply message from A-AAA, the S-AAA sends an Access-Accept message which includes the prefix allocated to this MN (Pref2) to S-MAG. Afterwards, the standard PMIP operations related to Pref2 are executed (e.g., location update and MN's address configuration). The S-LMA also obtains the A-LMA address from the S-AAA server. Then, the PBU/PBA messages are exchanged between the S-LMA and A-LMA to update their BCEs and routing related to Pref1.

7.3.3 Local Routing Considerations

After the receipt of the up-link packets from MN using Pref1 as source, the S-LMA will decide to forward them to the destination depending on the following cases: (i) if the CN is currently attached to its domain, the S-LMA simply forwards the packet to the corresponding MAG; (ii) if the CN's address belongs to its domain but the CN is currently

attached to another one, the S-LMA will forward the packets to the LMA that the CN is currently attached to; and iii) Otherwise, the packets will be routed following the normal internet routing.

7.3.4 Multicast Considerations

All proposals for the inter-domain mobility support do not take multicast into account. In general, when a listener moves to a new domain, the on-going multicast flows will be interrupted. Additionally, the MN then has to re-join these flows in the new domain. Thus, the main objectives are: i) keeping the MN unaware of mobility from multicast application point of view; and ii) reducing the potential service disruption. In our proposed solution, multicast support can be enabled by using the multicast context transfer function and extending the PBU/PBA message to convey the multicast subscription information of the MN, as described in Fig7.4. As stated in the previous section, the multicast context transfer function is developed as an independent module, which allows it to be easily integrated in any solution. The multicast-related signaling process is briefly described as follows. As

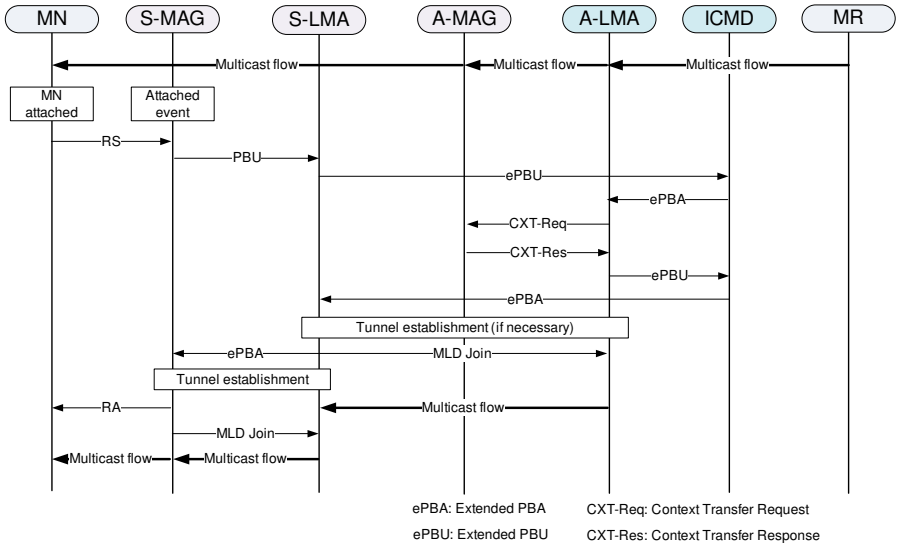


Figure 7.4 – Multicast mobility support in DP-PMIP.

stated in the previous section, upon the reception of PBU from the S-LMA, the ICMD sends a PBA to the A-LMA to update the current location of the MN. This PBA is extended to request the multicast subscription information of the MN. The A-LMA based on the context transfer function obtains the MN's subscription information from the A-MAG, and then sends it to the ICMD. The ICMD replies to the S-LMA by sending a PBA message including the MN's subscription information. The S-LMA, after establishing a tunnel with the A-LMA, sends an MLD Report to join the ongoing multicast flows of the MN via the A-LMA. The S-LMA also includes the subscription information in the PBA message to send to the S-MAG. The S-MAG, after adding the MN to a downstream interface of its MLD proxy, sends an MLD Report to the S-LMA to join these flows. Afterwards, the multicast packets are routed to the MN via the A-LMA, S-LMA and S-MAG.

7.4 Performance Analysis

In this section we analyze the performance of the proposed solutions in terms of signaling cost, handover latency and tunnel usage. We compare our solutions with the other ones for the inter-domain handover e.g., MIPv6, H-PMIP and I-PMIP.

7.4.1 Reference Model

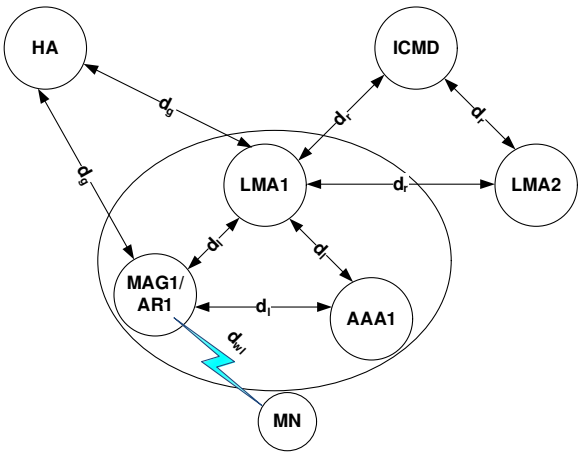


Figure 7.5 – Reference network topology for performance analysis.

Fig. 7.5 shows a reference topology for performance analysis. For simplicity, the average distance (number of hops) between the entities is defined as follows:

- The distance between the PMIPv6 entities in the same domain (local) is d_l (e.g., between the MAG and the LMA).
- The distance between two domains (region) is d_r (e.g., between two LMAs or between the LMA and the ICMD).
- The distance between LMA/AR and Home Agent (HA) (global) is d_g.
- The distance between the MAG/AR and the MN (wireless connection) is d_{wl}.

7.4.2 Signaling Cost

Signaling cost of a mobility management protocol is defined as the transmission cost of location update signaling when an MN performs handover. To measure the signaling cost in the inter-domain context, the handoff frequency should be taken into account. As a result, we use a well-known factor, called session-to-mobility ratio (SMR) which represents the relative ratio of session arrival rate to the user mobility rate. It is assumed that the subnet residence time (MAG subnet) and session duration follows an exponential distribution with parameter η and μ, respectively. Hence, the SMR is calculated as $\rho = \frac{\mu}{\eta}$ [198]. Each LMA coverage area is supposed to be circular with N subnets. According to [72], the intra-domain and the inter-domain handoff probability are defined as $\rho_{intra} = \frac{1}{1+\rho}$, $\rho_{inter} = \frac{1}{1+\rho\sqrt{N}}$. And the expected numbers of intra-handoff and inter-handoff are $E_{intra} = \frac{1}{\rho}$, $E_{inter} = \frac{1}{\rho\sqrt{N}}$

Thus, the average location update signaling is given by:

$$SC(.) = (E_{intra} - E_{inter})\, SC_{intra}(.) + E_{inter} SC_{inter}(.), \tag{7.1}$$

where SC_{intra} and SC_{inter} are signaling update cost for intra-domain and inter-domain handover, respectively. Although different signaling messages have different size, we assume that they have the same size for simplicity. Also, the cost for transmitting a signaling message is supposed to be proportional to the distance between source and destination. The proportion is α for wired and β for wireless link. The signaling cost of DP-PMIP is calculated as:

$$SC_{intra}(DP-PMIP) = 2\beta d_{wl} + 2\alpha d_l, \tag{7.2}$$

$$SC_{inter}(DP-PMIP) = 2\beta d_{wl} + 2\alpha d_l + 4\alpha d_r. \tag{7.3}$$

Similarly, we can derive the equations of the signaling cost for DF-PMIP, MIPv6 and H-PMIP. It is noted that the signaling cost for intra-domain handover of DF-PMIP and H-PMIP is the same and equal to that of DP-PMIP (PMIP handover cost).

$$SC_{inter}(DF-PMIP) = 4\beta d_{wl} + 6\alpha d_l + 4\alpha d_r. \tag{7.4}$$

$$SC_{inter}(MIP) = SC_{intra}(MIP) = 4\beta d_{wl} + 2\alpha d_g. \tag{7.5}$$

$$SC_{inter}(H-PMIP) = 4\beta d_{wl} + 2\alpha d_l + 2\alpha d_g. \tag{7.6}$$

7.4.3 Handover Latency

The Inter-domain handover latency (HO_{inter}) is defined as the total time taken to complete all the operations before the traffic can be forwarded to the current location of the MN. Let HO_{intra} denote the intra-domain handover delay. Then, the average value of handover latency is

$$HO(.) = (\rho_{intra} - \rho_{inter})\, HO_{intra}(.) + \rho_{inter} HO_{inter}(.). \tag{7.7}$$

Since the delay between two nodes depends on the bandwidth, the propagation delay and the distance between them, for simplicity, we suppose that the delay is proportional to the distance. The proportion is τ for wired link and κ for wireless link. Let t_{L2} denote the delay caused by Layer 2 handover. Thus, the intra-domain handover delay of DP-PMIP, DF-PMIP and H-PMIP are the same (PMIP handover delay) and are calculated as follows:

$$HO_{intra}(DP-PMIP) = t_{L2} + 2\kappa d_{wl} + 2\tau d_l. \tag{7.8}$$

On the other hand, the handover latency of DP-PMIP, DF-PMIP, MIPv6 and H-PMIP are given by the equations below.

$$HO_{inter}(DP-PMIP) = t_{L2} + 2\kappa d_{wl} + 2\tau d_l + 2\tau d_r. \tag{7.9}$$

$$HO_{inter}(DF-PMIP) = t_{L2} + 4\kappa d_{wl} + 6\tau d_l + 4\tau d_r. \tag{7.10}$$

$$HO_{inter}(MIP) = SD_{Intra}(MIP) = t_{L2} + 4\kappa d_{wl} + 2\tau d_g. \tag{7.11}$$

$$HO_{inter}(H-PMIP) = t_{L2} + 4\kappa d_{wl} + 2\tau d_r + 2\tau d_g. \tag{7.12}$$

7.4.4 Tunnel Usage

In this subsection, we will measure the tunnel usage ratio, called θ which is calculated as the ratio between the number of sessions using the tunnel (between the anchor and the current domain) and the total number of sessions. Thus, it can be used to show the advantage of using DMM in terms of dynamic provision of mobility service.

Since in MIPv6, H-PMIP and I-PMIP the traffic always passes the tunnel between the global anchor point and the current one, θ is equal to 1.

To measure θ in case of D-PMIP, the sessions are separated into new sessions and handoff sessions. Thanks to DMM, the tunnel is used only for the handoff sessions. Let $N_n(t)$ and

$N_h(t)$ denote the numbers of new sessions and handoff sessions up to time t, respectively. We suppose that $N_n(t)$ and $N_h(t)$ are a Poisson process with parameter λ_n and λ_h, respectively. Thus, we have $\theta = \frac{N_h(t)}{N_n(t)+N_h(t)}$. According to [198] $\lambda_h = E[H] * \lambda_n$, where E[H] is the handoff rate (in our case E[H] = $\frac{1}{\rho\sqrt{N}}$). Thus, we obtain:

$$\theta = \frac{1}{1+\rho\sqrt{N}}. \tag{7.13}$$

7.4.5 Multicast Service Disruption Time

Similar to the handover latency, the multicast service disruption time ($SD(.)$) is defined as

$$SD(DP{-}PMIP) = (\rho_{intra} - \rho_{inter})\, SD_{intra}(DP{-}PMIP) + \rho_{inter} SD_{inter}(DP{-}PMIP), \tag{7.14}$$

where $SD_{intra}(DP-PMIP)$ and $SD_{inter}(DP-PMIP)$ are the multicast service disruption time for intra- and inter-domain mobility, respectively. As can be seen in Fig. 7.4, $SD_{inter}(DP-PMIP)$ is calculated as

$$SD_{inter}(DP-PMIP) = t_{L2} + 2\kappa d_{wl} + 4\tau d_l + 4\tau d_r + 2max\{\tau d_l, \tau d_r\}. \tag{7.15}$$

The multicast service disruption, in case of intra-domain handover is given by (see Chapter 4)

$$SD_{intra}(DP-PMIP) = t_{L2} + 2\kappa d_{wl} + 6\tau d_l. \tag{7.16}$$

On the other hand, the average multicast service disruption time in PMIPv6 is given by

$$SD(PMIP) = \rho_{intra} SD_{intra}(DP-PMIP). \tag{7.17}$$

7.5 Numerical Results

This section presents the numerical results based on the analysis given in the previous section. The default parameter values for the analysis are introduced in Table 7.1 in which some parameters are taken from [72].

Table 7.1 – Parameters for Performance Analysis

Parameters	Values	Parameters	Values
d_{wl}	1 hops	d_l	6 hops
d_r	6 hops	d_g	12 hops
τ	2	κ	15
N	32	α	1
β	5	t_{L2}	50ms

Fig. 7.6 shows the signaling cost when SMR (ρ) is varying. We can observe that the signaling cost of the fully distributed solution is relatively high compared to the other. It is evident since more messages are required to get the address of the anchor LMA. The partially distributed solution and I-PMIP have lower signaling cost than that of the others. In highly mobile regimes ($\rho \ll 1$), the difference between the protocols becomes more clearly. Fig. 7.7 illustrates the handover latency as a function of SMR. The partially distributed solution (DP-PMIP) has better handover latency (lower is better) over the other solutions especially when ρ is small (in highly mobile regimes).

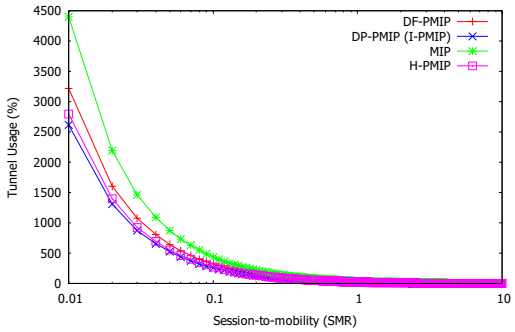


Figure 7.6 – Signaling cost variation with SMR (ρ).

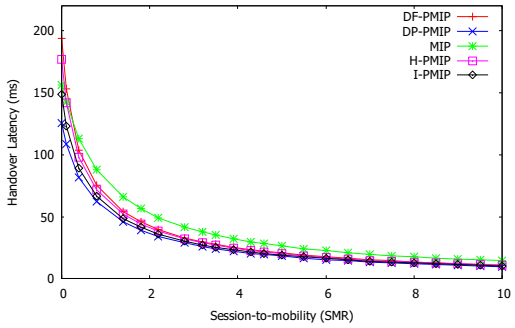


Figure 7.7 – Handover latency variation with SMR (ρ).

To measure the impact of domain size on the handover latency, we assume that the architecture of the inter-domain is hierarchically formed as a tree structure with a d_r-layer, while the structure of a PMIPv6 domain as a binary tree with a d_l-layer [199]. The size of the network is supposed to be fixed e.g., the distance between the ICMD and MAG is 12 hops. Therefore, d_l and d_r are calculated as $d_l = log_2(N)$, $d_r = 12 - log_2(N)$. Fig. 7.8 describes the impact of domain size on handover latency when the value of ρ is set to 0.1. It is observed that when the domain size is small, the handover latency is high for all solutions. When the domain size is increased, the handover latency is decreased and then makes a bit increase.

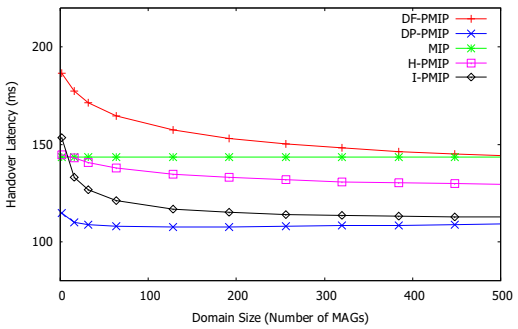


Figure 7.8 – Domain size effect.

The tunnel usage as a function of SMR is illustrated in Fig. 7.9. In low mobility regimes ($\rho \gg 1$) the tunnel usage is significantly decreased in D-PMIP (DP-PMIP, DF-PMIP) compared to the others. The reason is that the number of new sessions in low mobility regimes is definitely higher than that of handoff sessions.
Finally, Fig. 7.10 plots the average multicast service disruption time as a function of SMR.

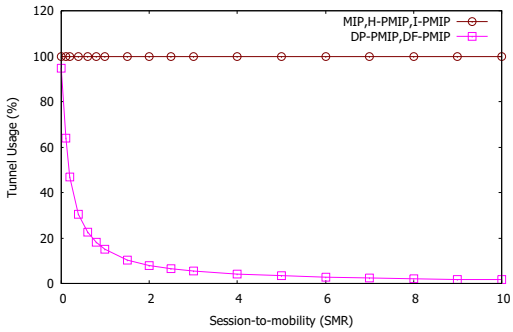


Figure 7.9 – Tunnel usage (θ) as a function of SMR (ρ).

We can observe that the average service disruption in case of DP-PMIP is slightly greater than that in case of intra-handover inside PMIPv6. It is because inter-domain handover latency is typically greater than that in case of intra-domain handover.

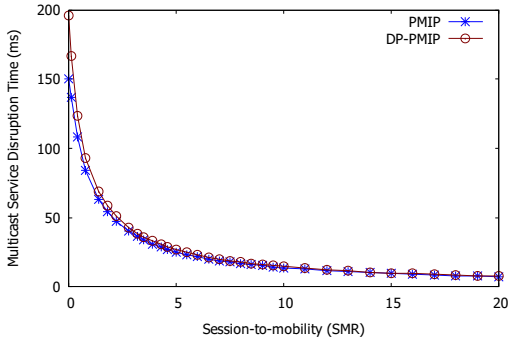


Figure 7.10 – Multicast service disruption time as a function of SMR (ρ).

7.6 Conclusion

This chapter proposes a solution (D-PMIP) that allows providing mobility service for the moving hosts between PMIPv6 domains. Based on the DMM concept, the proposal allows bringing the mobility anchors closer to the MN and dynamically providing the mobility service for only sessions which really need the service continuity. The D-PMIP also retains the advantageous features of a network-based mobility management form PMIPv6 that provides mobility service without the involvement of the MN. A numerical analysis demonstrates that the partially distributed solution gives better performance than the other solutions like MIPv6, H-PMIP, I-PMIP and the fully distributed solution in terms of signaling cost, handover latency and tunnel usage. Thus, at the moment the partially distributed solution seems to be more suitable than the fully distributed one.
The proposed solutions can be considered as a DMM-like approach applying to the existing PMIPv6 network to improve the mobility of the nodes. We then present a basic support for the multicast mobility in the partially distributed scheme. It allows keeping the MN unaware of mobility from the multicast service perspective. Also, the multicast service disruption time is slightly increased compared to the mobility inside a single PMIPv6 domain.

8

On the Efficiency of Dynamic Multicast Mobility Anchor in DMM

As stated in the previous chapter, IP multicast can be enabled in DMM by deploying the MLD proxy function at MAR. The multicast traffic is routed directly from the native multicast infrastructure via the current MAR for the new multicast flow. For the flow after handover, the multicast traffic is tunneled from the MAR where the flow is initiated to the current one via the mobility tunnel between them. Thus, the multicast mobility anchor (MMA) is assigned at the initial phase of the multicast flow (identical with the unicast mobility anchor): the MAR where the flow is initiated. The multicast flow will be anchored at the initially assigned MMA during its lifetime. Therefore, even when the MN moves far away from its anchor, the multicast traffic still traverses the anchor. As a result, it causes several issues to the ongoing multicast flow such as service disruption, non-optimal routing, end-to-end delay and packet duplication. These problems become serious when considering the interruption- and delay-sensitive services. Also, even the mobility anchors are distributed, some anchors are more overloaded than the others [200].

In this chapter, we mainly argue the need for a dynamic multicast mobility anchor (DMMA) mechanism. From a service point of view, it helps satisfy the requirements in terms of service disruption and delay, especially when considering the real-time services. It provides a mechanism to better distribute the load among MARs. Moreover, other issues like packet duplication and leave latency (waste of resource) can be reduced. The DMMA takes into account not only the multicast service context (e.g., interruption-sensitive and delay-sensitive services) but also the mobile node's mobility context and the network context (such as current load of MARs and multicast channel policy), thus enabling a per-flow multicast support. In other words, each multicast flow can be treated differently upon different contexts.

The rest of this chapter is organized as follows. Section A.4.1 introduces the issues and different approaches for the multicast listener support in a DMM environment. Section A.4.2 presents the performance analysis regarding different metrics as service disruption, end-to-end delay, signaling cost and packet loss. The DMMA mechanism is presented in Section A.4.3. Section 8.4 discusses the implementation work, the scenario in which the multicast router is deployed at MAR as well as the multicast source support. Finally, Section 8.5 concludes this chapter and provides perspectives for future work.

8.1 Multicast Listener Mobility in DMM

This chapter follows the concept of the network-based DMM proposed by the IETF DMM Working Group[1] as described in Chapter 2. We recall some abbreviations introduced in the previous chapters to denote the role of MAR from a mobile node point of view:

- Current MAR (cMAR) is the MAR to which the MN is currently attached.
- Anchor MAR (aMAR) of an MN's address/session is the MAR where the prefix in use is allocated (and the session is initiated using this address as the source address).
- Previous MAR (pMAR) is the MAR where the MN was previously attached.

As mentioned in Chapter 2, there is a limited work for the multicast support since the DMM is still in an early stage of standardization. This chapter focuses on the scenario in which the MAR acts as an MLD proxy. Also, only multicast listener mobility in the network-based DMM is further studied. In this case, when a multicast flow is initiated, the multicast traffic is received directly from the native multicast infrastructure via the cMAR. After handover, the traffic is routed from the anchor to the current MAR via the tunnel between them (like unicast traffic). In this chapter, it is called the default multicast mode in DMM. However, this mode does not address any multicast-related issues caused by the movement of listener such as service disruption, packet loss, non-optimal routing, end-to-end delay, and tunnel convergence problem (for further information, see Chapter 2). Regarding the service disruption, when a multicast listener moves from the pMAR to the cMAR, it may cause a noticeable service disruption for the ongoing flows. As a result, the multicast context transfer is required to avoid a large delay caused by multicast-related procedures (about 5s in the normal case, and 2.5s in the best case) [16]. This delay is much longer than the maximum tolerant interruption time for normal services, as specified in [162] is 500 ms. Even with the multicast context transfer, it is unable to meet the requirement in terms of service disruption for the interruption-sensitive service when the delay cMAR-aMAR is large [22, 129]. It is because the multicast traffic has to pass through the aMAR, which plays the role of multicast mobility anchor (MMA).
Also, since the multicast traffic always traverses the aMAR, it often results in a longer route (e.g., when the source and the listener are close to each other but far from the listener's aMAR). In particular, when considering a significant large domain, it can cause a high end-to-end delay. This issue becomes serious when the end-to-end delay sensitive service is considered.
In case of mobility, the utilization of the mobility tunnel for the multicast flow may result in the tunnel convergence problem. It occurs when multiple instances of the same multicast traffic converge to an MAR, leading to the redundant traffic. The main reason is that multiple MLD proxy instances are installed at MAR with their upstream interfaces configured to different aMARs. Since the purpose of DMM is moving the mobility anchors from the core to the edge of the networks, the number of mobility anchors in a DMM domain will be much more than that in a PMIPv6 domain. As a consequence, the tunnel convergence problem is supposed to be much more severe than that in PMIPv6. As stated in the DMM requirements [8], the multicast solutions in DMM should take this issue into consideration. By using an extension to MLD proxy to support multiple upstream interfaces [167], the tunnel convergence problem can be avoided. In this case, only one proxy instance will be installed at MAR with its upstream interfaces being configured towards different aMARs and its upstream MR. Accordingly, the MAR will receive only one instance of the multicast packet. To highlight these issues, this subsection considers different candidates for the MMA

[1] http://datatracker.ietf.org/wg/dmm/

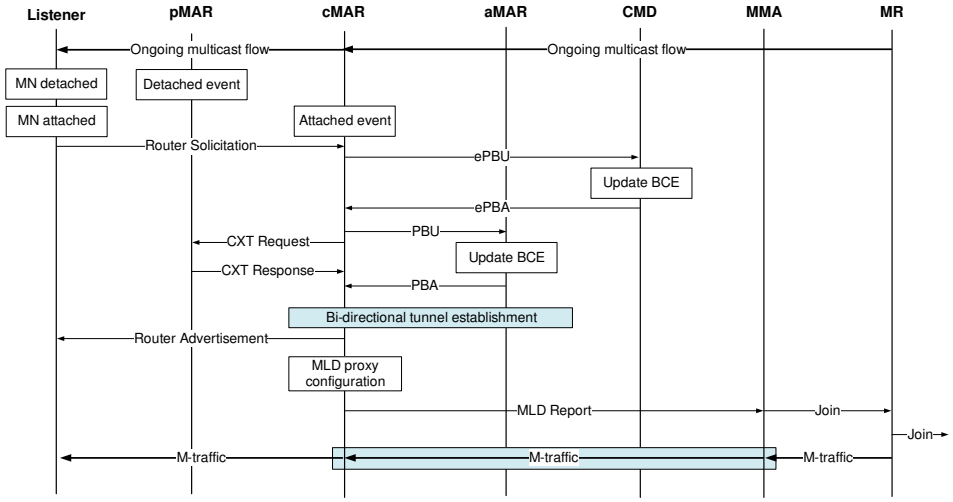


Figure 8.1 – Signaling when a listener performs a handover in DMM.

such as the aMAR (default mode), the pMAR, the cMAR (native subscription), or a common MMA (COMMA) which serves as only one MMA for the domain (as similar in [117]). Different approaches MMA_aMAR, MMA_pMAR, MMA_cMAR, and MMA_COMMA are considered, accordingly. We also consider the impact of deploying MLD proxy with multiple upstream interfaces on the service disruption time, end-to-end delay and signaling cost.

The signaling when a listener performs a handover in DMM is described in Fig. A.7. The operations are briefly described as follows. The central mobility database (CMD), as an extended LMA, stores the MN's home network prefixes, its corresponding anchor points (aMAR) and its current location (cMAR). In case of handover, the cMAR allocates a new network prefix for this MN. The cMAR then sends a PBU to the CMD for the new prefix registration as well as retrieves the address of the anchoring MARs of the ongoing sessions. This message includes the MN_ID, the allocated prefix at the current MAR. By looking up the BCE table, the CMD updates the entry corresponding to the MN_ID with the current location of the MN. The CMD then replies by an extended PBA including the list of previous addresses and the corresponding prefixes. Upon receiving this message, the cMAR exchanges the PBU/PBA messages with the anchor MARs in order to update the current location of the MN. Thus, the bi-directional tunnel is established between the cMAR and each aMAR, if necessary. In parallel, the multicast context transfer messages are exchanged between the cMAR and the pMAR allowing the cMAR to obtain the active multicast subscription of the MN. For each flow, the cMAR configures an upstream interface towards the MMA (if necessary), and sends an MLD report to the MMA to join the flow. The MMA, after joining the multicast delivery tree, forwards the multicast packets to the cMAR via the tunnel between them. Finally, they reach the MN.

8.2 Quantitative Analysis

This section presents the quantitative analysis of different approaches regarding different metrics such as multicast service disruption, end-to-end delay, signaling cost and packet loss.

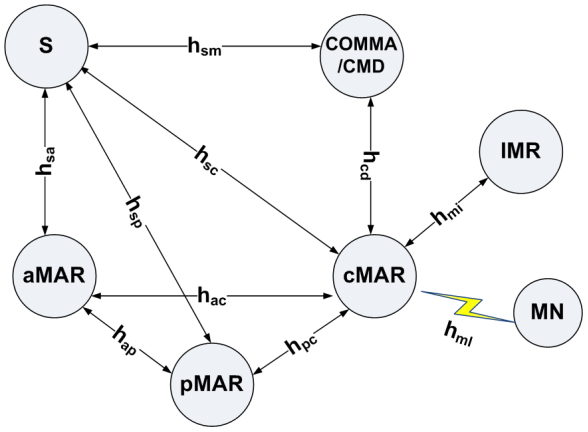


Figure 8.2 – Reference network topology.

8.2.1 Network Model and Performance Metrics

8.2.1.1 Reference model

Fig. A.8 shows a reference topology for the performance analysis. The hop-count distances between the entities are defined as follows:

- h_{ac}: the average number of hops between the aMAR and the cMAR.
- h_{ap}: the average number of hops between the aMAR and the pMAR.
- h_{pc}: the average number of hops between the pMAR and the cMAR.
- h_{cd}: the average number of hops between the MAR and the CMD/COMMA.
- h_{ml}: the average number of hops between the MAR and the listener (MN), it is assumed to be one (wireless link).
- h_{sa}: the average number of hops between the source S and the aMAR.
- h_{sp}: the average number of hops between the source S and the pMAR.
- h_{sc}: the average number of hops between the source S and the cMAR.
- h_{sm}: the average number of hops between the source S and the COMMA.
- h_{mr}: the average number of hops between the MAR and its upstream MR, it is assumed to be one.
- h_{mi}: the average number of hops between the cMAR and the intersection MR (IMR) which already has a multicast forwarding state for the group.

We then define the network scale ψ which is the ratio between the number of hops between two adjacent MARs (h_{mm}) and the number of hops between the MAR and the CMD (h_{cd}).

$$\psi = \frac{h_{mm}}{h_{cd}}. \tag{8.1}$$

Typically, the average number of hops between two adjacent MARs is less than that between an MAR and a centralized entity. That means $\psi \leq 1$. In this chapter, we will investigate the impact of the network scale on the performance metrics by varying the value of ψ over a range [0,1] (by varying h_{mm} while fixing the value of h_{cd}).

8.2.1.2 Messages Related to the Performance Analysis

As described in Fig. A.7, various messages are used in our analysis. For a sake of simplicity, we suppose that there is only one ongoing flow. The following message sizes in bytes are considered in our analysis:

- L_{RS}: It is the size of the Router Solicitation (RS) message, which is 52.
- L_{RA}: It is the size of the Router Advertisement (RA) message, which is 80.
- L_{PBU}: It is the size of the PBU message, which is 84.
- L_{PBA}: It is the size of the PBA message, which is 92.
- L_{ePBU}: It is the size of the extended PBU message, which is 84.
- L_{ePBA}: It is the size of the extended PBA message, which is 128.
- L_{M-Req}: It is the size of the multicast context transfer request message, which is 86.
- L_{M-Res}: It is the size of the multicast context transfer response message, which is 104.
- L_{C-Req}: It is the size of the channel configuration request message, which is 92.
- L_{C-Res}: It is the size of the channel configuration response message, which is 112.
- L_{MLD-R}: It is the size of the MLD Report message, which is 96.
- L_{Join}: It is the size of the PIM Join message, which is 110.
- L_{MP}: It is the size of the multicast packet, which is 200.
- L_T: It is the size of the tunneling header, which 40.

It is noted that the values of L_{PBU}, L_{PBA}, L_{ePBU}, L_{ePBA}, L_{M-Req} L_{M-Res}, L_{C-Req} and L_{C-Res} are taken from the real implementation of PMIPv6 [155] and the multicast context transfer function [161], while the others are from [73, 69].

8.2.1.3 Delay Model

As described in Chapter 3, we adopt the packet transmission delay model in [134] in which the packet transmission consists of the transmission time and the propagation time. Thus, the transmission delay of a wired link can be calculated as

$$d_{wd}(l,h) = h(\frac{l}{BW_{wd}} + D_{wd}), \tag{8.2}$$

where h is the hop-count distances between two nodes, l is the length of the packet, BW_{wd} is the bandwidth of wired link and D_{wd} is the wired link latency.
Unlike the wired transmission which can be considered as reliable, the wireless link is unreliable. The wireless transmission delay is therefore calculated as [134]

$$d_{wl}(l) = \frac{1}{1-q}(\frac{l}{BW_{wl}} + D_{wl}), \tag{8.3}$$

where q is the probability of wireless link failure, BW_{wl} is the bandwidth of wireless link and D_{wl} is the wireless link latency.

8.2.1.4 Mobility Model

In this chapter, we consider the case where the MN always moves from MAR to MAR as if they were linearly deployed (the user is moving further away from the first attached MAR and never attaches back to a previously visited MAR). It represents the worst-case scenario. Thus, we have $h_{ac} = h_{ap} + h_{pc}$. Let N_{mar} denote the average number of MARs involved in the data traffic forwarding to/from an MN. In our context, N_{mar} is also the number of handovers. We therefore obtain

$$h_{ac} = N_{mar} h_{mm}, \tag{8.4}$$

$$h_{pc} = h_{mm}. \tag{8.5}$$

In our analysis, the low value of N_{mar} represents the low mobility node and the short-lived flow scenarios. The higher value of N_{mar} corresponds to the high mobility and long-lived flow scenarios.

8.2.2 Analytical Modeling

This subsection develops an analytical model regarding the following performance metrics: the multicast service disruption time ($SD(.)$), representing the period when the listener cannot receive the multicast packet; the end-to-end delay ($E2E(.)$) - the transmission time from source to listener; the signaling cost ($SC(.)$) - the cost for supporting multicast handover; the packet delivery cost ($DC(.)$) - the cost to deliver multicast packets from the source to the listener; the packet tunneling cost ($TC(.)$) - the tunnel overhead; and packet loss (φ_p) - the number of lost packets during handover. In the performance analysis, we consider the normal case and the case where the MLD proxy supports the multiple upstream interfaces capability. We then highlight the impacts and benefits of using multiple upstream interfaces on these metrics.

8.2.2.1 Multicast Service Disruption Time Analysis

The multicast service disruption time ($SD(.)$) is defined as a period when a multicast listener is unable to receive the multicast packets. Assuming that the delay associated with the processing of the messages in the network entities (e.g., time for PBU processing and updating binding cache in MAR) is included in the total value of each variable. Then the service disruption time is (see Fig. A.7)

$$SD(.) = T_{L2} + d_{wl}(L_{RS}) + T_{CMD} + max\{T_{LU}, T_{CXT}\} + max\{d_{wl}(L_{MP}), T_M(.) + d_{wl}(L_{MP})\}, \tag{8.6}$$

where T_{L2} is the L2 handover duration, T_{CMD} is the time needed to get the address of the anchor/previous MAR from the CMD, T_{LU} is the location update time (at the aMAR), T_{CXT} is the time for the context transfer messages exchanged, $T_M(.)$ is the time needed for the cMAR to join and get the first multicast packet after handovers.
In Eq. (A.6), except $T_M(.)$, the other components are the same in different approaches, and given by

$$T_{CMD} = d_{wd}(L_{ePBU}, h_{cd}) + d_{wd}(L_{ePBA}, h_{cd}), \tag{8.7}$$

$$T_{LU} = d_{wd}(L_{PBA}, h_{ac}) + d_{wd}(L_{PBU}, h_{ac}), \tag{8.8}$$

$$T_{CXT} = d_{wd}(L_{M-Req}, h_{pc}) + d_{wd}(L_{M-Res}, h_{pc}). \tag{8.9}$$

In (A.6), $T_M^{(.)}$ represents the time needed for the cMAR to join and get the first multicast packet. In case of MMA_cMAR, the cMAR has to get the multicast traffic from the IMR

which already has a multicast forwarding state for this group. Thus,

$$T_M(cMAR) = \begin{cases} \overline{w}_{mr} \quad \text{if } h_{mi} = 0, \\ (h_{mi}+1)\overline{w}_{mr} + d_{wd}(L_{MLD-R}) + d_{wd}(L_{MP}) + d_{wd}(L_{Join}, h_{mi}-1) \\ +d_{wd}(L_{MP}, h_{mi}-1) \quad \text{if } h_{mi} \geq 1. \end{cases}$$

where $\overline{w}_{mr}$ is the delay time in which an MR (and an MLD proxy) needs to join a multicast flow at each router (proxy) in the internet [104].
In case of MMA_pMAR, the pMAR already had the multicast state for this flow. We have

$$T_M(pMAR) = 2\overline{w}_{mr} + d_{wd}(L_{MLD-R} + L_T, h_{pc}) + d_{wd}(L_{MP} + L_T, h_{pc}). \tag{8.10}$$

In case of MMA_aMAR, there are two possibilities: the normal case (case 1, without deploying the multiple upstream interfaces, thus, corresponding to the default mode), and the case where MLD proxy with multiple upstream interfaces is deployed at MARs. In the latter case, in the worst situation, the aMAR needs to join the multicast channel, leading to an extra delay. It happens, for example, in case the multicast traffic was received from the multicast infrastructure in the pMAR and the aMAR has left the channel. Let p_a denote the probability that this situation happens. As a result, $T_M(.)$ is calculated as

$$T_M(aMAR) = (1-p_a)T_M(aMAR-c1) + p_a T_M(aMAR-wc), \tag{8.11}$$

where

$$T_M(aMAR-c1) = 2\overline{w}_{mr} + d_{wd}(L_{MLD-R} + L_T, h_{ac}) + d_{wd}(L_{MP} + L_T, h_{ac}), \tag{8.12}$$

$$T_M(aMAR-wc) = \begin{cases} T_M(aMAR-c1) \quad \text{if } h_{mi} = 0, \\ T_M(aMAR-c1) + d_{wd}(L_{MLD-R}) + d_{wd}(L_{MP}) + d_{wd}(L_{Join}, h_{mi}-1) \\ +(h_{mi}+1)\overline{w}_{mr} + d_{wd}(L_{MP}, h_{mi}-1) \quad \text{if } h_{mi} \geq 1. \end{cases}$$

It is noted that $T_M(aMAR-c1)$ represents the multicast service disruption time in the default mode, when $T_M(aMAR)$ shows the impact of using MLD proxy with multiple upstream interfaces on the service disruption time. As a result, $SD(aMAR)$ can be considered as a trade-off between the service disruption and the tunnel convergence problem.
In case of MMA_COMMA, we have

$$T_M(COMMA) = 2\overline{w}_{mr} + d_{wd}(L_{MLD-R} + L_T, h_{cd}) + d_{wd}(L_{MP} + L_T, h_{cd}). \tag{8.13}$$

8.2.2.2 End-to-End Delay

End-to-end delay ($E2E(.)$) is the packet transmission delay from the source to the listener. In the MMA_cMAR, the cMAR receives the multicast traffic directly from the multicast infrastructure. Hence, the end-to-end delay is given by

$$E2E(cMAR) = d_{wd}(L_{MP}, h_{sc}) + d_{wl}(L_{MP}). \tag{8.14}$$

In the MMA_aMAR, the multicast packet is routed from the source to the cMAR via the aMAR, representing the default multicast mode. We have

$$E2E(aMAR) = d_{wd}(L_{MP}, h_{sa}) + d_{wd}(L_{MP} + L_T, h_{ac}) + d_{wl}(L_{MP}). \tag{8.15}$$

In case of MMA_pMAR, the MAR always receives the multicast traffic from its pMAR in the normal case. Therefore, the end-to-end delay is given as follows

$$E2E(pMAR-c1) = d_{wd}(L_{MP}, h_{sa}) + d_{wd}(L_{MP}+L_T, h_{ap}) + d_{wd}(L_{MP}+L_T, h_{pc}) + d_{wl}(L_{MP}). \tag{8.16}$$

In case of using multiple upstream interfaces, we suppose that p_p is the probability that the MAR gets multicast traffic from its upstream interfaces. Thus, $1 - p_p$ is the probability the MAR gets the multicast traffic from its pMAR. The end-to-end delay in case of MMA_pMAR is therefore given by

$$E2E(pMAR) = d_{wl}(L_{MP}) + [d_{wd}(L_{MP}, h_{sa}) + N_{mar}d_{wd}(L_{MP} + L_T, h_{mm})]p_p^{N_{mar}-1} + \sum_{i=1}^{N_{mar}-1} [d_{wd}(L_{MP}, h_i) + (N_{mar} - i)d_{wd}(L_{MP} + L_T, h_{mm})]p_p^{N_{mar}-i-1}(1 - p_p), \quad (8.17)$$

where h_i is the hop-count distances from the source to the i^{th} MAR in the moving path of the MN (from the aMAR to the cMAR), for example, $h_{N_{mar}-1} = h_{sp}$.
Considering the MMA_COMMA, the end-to-end delay is expressed as

$$E2E(COMMA) = d_{wd}(L_{MP}, h_{sm}) + d_{wd}(L_{MP} + L_T, h_{cd}) + d_{wl}(L_{MP}). \quad (8.18)$$

8.2.2.3 Cost Analysis

In this subsection, the signaling cost ($SC(.)$), the packet delivery cost ($PC(.)$) and the tunneling cost ($TC(.)$) are investigated. The signaling cost (per handover) is the signaling overhead for supporting the handover including multicast-related procedures. It can be calculated as

$$SC(.) = SC_{LU} + SC_M(.), \quad (8.19)$$

where SC_{LU}, $SC_M(.)$ is the signaling cost for the location update and the multicast-related procedures, respectively. As mentioned in Chapter 3, the signaling message delivery cost is calculated as the product of the message size, the hop distance and the unit transmission cost in a wired/wireless link (α for the wired and β for the wireless link). SC_{LU} is therefore given by

$$SC_{LU} = \beta(L_{RS} + L_{RA}) + \alpha(L_{ePBU}h_{cd} + L_{ePBA}h_{cd}) + \alpha(L_{PBU}h_{ac} + L_{PBA}h_{ac}). \quad (8.20)$$

$SC_M(.)$ is expressed as

$$SC_M(cMAR) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R} + L_{Join}h_{mi}). \quad (8.21)$$

$$SC_M(pMAR) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{pc}). \quad (8.22)$$

$$SC_M(aMAR) = (1 - p_a)SC_M(aMAR - c1) + p_aSC_M(aMAR - wc), \quad (8.23)$$

where

$$SC_M(aMAR - c1) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{ac}), \quad (8.24)$$

$$SC_M(aMAR - wc) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{ac} + L_{MRD-R} + L_{Join}h_{mi}). \quad (8.25)$$

$$SC_M(COMMA) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{cd}). \quad (8.26)$$

The packet delivery cost represents the cost of delivering multicast packets to the MN per unit of time. Let S_c, λ_p denote the average session length at the cMAR and the packet arrival rate, respectively. Again, the packet delivery cost in the MMA_aMAR corresponds to the default multicast mode. The packet delivery cost is expressed as

$$PC(cMAR) = S_c\lambda_p(\alpha L_{MP}h_{sc} + \beta L_{MP}). \quad (8.27)$$

$$PC(aMAR) = S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha(L_{MP} + L_T)h_{ac} + \beta L_{MP}]. \quad (8.28)$$

In case of MMA_pMAR, in the normal case, the MAR always receives the multicast traffic from its pMAR. Thus, the packet delivery cost is given as follows

$$PC(pMAR - c1) = S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha(L_{MP} + L_T)(h_{ap} + h_{pc}) + \beta L_{MP}]. \quad (8.29)$$

Using the multiple upstream interfaces, the packet delivery cost is calculated as

$$\begin{aligned} PC(pMAR) &= S_c\lambda_p\beta L_{MP} + S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha N_{mar}(L_{MP} + L_T)h_{mm}]p_p^{N_{mar}-1} \\ &+ S_c\lambda_p \sum_{i=1}^{N_{mar}-1} [\alpha L_{MP}h_i + \alpha(N_{mar} - i)(L_{MP} + L_T)h_{mm}]p_p^{N_{mar}-i-1}(1 - p_p). \end{aligned} \quad (8.30)$$

In case of MMA_COMMA, the packet delivery cost is

$$PC(COMMA) = S_c\lambda_p[\alpha L_{MP}h_{sm} + \alpha(L_{MP} + L_T)h_{cd} + \beta L_{MP}]. \quad (8.31)$$

Regarding the packet tunneling cost, it is defined as the additional cost from the tunneling overhead. In MMA_cMAR, the multicast traffic is received directly from the multicast infrastructure, thus, there is no tunneling cost. On the contrary, in MMA_aMAR, MMA_pMAR, and MMA_COMMA the traffic is routed via the tunnel aMAR-cMAR, pMAR-cMAR, and cMAR-COMMA, respectively. Note that the tunneling cost in the MMA_aMAR corresponds to the default multicast mode. The tunneling cost is therefore computed as

$$TC(cMAR) = 0. \quad (8.32)$$

$$TC(aMAR) = \alpha S_c\lambda_p(L_{MP} + L_T)h_{ac}. \quad (8.33)$$

$$TC(pMAR) = \alpha S_c\lambda_p(L_{MP} + L_T)h_{mm} \sum_{i=0}^{N_{mar-1}} (N_{mar} - i)p_p^{N_{mar}-i-1}(1 - \theta p_p). \quad (8.34)$$

where

$$\theta = \begin{cases} 0 & \text{if } i = 0, \\ 1 & \text{if } i \geq 1. \end{cases}$$

$$TC(COMMA) = \alpha S_c\lambda_p(L_{MP} + L_T)h_{cd}. \quad (8.35)$$

The signaling cost in general is an important factor which influences the scalability of the networks. However, as data and control plane are no longer coupled, in case where a huge amount of traffic is generated in the network, the packet delivery cost and tunneling cost play more important role.

8.2.2.4 Packet Loss

During the handover, packets may be lost. The number of lost packets is proportional to the service disruption time and the packet arrival rate. As a result, the number of lost packets is given by

$$\varphi_p(.) = \lambda_p SD(.). \quad (8.36)$$

8.2.3 Numerical Results

This subsection presents the numerical results based on the analysis given in the previous one. The default parameter values for the analysis are introduced in Table A.1, in which some parameters are taken from [177][161]. It is worth noting that the $SD(aMAR-c1)$, $E2E(aMAR)$, $SC(aMAR-c1)$, $PC(aMAR)$, and $TC(aMAR)$ correspond to the default mode in our analysis.

Table 8.1 – Parameters for the performance analysis.

Parameter	Value	Parameter	Value	Parameter	Value
T_{L2}	50ms	BW_{wd}	100Mbps	BW_{wl}	11 Mbps
D_{wd}	2ms	D_{wl}	10ms	q	0.35
$\overline{w}_{mr}$	10 ms	h_{mm}	3 hops	h_{cd}	12 hops
h_{mi}	2 hops	h_{sa}	16 hops	h_{sp}	16 hops
h_{sc}	16 hops	h_{sm}	16 hops	S_c	60 s
λ_p	10 packets/s	α	1	β	5
p_p	0.9	p_a	0.5		

8.2.3.1 Multicast Service Disruption Time

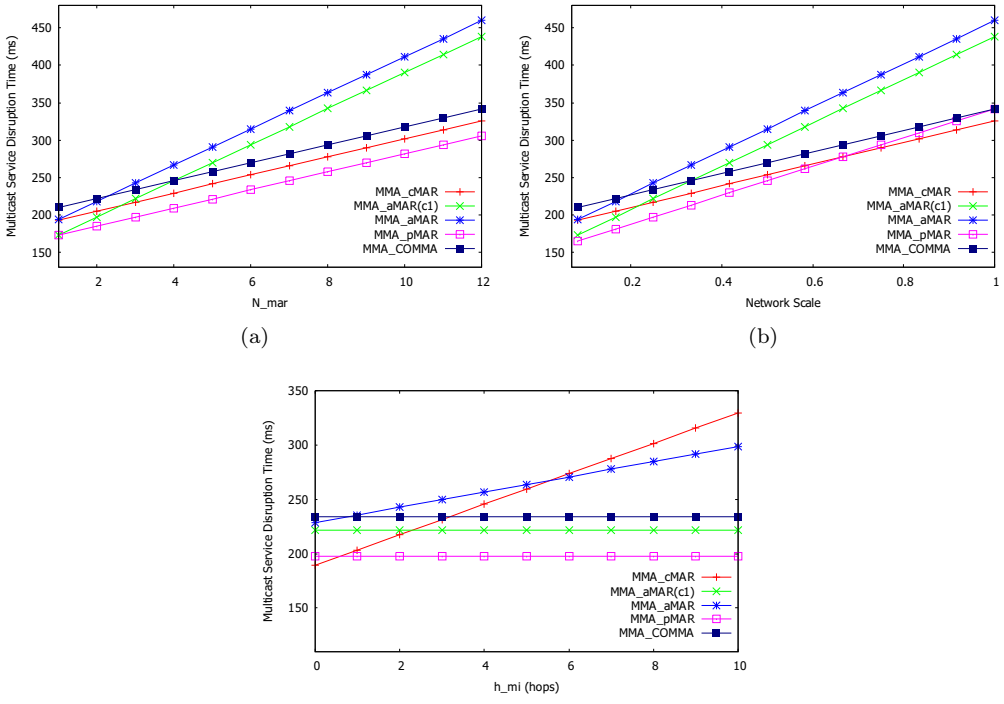


Figure 8.3 – Multicast service disruption time as a function of: (a) N_{mar}, (b) ψ, (c) h_{mi}.

Fig. A.9a shows the multicast service disruption time when N_{mar} is varied over a range from 1 to 12. It appears clearly that the MMA_pMAR approach gives a better performance than the others (lower is better). The service disruption time in the MMA_cMAR is slightly greater than that in the MMA_pMAR since the value of h_{mi} in this case is quite small (2

hops). When N_{mar} is small (less than 5), all approaches satisfy the requirement in terms of service disruption for real-time services (lower than 300ms). When N_{mar} is relatively big, the service disruption in case of MMA_aMAR is significantly increased. We also investigate the impact of the network scale (ψ) on the service disruption time. In this case, N_{mar} is set to a value of 3. In general, the impact of ψ is similar to that of N_{mar}. Especially, Fig. A.9b shows that there is an area where the MMA_cMAR outperforms the MMA_pMAR (when the network scale is larger than 0.62).

Fig. A.9c shows the multicast service disruption time when h_{mi} is varied over a range from 0 to 10 hops. A small value of h_{mi} indicates a high listener density scenario while a high value of h_{mi} represents a low listener density scenario. The service disruption in the MMA_pMAR is lower than that in the others (except when $h_{mi} = 0$ indicating the case where the multicast traffic is already available at the cMAR's upstream MR). As the value of h_{mi} increases, the service disruption time in the MMA_pMAR, MMA_aMAR (c1) and MMA_COMMA is kept constant while that in the other cases is significantly increased. As a result, the difference between the approaches is increased. It comes from the fact that the multicast traffic is already available at the pMAR, aMAR, and COMMA in case of MMA_pMAR, MMA_aMAR(c1) and MMA_COMMA, respectively. Additionally, the service disruption time in the MMA_cMAR strongly depends on the value of h_{mi}. In other words, it cannot be guaranteed in the MMA_cMAR approach. Also, in the MMA_aMAR, it increases significantly compared to that in the MMA_aMAR (c1) as a consequence of using multiple upstream interfaces in DMM.

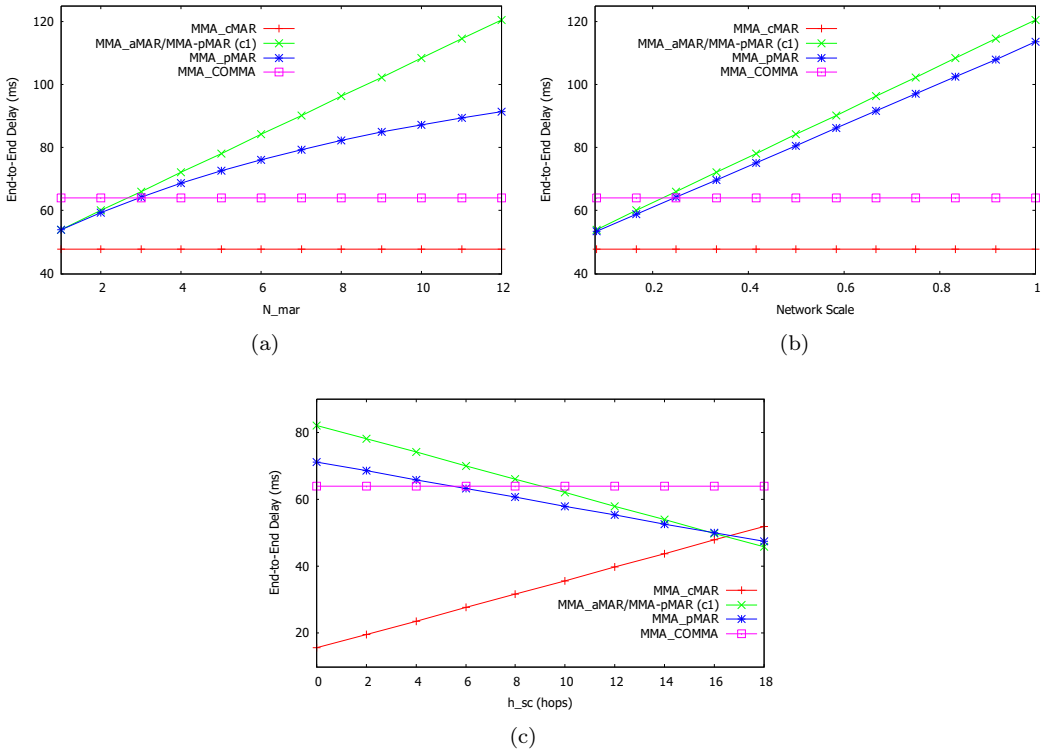


Figure 8.4 – End-to-end delay as a function of: (a) N_{mar}, (b) ψ, (c) h_{sc}.

In conclusion, MMA_pMAR is generally well suited for service interruption sensitive services. Moreover, the service disruption in the MMA_aMAR is always greater than that in the MMA_aMAR (c1). Thus, the increasing of service disruption time, which is caused

by enabling the multiple upstream interfaces for the MLD proxy, can be considered as a trade-off between the service disruption time and the tunnel convergence problem.

8.2.3.2 End-to-End delay

Now we investigate the impact of N_{mar} on the end-to-end delay. Fig. A.10a shows the plot for the end-to-end delay versus the number of handover N_{mar}. As N_{mar} increases (h_{ac} increases) the end-to-end delay in case of MMA_aMAR and MMA_pMAR rapidly increases, while that in MMA_cMAR and MMA_COMMA is kept constant. Note that the end-to-end delay in MMA_cMAR is kept below the value 50 ms. That means the MMA_cMAR satisfies the strict requirement in terms of end-to-end delay (for real-time gaming [201]). The delay in MMA_pMAR(c1) is greater than that in MMA_pMAR as a result of using the multiple upstream interfaces. As can be seen in Fig. A.10b, in general, the network scale has a similar impact on the end-to-end delay as N_{mar}. The major difference is that the increasing line of MMA_pMAR in Fig. A.10b is faster than that in Fig. A.10a. Then, N_{mar} is set to a value of 6 (corresponding to the medium/long-lived and medium/high mobility scenario) while the value of h_{sc} is varied. At this stage, we suppose that $h_{sa} + h_{sc}$ is a fixed value, for example, 18 hops and $h_{sp} = h_{sc}$. This scenario is used to illustrate the case where the source is extremely close to the aMAR (right-side of Fig. A.10c) or extremely close to the cMAR (left side of Fig. A.10c). As can be observed in Fig. A.10c, even when the source is very close to the aMAR (h_{sa}=2, h_{sc}=16), the MMA_cMAR approach gives a better performance in terms of end-to-end delay than the others (lower is better). Thus, the impact of the mobility tunnel (cMAR-aMAR and cMAR-pMAR) on the end-to-end delay is obvious. In conclusion, the cMAR is generally well suited for the delay-sensitive flows.

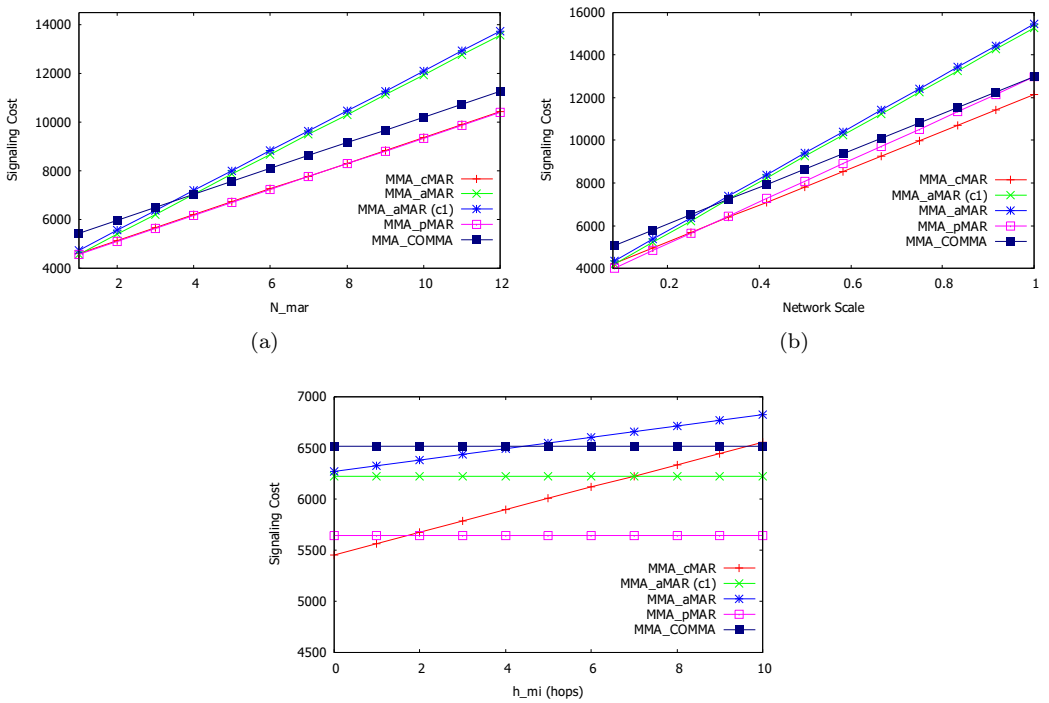


Figure 8.5 – Signaling cost as a function of: (a) N_{mar}, (b) ψ, (c) h_{mi}.

8.2.3.3 Signaling Cost

Fig. A.11 shows the signaling cost as a function of N_{mar}, ψ, and h_{mi}. In general, the signaling cost increases when N_{mar} and ψ increase. In Fig. A.11a, the signaling cost in the MMA_cMAR and MMA_pMAR is lower than that in the other cases. In Fig. 8.5b, the signaling cost in the MMA_pMAR is lowest when ψ is small. Otherwise, it is the lowest in the MMA_cMAR. In both cases, when N_{mar} and ψ are small enough, the signaling cost in case of MMA_COMMA is getting highest. Otherwise, the signaling cost in case of MMA_aMAR becomes highest. As can be seen in Fig. A.11b (when h_{mi} is varied), the MMA_pMAR outperforms the others when h_{mi} is greater than 2.

8.2.3.4 Packet Delivery Cost

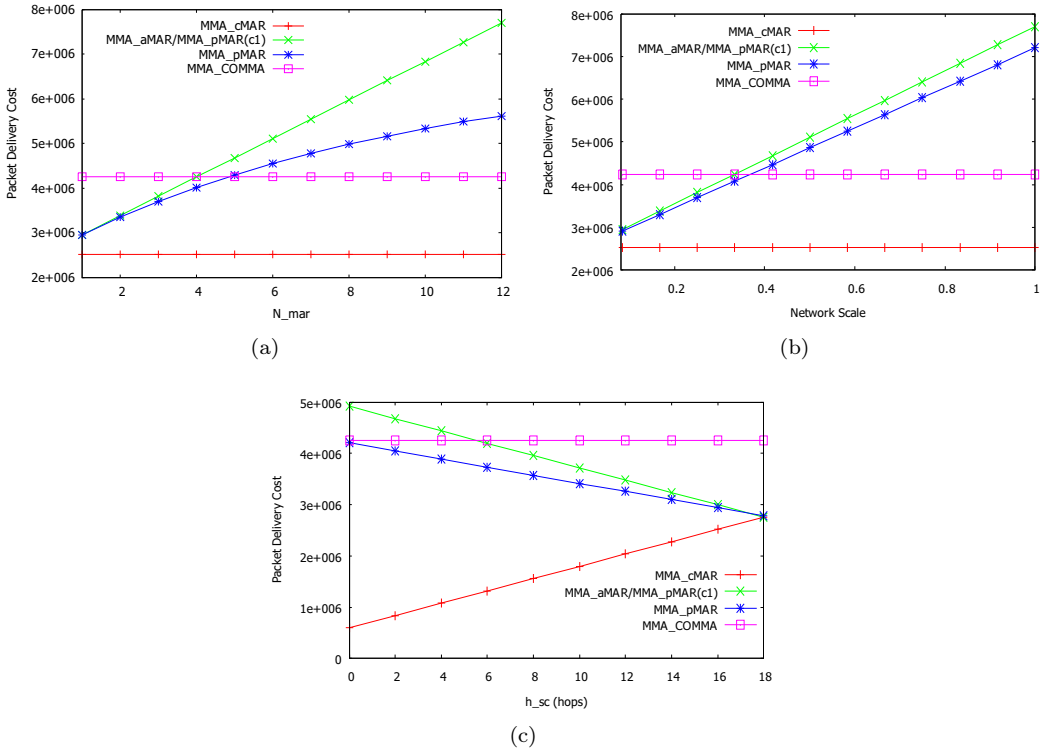


Figure 8.6 – Packet delivery cost a function of: (a) N_{mar}, (b) ψ, (c) h_{sc}.

Similar to the end-to-end delay, the packet delivery cost (as a function of N_{mar} and ψ) in case of MMA_cMAR and MMA_COMMA is kept constant while that in case of MMA_aMAR and MMA_pMAR is greatly increased. Fig. A.12b shows the packet delivery cost as a function of h_{sc} when $h_{sa} + h_{sc}$ is fixed (18 hops). It appears clearly that the packet delivery cost in MMA_cMAR is definitely lower than that in the others, even when the source is very close to the aMAR. Also, we can observe that this cost in case of MMA_pMAR(c1) is greater than that in MMA_pMAR as a result of enabling the multiple upstream interfaces.

8.2.3.5 Tunneling Cost

Regarding the tunneling cost, Fig. A.13 plots the tunneling cost as a function of N_{mar}. The MMA_cMAR does not introduce any tunneling overhead, while the tunneling cost in the

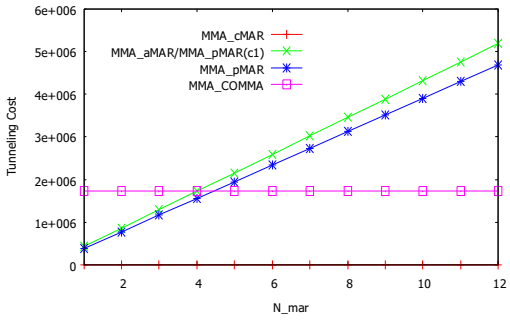
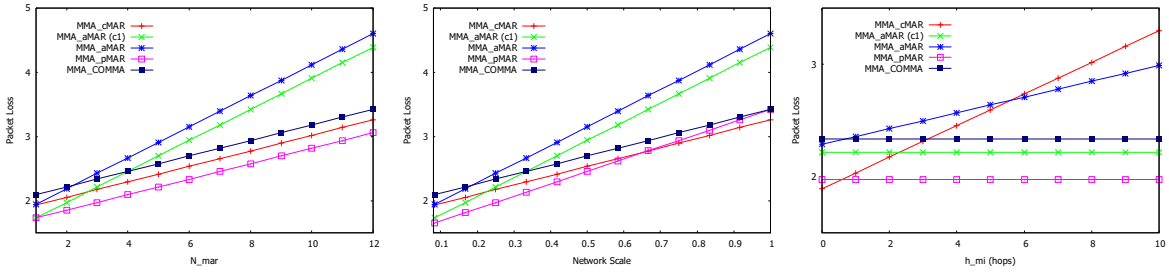


Figure 8.7 – Tunneling cost as a function of N_{mar}.

MMA_COMMA is fixed. On the other hand, it is significantly increased as N_{mar} increases in case of MMA_aMAR and MMA_pMAR. Again, by applying the multiple upstream interfaces, the tunneling cost in case of MMA_pMAR slightly increases.

8.2.3.6 Packet Loss



(a) (b) (c)

Figure 8.8 – Packet loss as a function of: (a) N_{mar}, (b) ψ, (c) h_{mi}.

Fig. 8.8 illustrates the packet loss. Since the number of lost packets during handover is directly proportional to the service disruption time, the shape of the curves is similar to that in Fig. A.9.

8.2.3.7 Expected Number of Handovers

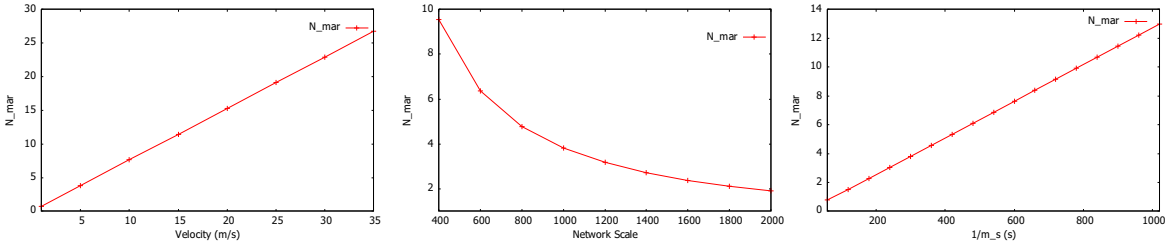
Now we investigate the relation between number of handovers N_{mar}, the velocity and the MAR's coverage area. It is assumed that the subnet residence time (MAR subnet) and the session duration are random variables which follow an exponential distribution with mean value $1/\mu_c$ and $1/\mu_s$, respectively. According to [72], the expected number of handovers is defined as

$$E = \frac{\mu_c}{\mu_s}. \tag{8.37}$$

In this chapter, we consider the case where the MN always moves from MAR to MAR as if they were linearly deployed (the user is moving further away from the first attached MAR and never attaches back to a previously visited MAR, representing the worst-case scenario). Thus, $N_{mar} = E$. Assuming that MAR's coverage area is circular with radius R, then, μ_c is calculated as [72]

$$\mu_c = \frac{2\upsilon}{\pi R}, \tag{8.38}$$

where υ is the average velocity of the MN.



(a) (b) (c)

Figure 8.9 – N_{mar} as a function of: (a) velocity, (b) subnet radius, (c) $1/\mu_s$.

Fig. 8.9a depicts N_{mar} as a function of the velocity when $1/\mu_s$ is fixed to 600s. As the velocity increases, N_{mar} increases. Thus, the high value of N_{mar} corresponds to the high mobility scenario. Then we take a look at the impact of subnet radius R on the value of N_{mar}. The higher value of R means the size of the access network is bigger. As R increases, the residence time in a subnet decreases, thus the number of handover (N_{mar}) decreases (see Fig. 8.9b). Fig. 8.9c plots N_{mar} as a function of $1/\mu_s$ when υ and R are set to 10m/s and 500m, respectively. As $1/\mu_s$ increases, N_{mar} increases. In our analysis, the high value of $1/\mu_s$ illustrates the long-lived flow scenario.

8.2.4 Conclusion of the Quantitative Analysis

From the performance analysis and numerical results, we conclude that none of the approaches is always better than the others. For example, the MMA_pMAR generally is a good choice when considering the multicast service disruption; the MMA_cMAR, in contrast, is a better choice regarding the end-to-end delay. The other approaches can be the most suitable, however, in a specific situation. The performance analysis also gives an idea of using a common MMA (COMMA) which serves as an only multicast anchor for all the nodes in the domain, thus, reflecting the PMIPv6 deployment. Although this approach introduces an acceptable performance, e.g., when N_{mar} and ψ are small, COMMA poses a bottleneck and a single point of failure. It is also not a good choice when a local content is available. As a result, the comparison between the MMA_COMMA and the default mode gives the idea of the performance of DMM with respect to PMIPv6 regarding multicast service.

Basically, the performance of the approaches depends on such factors as the number of handovers (N_{mar}, which can be considered as a function of the velocity and the subnet radius), the network scale (ψ), the position of the source (h_{sc}, h_{sa}) and the listener density (h_{mi}). Those are the reasons why a fixed MMA is not a good strategy. In addition, the daily mobile users spend up to 62% of their time at home and work (in general, typical location) [202]. Thus, in some cases, the typical location would also be a good candidate. Even the mobility anchors are distributed, some of them are overloaded more than the others [200]. As a result, a per-flow multicast support should be provided.

In the next section, a dynamic multicast mobility anchor mechanism will be introduced. Based on the collected contexts, the MMA will be selected dynamically in order to meet a set of requirements. From a service point of view, it helps satisfy the requirements in terms of service disruption and delay, especially when considering real-time services. It

also provides a mechanism to better distribute the load among MARs. Other issues such as packet duplication and leave latency (waste of resource) can be reduced. The MMA selection takes into account not only the multicast service context (e.g., interruption-sensitive and delay-sensitive services) but also the mobile node's mobility context and the network context (such as the load of MARs and the multicast channel policy), thus enabling a per-flow multicast support. In other words, each multicast flow can be treated differently up on the contexts. The MMA selection can be made dynamically when a multicast flow is initiated or when the listener performs a handover thanks to the MLD proxy supporting multiple upstream interfaces.

8.3 Dynamic Multicast Mobility Anchor Selection

To mitigate the issues caused by the movement of a listener following the multicast default mode, this section proposes a mechanism which allows dynamically selecting and using the appropriate MMA among the candidates, namely dynamic multicast mobility anchor mechanism or DMMA. This idea follows the assumption of the DMM protocol specified by the IETF [203]. The MMA selection can be made whenever the listener performs a handover or a multicast flow is initiated. As a result, the tunnel convergence problem is completely avoided.

To dynamically select the appropriate MMA, different contexts should be taken into account as the multicast service context (e.g., interruption-sensitive, delay-sensitive, and long-lived/short-lived flow), the MN's mobility context (high/low mobility)[2], and the network context (like load of MARs, geographical proximity, and multicast channel policy). Each context can be assigned with a priority number. For example, a lower value indicates the more important context.

At this stage, similar to the default mode, when a listener initiates a multicast flow, the cMAR will act as the MMA for this flow (the multicast traffic will be received directly from the native multicast infrastructure). This means the MMA selection in the initial phase will be left for future works. For a handover flow, the multicast traffic can be received from the aMAR, the pMAR, the cMAR, or even an MAR in which the multicast channel is already available, or a less loaded MAR so as to meet a set of requirements. In addition, we consider the typical location (tMAR) corresponding to the MMA_tMAR approach.

Our solution is not only for the service disruption and the end-to-end delay issues, but also for another multicast related issues. Thus, it can offer such benefits as:

- *A complete solution* for most of the multicast listener mobility-related issues (including service disruption, tunnel convergence problem, leave latency (network resource waste), sub-optimal routing and packet loss);
- *Route optimization*: The multicast flows will be routed in a better route since they do not always pass through their mobility anchor.
- *Tunnel convergence problem avoidance*: This solution can fully resolve the tunnel convergence problem;
- *Dynamic utilization of mobility tunnel*: The utilization of mobility tunnel for the ongoing multicast sessions is enabled in appropriate cases e.g., for remote content, or for a channel with strict delay requirements;

[2]The MMA selection also depends on the role of the node in the multicast session (source or listener).

- *Effective tunnel management*: In a DMM environment, it is unfeasible to pre-establish all the tunnels between MARs since the number of MARs is supposed to be large. By enabling the multiple upstream interfaces in DMM, it may cause the complex tunnel management (e.g., maintenance of the tunnel and keep alive signaling). Thus, the proposed solution, which is based on the multicast mobility management module, can help to solve this issue;
- *Multicast flow load distribution*: Since the MMA selection takes the current load of the MARs into account, it helps better distribute the multicast traffic load among MARs.
- *Centralized channel management*: The central entity (Multicast Control Entity, or MCE) collects and manages the considered contexts (e.g., the multicast channels and their scope (local or remote), thus enhancing the control of network providers;
- *Possibility to be applied with multicast source mobility*;
- *Compatibility with unicast mobility.*

8.3.1 Considered Contexts

Multicast service context When services are sensitive to interruption or packet loss, the service disruption time should be minimized. For instance, it should be less than 300ms for a real-time service, while 500ms for a normal one [162]. For the end-to-end delay-sensitive service, the long mobility tunnel, which can result in a high end-to-end delay, should be avoided. ITU-T Recommendation G.114 [204] suggests that if one-way transmission time for connection delays can be kept below 150ms, most applications will experience a transparent interactivity. Moreover, the long-lived flows may perform many handovers while the short-lived ones seem to be initiated and terminated at the same MAR without performing any handover. Even if a short-lived flow could make it, it is expected that the flow does not last long after the handover.

Mobile node context A mobile node with high mobility performs frequent handovers. In this case, almost all ongoing multicast flows are the handover ones which may cause the longer tunnel. If the multicast traffic is always routed through the aMAR, the longer dwell time is, the more serious the impact will be. Also, the number of anchors and tunnels may be increased. On the contrary, for the low mobility node, the MN is expected to stay at one or several MARs most of the time. Since the users spend most Internet usage time at their typical locations (tMAR), in some cases, the tMAR can be a good candidate.

Network context The MMA selection can also be based on several network contexts such as current load of the MARs, geographical proximity of the MAR to the MN as well as the multicast channel policy[3]. For example, when the load of MAR is high, it may cause long delays and packet losses if it is selected as the multicast anchor. In this case, the least loaded MAR (among the MARs having the multicast forwarding state for this channel) can be a potential candidate. The reason lies in the fact that if the channel is already available at the selected MAR, the service disruption time can be minimized (no need extra time to join the multicast channel). Also, with a negligible increase of load, this MAR can forward the traffic to the cMAR [28].

[3]The network operator can define the channel policy in which some channels should be received directly from the native multicast infrastructure (to gain benefit from local content) while the others from their anchor MAR [20]

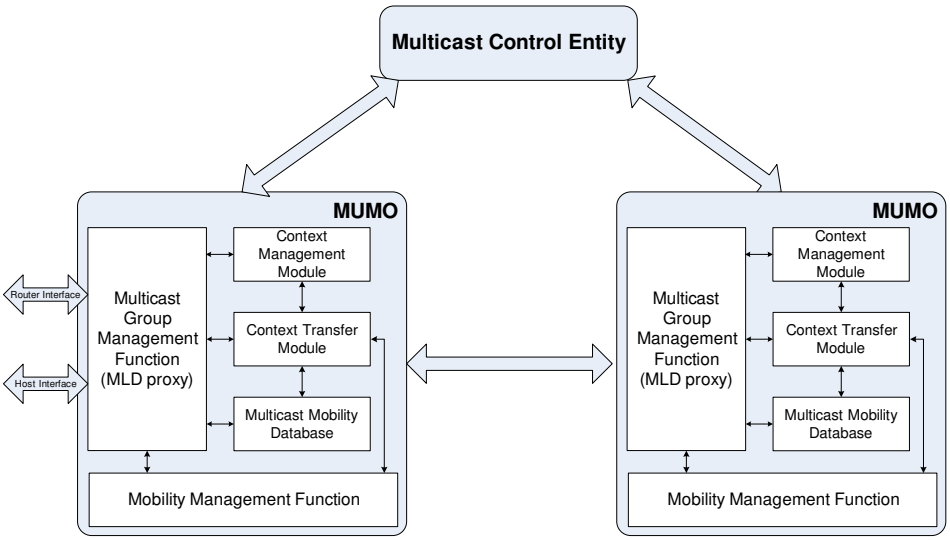


Figure 8.10 – Multicast mobility management module (MUMO) in the MAR.

8.3.2 Architecture Description

In order to collect and manage the considered contexts, a network entity, called Multicast Control Entity (MCE) is introduced. The MCE can be collocated with the CMD. The MAR periodically updates the MN context and MAR's current load to the MCE by using an extension of PBU/PBA (or an extension of the Heartbeat messages [205]). The MCE also manages all the multicast channel in the domain for network policy configuration. The service context can be defined based on the QoS class.
Residing in the MAR, the multicast mobility management module (MUMO) takes responsibility for all actions related to the multicast mobility. The structure of this module is depicted in Fig. A.14 and briefly described as follows:

- The multicast group management function (MGMF) refers to the multicast group management operations and information storage, which is developed based on the MLD proxy with multiple upstream interfaces[4]. This module also supports the multicast explicit tracking function in order to keep a per-host multicast membership state [51]. It is done based on its Multicast Mobility Database (MMD), which stores entries with the following information: i) MN's identifier (MN_ID); MN's address; and multicast subscriptions (aligned with the structure of MLD multicast information). Besides, it holds a counter structure for the number of listeners per IP multicast channel, allowing it to identify when a node is the last subscriber of a group. This information is in particular essential for a proper multicast context transfer operation.
- The context management function (CMF) communicates with the MCE to retrieve the channel configuration information including the address of the corresponding MMA, and MMA type (i.e., the previous, anchor, and current MAR or another). Based on this information, MLD proxy configures its upstream interfaces towards the corresponding MAR.
- The multicast context transfer function (MCTF) is responsible for exchanging the MN's multicast subscription information between MARs. So that the new MAR can join the on-going flows in advance to minimize the service disruption.

[4]This module can also be relied on the multicast router function e.g., MRDv6.

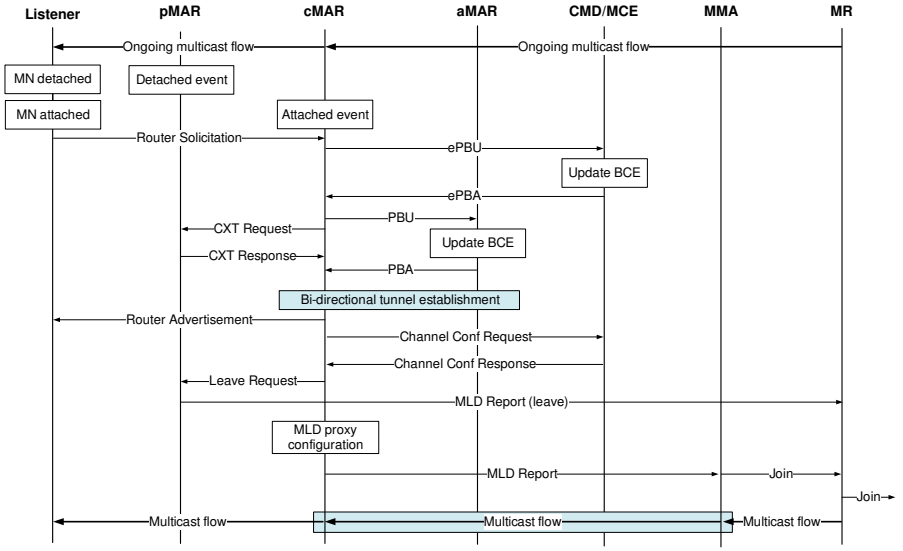


Figure 8.11 – Multicast-related handover signaling with the multicast context transfer.

- The mobility management function (MMF) resembles the mobility protocol stack. It is responsible for assigning and maintaining the IP connectivity of an MN roaming inside the DMM domain. In other words, it is responsible for all the mobility management-related actions.

8.3.3 Operations of the Solution

The operations of the solution are briefly introduced as follows. Once the MN enters a DMM domain (attaches to MAR1), a network prefix is allocated to it (say Pref1). MAR1 then sends a PBU message including the MN's identifier (MN_ID) and Pref1 to the CMD to register this MN. After receiving the PBU, the CMD creates a BCE which consists of the MN_ID, the Pref1, and the address of MAR1 (as aMAR) for this MN. In response, the PBA message is sent from CMD to MAR1 to inform that the location of the MN is updated. MAR1 then sends a Router Advertisement including the allocated prefix to the MN. The MN, after configuring its IPv6 address, can join a multicast flow via the cMAR (MAR1).
In case of handover (see Fig. A.15), the cMAR allocates a new network prefix for this MN (called Pref2). The cMAR then sends a PBU to the CMD for the new prefix registration. This message includes the MN_ID, the new prefix allocated at the current MAR (Pref2). By looking up the BCE table, the CMD updates the entry corresponding to the MN_ID with the current location of the MN. The CMD then replies by a PBA including the list of addresses of the anchors, the corresponding prefixes, and the address of the previous MAR. Upon receiving this message, the cMAR exchanges the PBU/PBA messages with the anchor MARs to update the current location of the MN. Thus, the bi-directional tunnel is established between the cMAR and the aMAR, if necessary. The cMAR then sends a RA message including the new prefix allocated to the MN. The MN, upon this prefix, can configure its IPv6 address and start a new communication with the CN. In parallel, the multicast context transfer messages are exchanged between the cMAR and the pMAR allowing the cMAR to obtain the ongoing multicast flows of the MN. Based on this information, the cMAR contacts with the MCE to get the channel configurations which consist of the following information (per channel): S, G, MMA's address, and a field indicating the

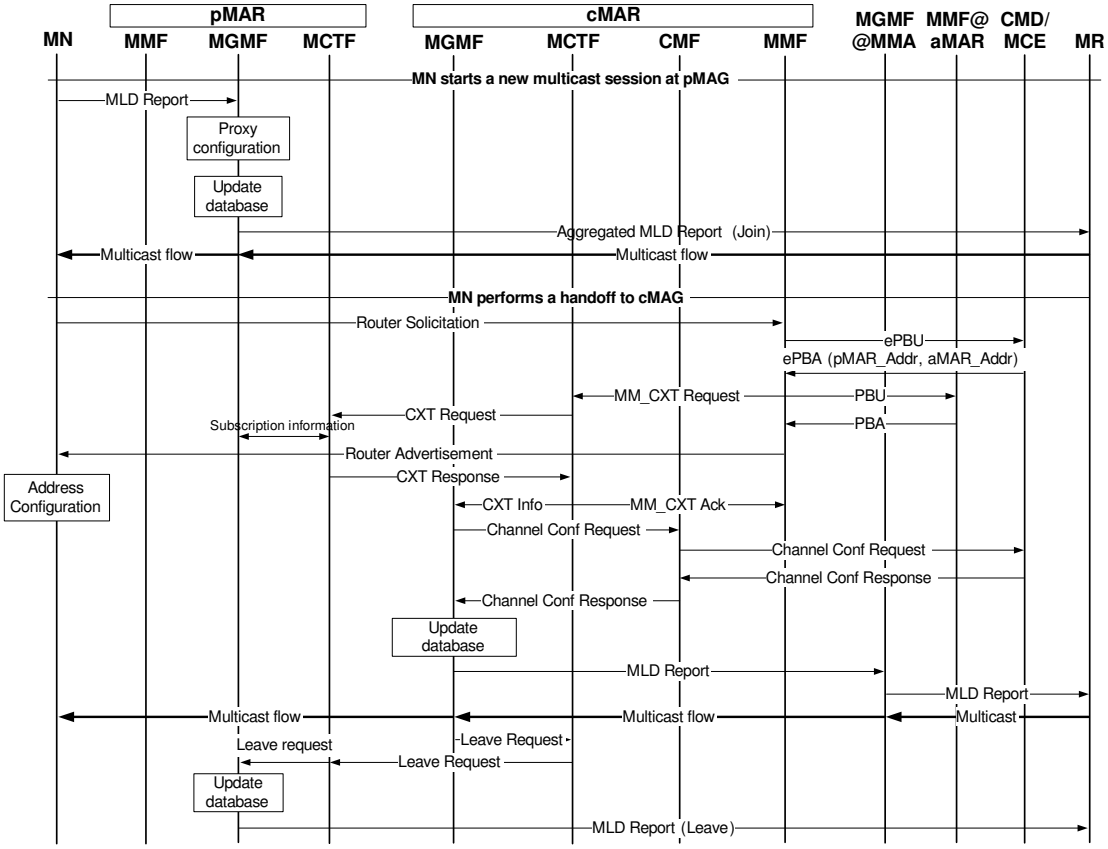


Figure 8.12 – Multicast-related handover signaling: Interactions between the modules.

role of MMA (e.g., 0 for cMAR, 1 for pMAR, 2 for aMAR, 3 for COMMA, 4 for tMAR, and 5 for others). The PBU/PBA messages can be extended to convey the channel configuration information. The cMAR then configures an upstream interface towards the MMA, and sends an MLD report to the MMA to join the ongoing multicast channel. After joining the multicast delivery tree (if necessary), the MMA forwards the multicast packets to the cMAR, and they finally reach the MN. If the cMAR does not get the multicast traffic from the pMAR, it will request the pMAR to stop forwarding the channel. Thanks to the explicit tracking function, the pMAR stops forwarding the channel if the MN is the last member of the channel. Thus, it shortens the leave latency and reduces waste of resources. The operation in details is illustrated in Fig. 8.12 (Further information on the interactions between modules inside MUMO can be found in [20, 161]).

8.3.4 Other Considerations

To reduce the complexity of MCE and the signaling cost for the context collection process, two possible enhancements can be considered as follows:

- The mobile node's and the multicast service contexts can be collected and managed by the CMF module while the MCE is responsible for managing the network context[5].

[5]Also, in case of the fully distributed scheme, the MCE functionality will be responsible by the CMF in a distributed manner

- The MCE can store the MN's subscription information but only for the channels with strict requirement in terms of service disruption and end-to-end delay. For those channels, the MMA selection will be taken by the MCE while for the normal channels, it is done by the MUMO at the cMAR. As a result, for the channels with the strict requirement, the channel configuration will be conveyed via the extended PBA from the CMD/MCE to the cMAR.

8.3.5 Performance Evaluation

Compared to the performance analysis in the previous section, the DMMA may introduce an extra delay to the lowest value of the multicast service disruption (from the channel configuration acquisition process). The additional delay is calculated as

$$T_{AD} = max\{T_{CXT} + T_{CF}, T_{LU}\} - max\{T_{CXT}, T_{LU}\}, \tag{8.39}$$

where T_{CF} is the time needed for the channel configuration acquisition, and is given by

$$T_{CF} = d_{wd}(L_{CF-Req}, h_{cd}) + d_{wd}(L_{CF-Res}, h_{cd}). \tag{8.40}$$

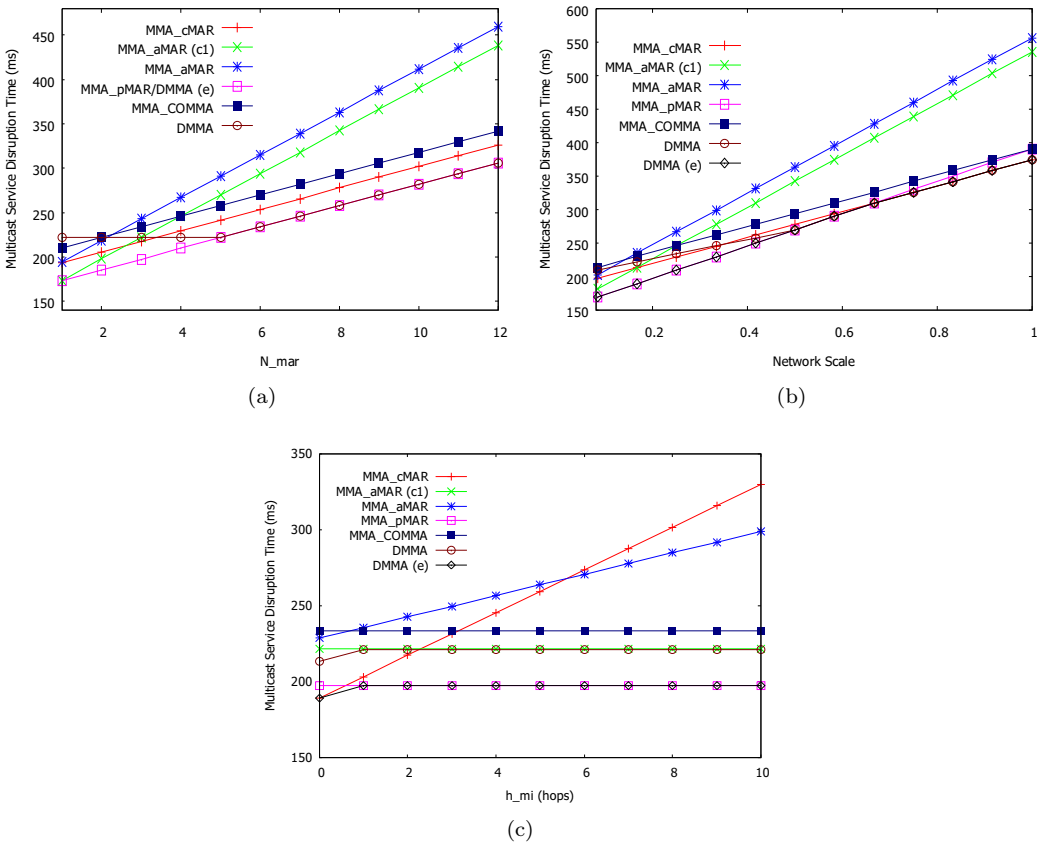


Figure 8.13 – Multicast service disruption time in DMMA: (a) N_{mar}, (b) ψ, (c) h_{mi}.

When applying the first enhancement, the cMAR will be responsible for the MMA selection, thus, there is no need for the channel configuration acquisition. Similarly, in the second enhancement, the channel configuration information can be conveyed in the PBA message from the CMD to the cMAR. As a result, in both cases the DMMA does not introduce any

additional delay. Fig. 8.13a shows the performance of the DMMA solution compared to the other approaches regarding the multicast service disruption time.
Also, the DMMA does not introduce any extra delay regarding the end-to-end delay. The same thing happens in case of packet delivery cost, tunneling cost and packet loss. In other words, the lowest value in the end-to-end delay, packet delivery cost, tunneling cost and packet loss is set to the corresponding value of DMMA.

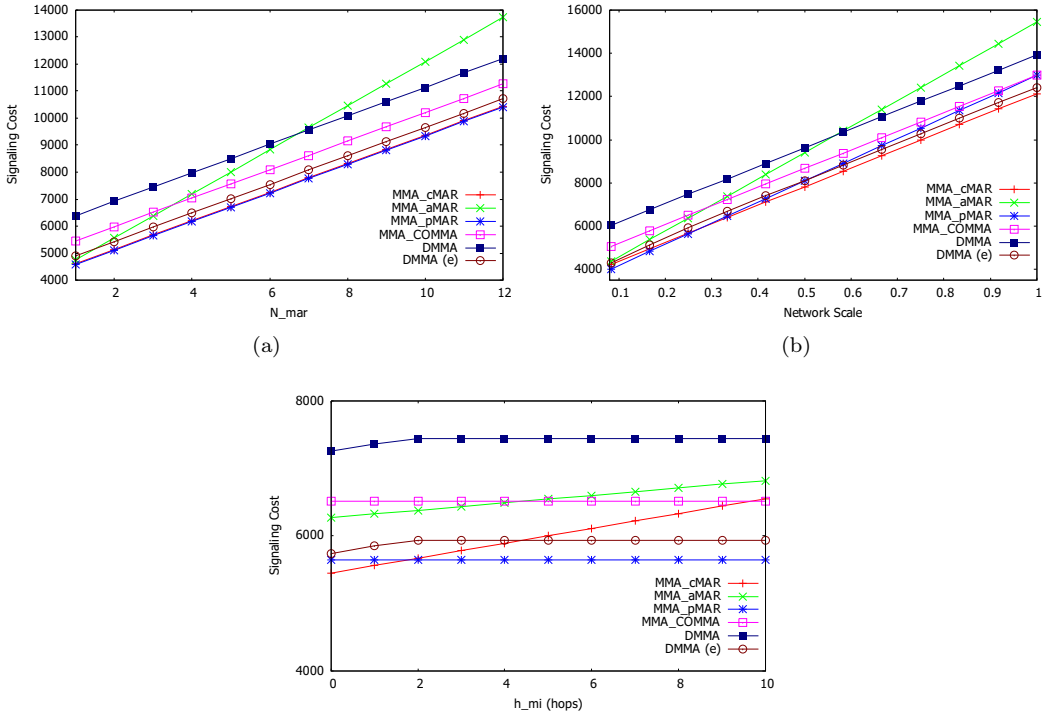


Figure 8.14 – Signaling cost in DMMA: (a) N_{mar}, (b) ψ, (c) h_{mi}.

Regarding the signaling cost, the additional cost is calculated as

$$SC_{AD} = \alpha L_{CF-Req} h_{cd} + \alpha L_{CF-Res} h_{cd} + \alpha L_{leave} h_{pc}, \tag{8.41}$$

where L_{leave} is the size of the leave request message sent from the cMAR to the pMAR, which is 96 bytes. When applying these enhancements, the additional cost is only derived from the leave request message. Fig. 8.14 shows the performance of the DMMA solution compared to the other approaches regarding the signaling cost. The signaling cost in case of DMMA is quite high compared to that in the MMA_pMAR and MMA_cMAR. On the contrary, in case of DMMA (e) it is slightly higher than the lowest value as an acceptable cost for the reduction of other metrics (service disruption time, end-to-end delay, packet delivery cost, tunneling cost).

8.4 Discussions

8.4.1 Implementation Work

An early version of the DMMA was available thanks to the Medieval project [161, 206, 23]. In this implementation, the context management module (CMF) executes in a simple way:

when the MN acts as a multicast listener, the cMAR always plays the role of the MMA. On the contrary, the aMARs acts as the MMA when the MN plays the role of a multicast source. However, the procedures for the considered contexts acquisition are still under development. Aslo, the MMF module is being developed based on the OAI PMIPv6 implementation. The other modules i.e., MGMF and MCTF are already available as described in Chapter 3 and Chapter 4. In the next step, the full implementation of the CMF module will be deployed. Experiments then will be conducted based on the testbed using the method described in Chapter 3.

8.4.2 Multicast Router Function Deployment at MAR

Our analysis can also be applied when the multicast router function is deployed at MAR. As in the Medieval project, the MGMF represents the functionality of a multicast router (e.g., based on MRD6 implementation). In this case, the Multicast Routing Information Base (MRIB) can be not only based on the unicast RIB, but also on the information from the CMF. For example, in order to set the pMAR as the upstream multicast router for a specific channel (say C1), the cMAR uses an explicit PIM join message to join the C1 at pMAR. In other words, pMAR becomes a RPF neighbor router of the cMAR regarding the channel C1.

8.4.3 Multicast Source Mobility Support

At this stage, our solution can also support source mobility in DMM. However, the aMAR will always act as the MMA for the source to avoid the potential impact on the service disruption. In case of ASM, an extension of PIM-SM [207] can be used to route the multicast traffic directly from the cMAR to the RP bypassing the aMAR. Thus, the multicast traffic is routed in a better way. In more details, the explicit reserve path forwarding (RPF) mechanism is used to build the multicast delivery tree via an explicitly configured path included in the PIM join messages. After receiving the unicast-encapsulation packets from the current MAR, the RP will send a Join message including the address of the sender (cMAR's address) in a new type-length-vector (TLV). It allows the RP to establish the shortest path tree towards the current location of the source. The native multicast traffic then will be sent via the new delivery tree from the cMAR and reaches the listeners (PIM phase two).

8.5 Conclusion

In this chapter, we have presented a performance analysis for different approaches to support the multicast listener mobility in DMM. The analytical results can be very useful in the design of IP mobile multicast solutions in a DMM environment. We argued that, under certain scenarios, it is hardly possible to achieve the requirements in terms of service interruption and delay for specific services (e.g., real-time service). We then introduced a dynamic multicast mobility anchor mechanism in order to mitigate these issues. This mechanism takes into account various contexts ranging from the multicast service, the mobile node's mobility to the network context, thereby, enabling a per-flow multicast support. Numerical results showed that for each scenario these requirements can be satisfied. Also, several benefits can be offered such as tunnel convergence avoidance, effective tunnel management, route optimization and waste of resource reduction.

Conclusion of Part III

In Chapter 7, a solution for inter-domain mobility for PMIPv6 has been presented. As DMM is still under discussion, it will not be deployed soon. In addition, since PMIP is widely accepted, the inter-domain PMIPv6 which is based on DMM concept can be considered as a step towards the deployment of DMM. The proposed solution allows the data packets to be routed via a near-optimal way by bringing the mobility anchors closer to the MN while the control management can be placed anywhere in the network. A basic mechanism for the listener mobility in an inter-domain environment was also introduced. It helps keep the MN unaware of mobility with an acceptable service disruption.

In Chapter 8, a dynamic multicast mobility anchor selection has been proposed in DMM. This mechanism takes into account various contexts ranging from the multicast service, the mobile node's mobility to the network context, thereby, enabling a per-flow multicast support. From a multicast service perspective, it helps satisfy a set of requirements in terms of service disruption and delay. Several benefits can also be offered such as tunnel convergence avoidance, effective tunnel management, route optimization, waste of resources reduction and multicast flow load distribution.

9
Conclusions and Outlook

9.1 Conclusion

The data volume in mobile networks is booming mostly due to the success of smartphones and tablets. Based on the fact that the mobile Internet traffic will be dominated by the mobile video, the scalability and bandwidth efficiency from multicast routing makes the IP multicast play more important role. However, when considering IP multicast in a wireless mobile environment, it raises several issues such as service disruption, end-to-end delay, packet duplication, non-optimal routing and waste of resource.
To tackle these issues, this thesis proposed the solutions in both PMIPv6 and DMM environments. Through this dissertation, the following objectives are achieved:

- *Identify the issues and challenges of IP mobile multicast and the evaluation metrics for IP mobile multicast*: In the scope of this thesis, we just highlight such issues as the multicast service disruption, non-optimal routing, end-to-end delay, packet duplication and waste of resource (leave latency) issues.

- *Propose an experimental method to achieve the realistic results at a low cost*: The proposed experimental method is a combination of the virtualization and the simulation technique. Based on this study, a PMIPv6 testbed has been implemented.

- *Present an effective method for optimizing the service continuity in PMIPv6 and deploy a near-to-real PMIPv6 testbed for IP mobile multicast*: The proposed solution is based on the multicast context transfer and the explicit tracking function allowing the new MAG to obtain the MN's subscription information in advance, thus reducing the multicast service disruption. The testbed allows simulating the mobility of multiple sources and listeners at the same time. Additionally, all modules deployed in the testbed can be used in a real one.

- *Propose a load balancing mechanism of multicast flows in PMIPv6*: The proposed solution helps better distribute the load among LMAs to improve the scalability and reliability of the system.

- *Introduce a solution for handover of a multihomed node in heterogeneous networks*: Logical interface is used as an abstract layer to hide the change of the physical interface to the IP stack. Thanks to this mechanism, the MN remains unaware of mobility from the multicast service point of view.

- *Present an inter-domain mobility support for PMIPv6 networks and a basic support for multicast listener mobility in an inter-domain environment*: The solution allows

the data packets to be routed via a near-optimal way by bringing the mobility anchors closer to the MN while the control management can be placed anywhere in the network.

- *Propose a dynamic multicast mobility anchor (DMMA) mechanism in DMM*: The DMMA not only helps the services to satisfy the strict requirement in terms of service disruption and end-to-end delay, but also offers such benefits as tunnel convergence avoidance, effective tunnel management, route optimization, waste of resource reduction and multicast flow load distribution.

Benefit of the Solutions - Application to Real System and Projects A part of the dynamic multicast mobility anchor (DMMA) has been implemented in the MEDIEVAL project[1]. This project aims at providing an architecture to enhance the current mobile Internet and deliver more efficiently mobile video applications. A cross-layer solution has been developed in which two typical services related to multicast are considered i.e., Mobile TV and PBS. Regarding the multicast mobility support, a solution for both multicast listener and source in a DMM environment has been provided. As a part of the overall solution, the multicast mobility module which manages the IP mobility support for the multicast flows has been implemented. In more details, the multicast context transfer and the explicit tracking function are used to accelerate the MN's subscription acquisition process to reduce the service disruption time. For the listener, the multicast packet is always received directly from the multicast infrastructure at the current MAR. For the source, the multicast packet is routed from the current MAR to the anchor one via the mobility tunnel. The real testbed has been deployed to conduct the experiments. The experimental results showed that a small amount of packet loss was observed. Therefore, the session continuity of the video player was possible, with an almost imperceptible handover [23].
In the VELCRI project, the solution for handover across heterogeneous networks is one part of the communication system (including Vehicle-to-Grid and Grid-to-Vehicle) to provide the charging service for the EV (Electric Vehicle Charging Services - EVCS). The communication system allows the EV to be always connected to the Smart Grid using different wireless technologies in different phases such as LTE while driving, WLAN while approaching a charging station, and PLC while being docked at a charging station.
In the SYSTUF project[2], the DMMA will be used to provide the multicast service for the users on the public transports e.g., tram and metro. In more details, the goal of the project is to define and implement new services and broadband end-to-end communication system between ground and moving vehicles to improve the quality of urban guided transports. The DMMA will be considered in a high mobility scenario. Also, the mobility predictions can be used to improve the performance of the DMMA.

9.2 Perspectives and Future work

With the desire to support IP multicast services in a wireless mobile environment, this thesis proposed the solutions for the IP mobile multicast-related issues. However, due to the wide range of the topic defined, several aspects could not be analysed in details, which may potentially be improved. For example, while the focus of this thesis so far has been on the multicast listener mobility, similar idea can be applied for the source mobility. Also, more multicast routing protocols should be investigated e.g., Bidirectional Protocol Independent Multicast (BIDIR-PIM).

[1]MEDIEVAL project, Homepage: http://www.ict-medieval.eu
[2]SYSTUF project: http://systuf.ifsttar.fr/index-en.php

Another topic, which would be considered, is the mobility of the node. More mobility models would be applied to study the impact of mobility pattern on the performance of the solution. It can be done by using the existing mobility model in NS-3.
As the proposed solution in Chapter 8 was only validated by the mathematical analysis, a DMM testbed is being deployed using the method described in Chapter 4. Additionally, mobility predictions can be used to improve the performance of the DMMA which allows selecting the suitable multicast mobility anchor not only when performing a handover but also at the time the multicast flow is initiated.
The growing interest in LTE technology by operators brings Multicast/Broadcast Multimedia Service (MBMS) and MBSFN (Multicast/Broadcast over a Single Frequency Network) back to the agenda to support the exponential increase of multimedia distribution services over cellular networks in the next few years. As we do not consider any specific wireless access technology, the IP mobile multicast would be considered in the 3GPP architecture.
In the future, billions of vehicles will be connected to the networks, that creates both new challenges and opportunities for the network operators. Therefore, the DMMA mechanism should be considered, for example, for users on the high-speed vehicles (in the context of NEMO).
Last but not least, we should put our solution in the relation with other technologies e.g., Software Defined Networking (SDN), Internet of Thing (IoT) and Cloud Computing. For example, the SDN techniques can change mobile core networks and allow for an optimized distributed deployment of virtualized instances of mobile gateways. This could make much more flexible way to process IP packets and flows. Besides, since IoT applications including Intelligent Transport System (ITS) attract great interests recently, mobility support in IoT is also gaining a lot of momentum. On the other hand, the cloud and the benefits of cloud computing continue to gain significant momentum. Since applications running on clouds are rich media enabled, or collaboration applications, IP multicast can offer benefits to the users as well as to the network operators [208]. Also, sharing the Cloud Computing infrastructure among different network operators also influences the development scenario of DMM [209].

Appendix A
Résumé de la Thèse en Français

A.1 Introduction

Avec le développement de la technologie d'accès sans fil ainsi que l'explosion des appareils mobiles (tels que les smartphones et les tablettes), le réseau mobile de prochaine génération n'est pas seulement limité à fournir des services vocaux traditionnels, mais aussi des services de données. En d'autres termes, il évolue vers des systèmes tout-IP. En fait, les services de données mobiles sont devenus une partie essentielle de la vie de nombreux consommateurs [1, 2]. Par conséquent, le trafic de données mobiles a été presque doublé chaque année au cours de ces dernières années [1, 6]. Cette tendance devrait se poursuivre dans les années à venir, notamment avec le déploiement des réseaux de quatrième génération (4G). Malgré l'augmentation du volume de trafic, le chiffre d'affaires moyen par utilisateur est en chute libre [7]. En outre, les nœuds mobiles peuvent souvent changer leur point d'attache au réseau. La gestion de la mobilité IP est donc un concept essentiel pour répondre à la demande de connectivité d'Internet omniprésente ainsi que des nouvelles exigences en matière de services, tels qu'un handover transparent sur des réseaux hétérogènes, une qualité constante de l'expérience et des contraintes strictes de retard.

Dans ce contexte, MIPv6, le premier protocole de mobilité normalisé par l'IETF pour les réseaux IPv6, maintient l'accessibilité du terminal mobile quand il est loin de la maison. En d'autres termes, MIPv6 permet de communiquer avec un terminal mobile quelque soit l'endroit où il se trouve. Il se fait par l'introduction d'une entité centrale, à savoir l'Agent Mère (Home Agent - HA) situé au réseau de la maison d'un nœud mobile (mobile node - MN), ce qui est un point d'ancre topologique de l'adresse IP d'origine du MN (l'adresse du domicile - Home Address). Grâce à son adresse du domicile, le MN peut communiquer indépendamment de son emplacement actuel dans l'Internet. Cependant, dans MIPv6, le MN doit effectuer la signalisation liée à la mobilité, cela signifie que la pile de protocole MIPv6 est nécessaire au MN. Il est le principal obstacle au déploiement de MIPv6 dans le monde réel. Pour cette raison, PMIPv6, comme un protocole de gestion de la mobilité basée sur le réseau, permet d'éviter la mise en place supplémentaire dans le MN de sorte que le MN peut être simple. En d'autres termes, la mobilité peut être transparente offerte à tous les MNs existants.

Les opérateurs des réseaux mobiles sont mis au défi par l'augmentation du trafic de données mobiles (en particulier le trafic de vidéo) et les nouvelles exigences, par exemple, fournir une connectivité partout et à tout moment avec la cohérence de l'expérience d'utilisateur, tout en préservant l'économie de leurs réseaux et de créer de nouvelles opportunités pour la croissance de revenus. Face à ces défis, les opérateurs cherchent des solutions innovantes pour améliorer la performance et l'efficacité du réseau, ainsi que réduire le coût dépensé sur le fonctionnement et la maintenance du réseau. Deux axes majeurs sont: i) l'augmentation

de la capacité de système de communication sans fil; et ii) la conception et la mise en œuvre d'un système efficace de transférer de données. En ce qui concerne le premier aspect, l'augmentation dramatique de la capacité des réseaux radio du haut débit viendra avec la mise en œuvre de nouvelles technologies sans fil telles que WiMAX, HSPA, et LTE. Cependant, le spectre pour les opérateurs est à la fois limité et trop cher. Ainsi, ils cherchent à différentes méthodes pour augmenter la capacité du système comme le déploiement des cellules femto et pico, et la sélection du trafic déchargé entre les spectres sans licence. Regardant le deuxième aspect, l'objectif est de simplifier l'architecture de réseau, ainsi que d'optimiser le coût de transmission de données. En conséquence, le réseau mobile est en train d'évoluer vers une architecture plate. Un exemple est l'architecture LIPA/SIPTO définie par le 3GPP. Suivant la même idée, l'IETF a récemment affrété un groupe de travail de gestion de la mobilité, appelé DMM (Distributed Mobility Management), qui précise les solutions pour résoudre les problèmes et les limites de la gestion de la mobilité centralisée. En fait, la gestion de la mobilité IP traditionnelle (par exemple, MIPv6 et PMIPv6) s'appuie sur l'approche de gestion de la mobilité centralisée, donc, soulève plusieurs problèmes pour les opérateurs tels que l'utilisation inefficace des ressources, une mauvaise performance, et le problème d'évolutivité lorsqu'on considère un grand nombre des appareils mobiles et leur demande de trafic [8, 9, 10]. DMM est une des solutions pour aider les opérateurs mobiles à répondre à ces limites.

Comme l'Internet est largement déployé et répartis sur une grande surface, il offre une grande variété de ressources communs et de services d'information communs. Dans un monde partagé, le service de communication de groupe, qui se réfère à la capacité d'envoyer de données à plusieurs récepteurs en même temps, naturellement deviens de plus en plus important, en particulier dans certains domaines comme la distribution de multimédia, les jeux et les services financiers, etc. Dans ce contexte, l'évolutivité et la bande passante efficacité du routage multicast rend multicast une remarquable solution du point de vue de l'application pour faire face à un grand nombre de trafic (notamment, dans des environnements mobiles où les utilisateurs partagent généralement des bandes de fréquences et la capacité limitée [11]). Mais l'un des principaux défis pour le support de multicast est lorsque la mobilité est considérée. Il vient du fait que les protocoles de multicast ont été crées pour les réseaux fixes. En tant que tel, il soulève des problèmes à cause de l'interaction entre les protocoles de multicast et les protocoles de mobilité IP. Ces problèmes sont l'interruption de service, la perte de paquets, le gaspillage de ressources, le routage non optimal, et la duplication de paquets.

En ce qui concerne la mobilité multicast IP, après plus d'une décennie d'efforts de recherche et développement, nombreuses approches ont été proposées, mais la plupart d'entre eux sont basés sur les protocoles de gestion de mobilité basés sur le client comme MIPv6. Cependant, le principal inconvénient de ces protocoles est qu'ils nécessitent le MN pour modifier sa pile IP pour participer dans le processus de signalisation de mobilité. En outre, les approches antérieures multicast IP ne peuvent pas être appliquées directement à une gestion de mobilité basée sur le réseau, dans lequel le MN n'est pas au courant de processus de la mobilité. Pour résoudre les problèmes mentionnés ci-dessus, l'IETF a travaillé dans différentes solutions mettant en évidence la différence entre la source et l'auditeur. Cependant, les solutions proposées restent incapables de résoudre les problèmes de l'évolutivité, de l'optimisation de la performance et la compatibilité avec la mobilité unicast en même temps. En DMM, il n'y a pas de solution complète pour la mobilité du terminal multicast.

Il est généralement reconnu que la solution proposée ne peut pas être largement acceptée sans les résultats d'une expérimentation. La validation peut être obtenue par différentes méthodes, chacune avec ses avantages et ses limitations. Dans le domaine de la recherche en

réseau, la fiabilité des résultats est l'un des problèmes les plus critiques. Dans ce contexte, la méthode la plus largement utilisée - simulation - manque parfois de crédibilité. La méthode moins utilisée mais la plus crédible - un banc d'essai réel - est trop chère et difficile à l'échelle et à gérer.
Dans cette thèse, notre objectif principal est de faire face aux problèmes liés à la mobilité du nœud multicast. Les solutions sont proposées dans le cadre de l'évolution de la direction actuelle de la mobilité IP : à partir de la gestion mobilité orientée client vers la gestion de la mobilité orientée réseau, et aussi à partir de la gestion centralisée vers la gestion distribuée de la mobilité. Plus précisément, pour un domaine PMIPv6, nous introduisons une méthode pour réduire l'interruption de service et le gaspillage de ressources. Nous présentons ensuite une solution du point de vue de l'équilibrage de charge pour régler les problèmes de l'interruption de service et la duplication de paquets. Comme DMM n'a pas été normalisé, nous proposons une solution de mobilité inter-domaine, qui peut être considérée comme une étape dans l'évolution de PMIP vers DMM. Enfin, nous convergeons vers une architecture finale dans un domaine DMM qui peut offrir divers avantages et résoudre la plupart des problèmes liés à la mobilité des clients multicast. Tout au long de cette thèse, un banc d'essai proche d'un réseau réel est utilisé pour démontrer des résultats réalistes.

A.2 Technologies de Référence et Défis

A.2.1 Multicast IP

Contrairement au modèle traditionnel de communication où les données sont envoyées à partir d'une source vers une destination (appelé unicast ou communication un à un) ou à tous les nœuds dans un portée spécifique (broadcast), la technologie multicast permet la transmission de données à un ensemble d'utilisateurs qui sont intéressé à recevoir le même contenu en même temps. En utilisant la technologie multicast, l'expéditeur a seulement besoin d'envoyer une copie unique de données pour accéder à tous les membres du groupe, au lieu de l'envoi d'une copie séparée pour chaque récepteur. Les routeurs intermédiaires alors reproduisent les paquets de données jusqu'à ce qu'ils atteignent les récepteurs. En conséquence, le multicast apporte certains avantages par rapport à la diffusion individuelle (unicast) et le broadcast, tels que la réduction de la charge du serveur et l'élimination de trafic redondant, donc améliorant l'utilisation ensemble des ressources [28].
Afin de fournir un service multicast, deux groupes de protocole doivent être déployés: les protocoles stations-routeurs et les protocoles de routage. Les protocoles stations-routeurs permettent aux clients de rejoindre dynamiquement / quitter le groupe ainsi qu'aux routeurs de multicast (MR) d'être conscients des récepteurs intéressés et de gérer les abonnements des clients. Les protocoles de routage multicast permettent une collection de routeurs (MRs) de construire des arbres de distribution pour acheminer le trafic multicast à partir des sources de tous les membres d'un groupe multicast. Les protocoles stations-routeurs, selon la version IP, sont Internet Group Management Protocol (IGMP) [34] pour IPv4 et Multicast Listener Discovery (MLD) [35] pour IPv6. En ce qui concerne les protocoles de routage, chaque protocole utilise son algorithme de routage pour construire les arbres de distribution. Dans cette thèse, nous considérons le PIM-SM (Protocol Independent Multicast - Spare Mode) et une version améliorée de PIM-SM pour la source spécifique (PIM-SSM [41]) comme le protocole de référence. Cependant, les solutions proposées ne sont pas limitées à ce protocole. En outre, le proxy Multicast Listener Discovery (MLD) qui est un protocole léger peut être utilisé pour simplifier la conception et la mise en œuvre du routeur. Les proxies peuvent être placés entre le routeur et le client. La fonction de

proxy permet à un nœud d'apparaître comme un routeur pour les clients « en aval » et en tant qu'un client pour le MR « en amont ». Par conséquent, du point de vue pratique, nous nous concentrons sur le scénario où la fonction proxy est déployée au niveau du routeur dans le réseau d'accès.

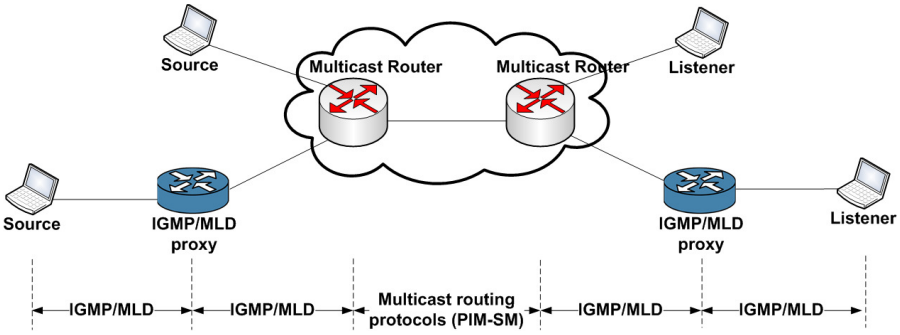


Figure A.1 – Une scenario de déploiement du service multicast: en point de vue des protocoles multicast.

Profitant de la technologie multicast, nombreuses applications, qui peuvent être classées en différents groupes suivant des critères différents, peuvent être déployées. En termes de modèle multicast, les applications peuvent être classées en trois catégories principales: la communication une-à-plusieurs (une seule source d'envoi à plusieurs récepteurs), la communication plusieurs-à-plusieurs (plusieurs sources d'envoi à plusieurs récepteurs), et la communication plusieurs-à-un (plusieurs sources envoyer à un récepteur).

A.2.2 La gestion de la mobilité IP

Dans les réseaux mobiles-tous IP, la mobilité IP est un concept essentiel pour répondre à la demande de connectivité d'Internet omniprésente ainsi que des nouvelles exigences en matière de services, tels qu'un handover transparent sur les réseaux hétérogènes, une qualité constante de l'expérience et les contraintes strictes de délai. Les protocoles de gestion de la mobilité à la couche réseau peuvent être classés selon différents critères tels que la gamme de la mobilité (micro- et macro-mobilité) et la signalisation de la mobilité (la gestion mobilité orientée client et la gestion de la mobilité orientée réseau) [53, 54, 61, 55].
MIPv6 [70] est le premier protocole de mobilité normalisé par l'IETF pour les réseaux IPv6. Comme un protocole de mobilité globale, MIPv6 maintient l'accessibilité du nœud mobile quel que soit la position géographique du mobile. Elle se fait par l'introduction d'une mobilité central, appelé Home Agent (HA ou Agent Mère) situé au réseau mère d'un mobile. L'HA est un point d'ancre de l'adresse IP unique du MN (Home Address or HoA). Lorsque le MN est éloigné de son réseau mère, le MN enregistre alors son emplacement actuel avec son HA au moyen des messages Binding Update (BU) et Binding Acknowledgement. Un tunnel bidirectionnel est alors établie entre l'HA et le MN pour rediriger les paquets de / vers l'emplacement actuel du MN. En outre, MIPv6, comme une solution globale de mobilité IP, peut entraîner une latence élevé (et la perte de paquets) qui pourraient affecter de manière significative la performance des sessions courants [72, 73]. Une haute charge de signalisation est également nécessaire.
Contrairement au MIP6 dans lequel les fonctions de mobilité doivent être déployées à la fois le réseau et le terminal, PMIPv6 [76], qui a été normalisé par l'IETF, est un protocole de gestion de la mobilité orientée réseau. PMIPv6 fournit une mobilité sans le soutien à la mobilité du MN. En d'autres termes, le réseau est en charge de la gestion de la mobilité IP

pour le terminal mobile. Ceci est réalisé en introduisant l'entité de réseau appelée MAG, qui effectue la signalisation liée à la mobilité au nom des MNs. L'ancre de mobilité locale (Local Mobility Anchor - LMA), similaire à l'HA, est responsable du maintien de l'état d'accessibilité du MN et transmet le trafic de / vers l'emplacement actuel du MN. Pour rediriger les paquets, LMA utilise les mécanismes IPv6 d'encapsulation.

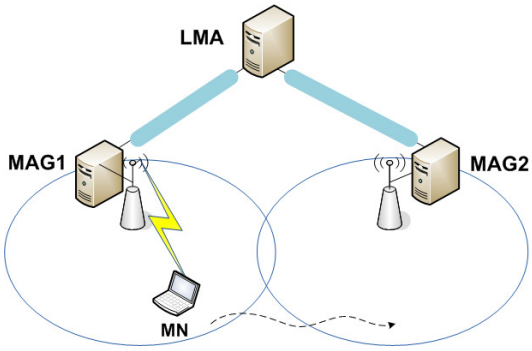


Figure A.2 – L'achitecture d'un domaine PMIPv6.

Par rapport à MIPv6, PMIPv6 apporte certains avantages tels que: (i) évitant la complexité de la pile de protocole au MN; (ii) soutenant la mobilité sans la participation du MN; (iii) réduisant les surcharges de tunnel (sur l'air); et (iv) diminuant la latence [73].
L'opération de PMIPv6 est brièvement présentée comme suit : quand un MN entre dans un domaine PMIPv6 (attache à MAG1, par exemple), MAG1 va chercher le profil de MN (par exemple, à partir d'un serveur AAA). Puis deux messages de signalisation, le PBU et le PBA sont échangés entre MAG1 et LMA pour d'attribuer un (ou plusieurs) préfixe (s) (HNP) et mettre à jour l'emplacement actuel du MN. Un tunnel bidirectionnel est établi entre MAG1 et LMA pour rediriger le trafic de / vers le MN. Le MAG1 envoie alors un message RA, y compris l'HNP au MN. Le MN, basé sur l'HNP affecté, configure son adresse et peut l'utiliser pour communiquer avec un nœud correspondant (CN). Lorsque le MN effectue un handover de MAG1 à MAG2, le processus similaire sera exécuté pour mettre à jour l'emplacement actuel du MN au LMA. Le MAG2 obtient le même préfixe pour ce MN et peut émuler le réseau de la maison du MN (envoi des messages RA avec le même HNP). En conséquence, le MN n'est pas conscient de la mobilité et continue à utiliser la même adresse IP que précédemment.
L'architecture actuelle de réseau mobile est très centralisée et hiérarchique. Ainsi les protocoles de mobilité IP (tels que PMIPv6 et DSMIPv6), qui ont été adoptés comme les protocoles de mobilité IP pour l'architecture EPC 3GPP, sont en ligne avec l'architecture centralisée et hiérarchique du réseau. Suite à l'architecture hiérarchique, les protocoles de gestion de la mobilité centralisée sont basés sur l'ancre de mobilité (HA dans MIPv6 et LMA dans PMIPv6) pour support à la mobilité. Par conséquent, à la fois le contexte de mobilité et l'encapsulation de trafic doivent être maintenus à l'ancre de mobilité. L'augmentation du nombre d'appareils mobiles et de leurs demande de trafic font des solutions de gestion de la mobilité centralisée à rencontrer plusieurs problèmes et limitations comme indiqué dans [9, 10]. Parmi eux, nous soulignons simplement les problèmes suivants :

- Le routage non optimal et le délai bout-à-bout : Lorsque le trafic de données traverse toujours l'ancre de mobilité centrale, il entraîne souvent une route plus longue. En particulier, lorsque le CN et le MN sont proches les uns des autres, mais loin de l'ancre. La même chose se produit dans le cas de CDN, dans lequel les fournisseurs de contenu mettent leurs données à la bordure du réseau. En conséquence, le délai

de bout en bout sera augmenté.

- Le problème de l'évolutivité : La maintenance du contexte de MN et le traitement des paquets de / vers le MN nécessitent généralement des ressources de l'ancre de mobilité ainsi que les réseaux, donc réduisant l'évolutivité du système.

- Le gaspillage de ressources : Le service de la mobilité est toujours disponible même pour les sessions qui ne nécessitent pas le soutien de gestion de la mobilité. Ainsi, en apportant un soutien à la mobilité pour le MN/le service lorsque c'est vraiment nécessaire, les ressources de réseau peuvent être sauvées.

- La fiabilité: L'ancre de mobilité centrale en général constitue un goulot d'étranglement et point de défaillance unique.

La notion de DMM vise à répondre aux limites de l'approche de la mobilité centralisée soulevée quand un grand nombre d'appareils mobiles et le trafic de données sont pris en compte dans une architecture plate [9, 10]. DMM est actuellement un sujet brûlant, qui gagne beaucoup d'intérêt à la fois du monde universitaire et l'industrie. L'IETF a récemment affrété le groupe de travail DMM qui précise les solutions permettant de mettre en place des réseaux IP à l'appui d'un modèle d'ancrage distribué. Les concepts clés du DMM sont les suivants: i) les ancres de mobilité sont distribuées entre les entités de réseau et placées aussi près que possible du MN; et ii) la gestion de la mobilité est dynamique utilisée pour les sessions qui ont vraiment besoin de continuité de service. Dans DMM, une nouvelle entité est introduite - le MAR (Mobile Access Router). Cette entité peut jouer un rôle d'un HA, un LMA, un MAG ou un router normal.
Dans l'approche basée sur le client, le MN est nécessaire pour participer au processus de signalisation. Chaque fois qu'un MN attache à un MAR, il obtient une adresse IPv6. Le MAR courant (cMAR) joue le rôle d'HA pour l'adresse attribuée à son réseau. Quand le MN attache au cMAR, il peut commencer une nouvelle communication avec le CN en utilisant l'adresse courante comme l'adresse de source du flux. Ce flux est acheminé de manière standard sans le mécanisme de tunnel. Lorsque le MN effectue un handover, si ce flux est encore en vie, il est acheminé via le routeur où ce flux a été initialement lancé (aMAR) en utilisant le mécanisme de tunnel entre le routeur et le MN. Pour ce faire, le MN doit mettre à jour son emplacement actuel à l'aMAR qui joue le rôle de son HA. Il est à noter que le MN doit effectuer une mise à jour de localisation pour chaque adresse IP active. En conséquence, il est nécessaire que le MN gère la liste d'HoA actifs et les aMARs associés, ainsi que la liste de sessions actives. En outre, le MN a besoin d'un mécanisme supplémentaire qui permet de sélectionner la bonne adresse IP à utiliser pour chaque session.
Contrairement au DMM basé sur le client, l'approche basée sur le réseau ne nécessite pas le MN à participer au processus de signalisation. Le MAR effectue donc à la fois la fonctionnalité de LMA et de MAG. Agissant comme un MAG, le MAR détecte l'attachement du MN. Tout comme un LMA, il alloue une HNP au MN. Semblable au DMM basé sur le client, quand un MN attache à un MAR, il obtient une adresse IPv6. Typiquement, il peut utiliser l'adresse IP actuelle pour lancer des nouvelles sessions. Le trafic de données est acheminé en utilisant le routage IP normal sans aucun mécanisme de tunnelisation. Si le MN effectue un handover, le trafic sera acheminé à partir du MAR d'ancrage au MAR courant par le tunnel de la mobilité entre eux. Cependant, une question importante se pose est que la façon dont le cMAR apprend sur les adresses des aMARs. Il existe plusieurs mécanismes permettant le cMAR de connaître l'adresse des aMARs. La première méthode [90] repose sur une base de données centralisée (CMD) qui stocke les informations liées à la

mobilité de chaque MN dans le domaine tel que la liste des HoAs, et l'adresse des aMARs associés comme similaire à [93]. Bien que cela permette de s'assurer que le processus de mobilité est totalement transparent pour le MN, ce mécanisme présente encore un point d'ancre centrale, cependant, pour le plan de contrôle seulement. La seconde méthode est basée sur l'information fournie par le MN comme spécifié dans [65]. En conséquence, le MN n'est plus transparent pour le processus de mobilité. Par conséquent, dans certains documents [69, 66], cette méthode est considérée comme un système basé sur le client comme indiqué ci-dessus.

A.2.3 Multicast IP dans le contexte de la mobilité

Afin de permettre le multicast IP dans MIPv6, deux approches de base ont été proposées, à savoir le tunnel bidirectionnel et la souscription à distance. Les deux approches ont leurs avantages et leurs inconvénients. Le tunnel bidirectionnel cache le déplacement des nœuds en acheminant le trafic multicast via le tunnel de mobilité entre le nœud et sa HA au prix de routage triangulaire (conduisant à un long délai) et le problème de la convergence du tunnel. D'autre part, dans l'approche de souscription à distance, le nœud multicast doit rejoindre les sessions en cours après chaque handover, ce qui pourrait mener l'interruption de service importante. En outre, des problèmes plus graves peuvent être augmentés en cas de mobilité de la source comme la transparence d'adresse et la maintien d'état de routage [11, 12]. Une amélioration supplémentaire devrait également être envisagée afin de satisfaire aux exigences supplémentaires en termes d'interruption de service et la perte de paquets pour les services en temps réel. Depuis tous ces protocoles sont conçus pour MIPv6 qui exigent les nœuds mobiles à participer au processus de signalisation, ils ne peuvent pas être appliqués directement à PMIPv6. Pourtant, l'idée de ces solutions peut être réutilisée.
Comme les protocoles multicast sont conçus à l'origine pour un réseau fixe, considérant le multicast dans un environnement mobile apporte plusieurs défis au service multicast. La mobilité du nœud a des effets différents sur le service multicast, selon des facteurs tels que le rôle du nœud dans la session (source ou l'auditeur), le considéré modèle multicast (ASM ou SSM), le protocole de routage, le protocole de gestion du groupe et le protocole de mobilité en cours d'utilisation ainsi que la technologie d'accès sans fil. Par conséquent, les problèmes causé par la mobilité d'un nœud multicast peuvent être divisés en quatre groupes principaux : les problèmes généraux (en raison de protocoles multicast), les problèmes spécifiques de l'auditeur mobile, les problèmes spécifiques de la source mobile et les problèmes de déploiement [11, 12, 115]. Dans le cadre de cette thèse, nous nous concentrons sur les problèmes spécifiques de l'auditeur.
La mobilité d'un auditeur provoque plusieurs problèmes pour le service multicast. Les problèmes et les solutions possibles sont décrits comme suit :

- L'interruption de service et la perte de paquets : Puisque le nœud mobile dans la gestion de la mobilité basée sur le réseau n'est pas au courant du processus de la mobilité, il ne peut pas prendre des décisions relatives au multicast, évitant un doux reprise de la session multicast. En conséquence, quand un auditeur se déplace à un nouveau MAG, il doit attendre pour exprimer son intérêt à s'abonner à des canaux multicast en cours jusqu'à ce qu'il reçoive une requête MLD. Ainsi, il éprouve un certain retard dans la réception de contenu multicast en raison du temps supplémentaire lié à l'activation du service multicast, la transmission MLD Query / Report (en particulier l'activation du service multicast qui est typique en quelques secondes). Ce problème devient plus grave lorsque les services en temps réel sont considérés.
- La duplication de paquets : Dans certains cas, le MAG peut recevoir le même paquet multicast à partir de différents LMAs ou MRs. Cela se produit lorsque différents

tunnels MAG-LMA sont utilisés pour délivrer le trafic multicast.

- Le routage non optimal et le délai de bout en bout : Lorsque le trafic multicast doit passer par le point d'ancre de mobilité centrale (LMA), il entraîne souvent un plus long parcours. En conséquence, le délai de bout en bout sera augmenté. Ce problème devrait être prise en compte, en particulier lorsque les services en temps réel et les services sensibles au délai sont considérés.
- Le laisser de latence et le gaspillage des ressources de réseau : Puisque l'auditeur n'est pas conscient de la mobilité, il ne sera pas envoyer un rapport MLD pour quitter explicitement le groupe dans le MAG précédent (previous MAG - pMAG). En conséquence, si le dernier membre d'un groupe multicast se déplace à un autre MAG, le pMAG continuera d'offrir le trafic multicast jusqu'à ce qu'il met à jour ses informations des membres. Ainsi, il provoque une perte de ressources de réseau.
- En outre, l'auditeur peut recevoir le paquet hors de l'ordre en raison de handover. Dans de nombreux régimes sans fil, la signalisation liée au multicast doit être minimisée pour réduire la consommation d'énergie (avec la capacité limitée) et la ressource de réseau en cours d'utilisation. Encore une fois, l'ajustement des paramètres MLD [115] doit être soigneusement étudié comme un compromis des surcharges de signalisation et de l'interruption de service.

Les solutions en point de vue de l'IETF Suite à une architecture typique de déploiement, le support multicast peut être activé en déployant le proxy MLD et la fonction de MR dans le domaine. En général, les différentes propositions sont issues en correspondant de l'emplacement de MAG et LMA dans l'architecture de déploiement de multicast. En conséquence, il existe deux approches principales correspondant aux différents rôles de MAG et LMA comme : i) MAG agit comme un proxy MLD tandis que LMA agit comme un MR ou un proxy supplémentaire; et ii) MAG et LMA jouent le rôle d'un MR. La première approche est considérée comme une solution de base par l'IETF. Cette solution peut également être considérée comme une solution basée sur le mécanisme de tunnelisation en raison du fait que le trafic multicast est routé via le tunnel de mobilité entre LMA et MAG. Dans la seconde approche, par le déploiement de routage multicast à MAG, plusieurs problèmes peuvent être évités (par exemple, le routage sous-optimal, problème de convergence) à un coût de fonctionnement et de déploiement du router multicast.

La solution de base La solution de base, qui a été normalisée par l'IETF, offre le soutien de la mobilité de l'auditeur dans PMIPv6 en plaçant la fonction proxy MLD au MAG, tandis que le LMA agissant comme un MR ou un proxy supplémentaire. La fonction proxy MLD est mise en œuvre au MAG avec l'interface « en amont » étant configuré vers le LMA. Comme une opération typique du proxy MLD, les données arrivant d'une interface « en amont » seront transmises aux interfaces « en aval » qui ont états appropriés pour ce groupe. Ainsi, tout le trafic multicast passe par le tunnel MAG-LMA, comme le trafic unicast. Après chaque handover, le trafic multicast continue de fournir à l'auditeur dans le nouveau MAG, et la continuité de service est assurée en conséquence. En outre, du point de vue de service multicast, l'auditeur ne connaît pas la mobilité. Il est atteint puisque le nouveau MAG, après l'obtention d'informations sur l'abonnement de l'auditeur en utilisant les opérations normales de MLD, rejoint les flux multicast courants de la part de l'auditeur. La solution de base peut être également appliquée à la source multicast [118].
Lorsqu'un MN est attaché à un MAG (MAG1), après l'exécution des opérations PIMPv6 standards, MAG1 crée une instance proxy MLD (si nécessaire), qui sert comme un routeur « en amont » de tous les nœuds associés du LMA du MN. Cette instance ajoute le MN à son

interface « en aval » et configure son interface « en amont » vers le LMA du MN. Lorsque le MN exprime sa volonté de recevoir le trafic multicast d'un groupe, il envoie un rapport MLD à MAG1. Le MAG1 envoie alors un rapport agrégé au LMA à rejoindre le groupe au nom du MN. Le LMA, agissant comme un MR, rejoint le groupe de l'infrastructure multicast, et met à jour son état de transmission. Après avoir reçu les paquets multicast, le LMA les transmet aux MAGs appropriées (via le tunnel LMA-MAG) en fonction de son état de transmission. Le MAG1 transmet ensuite les paquets aux interfaces appropriées « en aval » et ils ont finalement atteint le MN. En cas de handover (de MAG1 à MAG2), puisque la mobilité est transparente pour le MN, le MN ne sera pas envoyer les rapports MLD non sollicités. Au lieu de cela, MAG2, lors de la détection d'un nouveau MN sur la liaison d'accès, ajoute le MN à une interface « en aval », et envoie des messages MLD de requête générale sur sa liaison attachée. Le MN répond alors par un message MLD y compris les états actuels des groupes multicast. Sur cette base, MAG2 peut rejoindre les groupes au nom du MN. Les paquets multicast sont acheminés depuis LMA à MAG2 et atteignent finalement le MN.
Bien que la solution de base soit un moyen très simple pour activer le support multicast dans PMIPv6, il ne traite pas des problèmes liés à la mobilité multicast. Dans plus de détails, l'utilisation de tunnel pour les flux multicast provoque la redondance du trafic (ou le problème de la convergence) au MAG. C'est parce que les différents nœuds, qui sont attachés au MAG et associés à différents LMAs peuvent s'abonner pour le même groupe. En outre, depuis plusieurs opérations doivent être exécutées pour permettre le MN continuer à recevoir le trafic multicast au nouveau MAG, il peut provoquer une longue interruption de service et un grand nombre de perte de paquets. En outre, comme le trafic multicast passe toujours par le LMA, il peut provoquer le problème de routage sous-optimal.

A.2.4 La mobilité d'un nœud multicast dans un domaine DMM orienté réseau

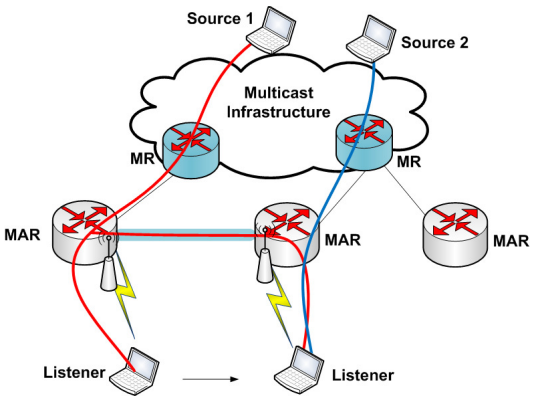


Figure A.3 – La mobilité d'un auditeur dans un environnement DMM (la fonction de proxy MLD est déployée à MARs).

Puisque DMM est encore à un stade précoce de la normalisation, il y a un travail limité pour le soutien au multicast. Jusqu'à présent, aucune solution complète n'a été trouvée pour le multicast dans DMM. En règle générale, tous les principaux aspects sont hérités du problème dans un domaine PMIPv6, tandis qu'une complexité supplémentaire est ajoutée. Il est à noter que cette section ne présente que les problèmes et les solutions en considérant un environnement DMM orienté réseau.

Comme dans PMIPv6, le soutien à la mobilité de l'auditeur multicast peut être activé dans DMM en déployant le proxy MLD à MAR [128, 22, 20]. Dans ce cas, quand un flux multicast est lancé, le trafic multicast est reçu directement à partir de l'infrastructure multicast native via le MAR courant. Dans le cas du handover, le trafic est acheminé à partir de MAR d'ancrage au MAR courant via le tunnel entre eux (comme le trafic d'unicast). Cependant, ce mode ne traite pas des problèmes relatifs au multicast. Parmi eux, nous soulignons seulement les problèmes y compris l'interruption de service, le routage non-optimal, le délai de bout en bout, et le problème de la convergence, et la perte de paquets.
Considérant le déploiement de la fonction MR à MARs, le MAR décidera le trafic multicast d'un MR pour un auditeur attaché basé sur le Reverse Path Forwarding (RPF). Par conséquent, la convergence du tunnel et le routage non-optimal seront évités. Cependant, le mouvement de l'auditeur provoque le problème de l'interruption de service. En outre, les opérateurs ne veulent pas déployer la fonction de routage multicast sur le MAR en raison de sa mise en œuvre et le coût d'exploitation par rapport à proxy MLD.

A.2.5 Evaluation de la performance

A.2.5.1 Métriques pour l'évaluation de la performance

Pour évaluer la performance d'un protocole de gestion de la mobilité, un ensemble de paramètres est en général considéré incluant le coût de signalisation, le temps de handover (temps de latence), le délai de bout en bout et le coût de tunnelisation. Le coût de signalisation est défini comme le coût de mettre à jour l'emplacement du MN. Il est un facteur important car il influence l'évolutivité du système ainsi que le coût de livraison de données, en particulier lorsqu'on considère environnement sans fil qui a typiquement une capacité limitée. En ce qui concerne le temps de latence, il est définie comme une période où un nœud ne peut pas recevoir / envoyer des paquets en effectuant un handover. C'est le temps écoulé entre le dernier paquet reçu via l'ancien routeur et l'arrivée du premier paquet via le nouveau routeur après un handover. Au cours de cette période, les paquets sont perdus. Ainsi, il peut entraîner de l'interruption notable de service, surtout dans le cas d'applications sensibles au délai comme la vidéo et la voix sur IP (VoIP). Le nombre de paquets perdus est généralement proportionnel à la latence de handover. Dans les réseaux basés sur IPv6, QoS peut être définie par la perte de paquets, la latence et les surcharges de signalisation [72]. En conséquence, une longue période de latence et un grand nombre de paquets perdus peuvent dégrader la qualité du service. Par conséquent, la réduction du temps de latence et de la perte de paquets améliore la performance de l'application. D'autre part, le délai de bout en bout entre deux nœuds est la somme des retards rencontrés au long du trajet entre ces nœuds. En général, le délai de bout-en-bout comprend non seulement le délai de la transmission sur les liens, mais également la mise en attente de traitement et de retard au niveau des nœuds intermédiaires [133]. Des nombreuses applications populaires de multimédia (par exemple, le jeu en temps réel, le streaming vidéo en direct et VoIP / Vidéo conversationnel) ont de délai strict.

A.2.5.2 Evaluation expérimentale pour les réseaux sans fil

Dans la recherche en réseau, il y a des diverses méthodes d'expérimentation, tels que : le banc d'essai réel, la simulation, l'émulation, la virtualisation et la modélisation mathématique (ou théorique). Chaque méthode a ses avantages et ses limites [135]. L'utilisation d'un banc d'essai réel est considérée comme la meilleure méthode expérimentale. Cependant, elle implique un coût plus élevé de déploiement et manque d'évolutivité. Bien que la

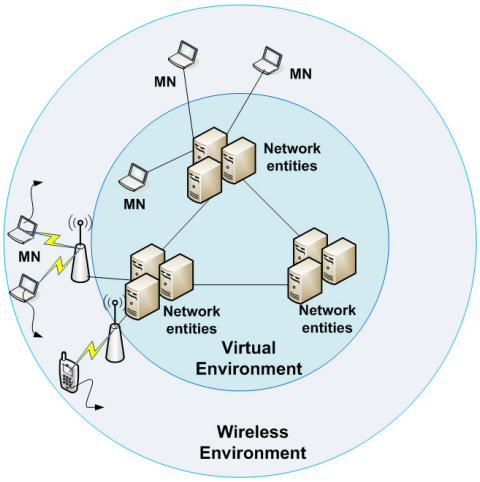


Figure A.4 – L'architecture d'un banc d'essai proche de réel.

simulation soit très populaire grâce à sa flexibilité et facile à déployer des fonctionnalités, les résultats obtenus dans certains cas, ne sont pas fiables. L'émulation peut être considérée comme un compromis entre la simulation et un banc d'essai réel apportant des résultats plus précis (par rapport à la simulation) et à moindre coût (par rapport au banc d'essai réel). Pourtant, l'émulation a des limites sur le déploiement et l'évolutivité, qui peuvent être atténués en utilisant la technique de virtualisation. Enfin, la modélisation mathématique est parfois utilisée, mais seulement d'une façon simplifiée, en faisant abstraction de la complexité. En outre, pour aider à justifier notre approche sur la méthode expérimentale, nous devons mentionner que notre étude concerne les environnements mobiles et nous devons donc garder à l'esprit les exigences les plus importantes que d'une méthode expérimentale doit se concentrer sur sont la précision, la fiabilité, la mobilité et l'évolutivité [136].

Dans cette thèse, nous introduisons un environnement d'expérimentation proche du réel qui se compose d'un environnement de virtualisation et simulation. La première partie peut être considérée comme l'infrastructure du réseau dans lequel les multiples machines virtuelles sont reliées, tandis que la seconde partie est un réseau d'accès sans fil essentiellement composé par le simulateur NS-3. En combinant ces éléments, nous avons produit une méthode qui peut atteindre un niveau supérieur de réalisme en conservant les avantages de la méthode de simulation et encore être en mesure d'exécuter des logiciels et des protocoles réels. Puisque cet environnement est un open-source et facile à déployer, il peut être réutilisé par d'autres chercheurs à créer leur propre environnement d'expérimentation. De plus, il permet la conception et l'évaluation du réseau de taille petit à moyenne et de déployer les protocoles dont les résultats peuvent être facilement convertis dans le monde réel. En particulier, cette méthode est appropriée pour les cas suivants : i) l'infrastructure fixe; ii) la mobilité et les réseaux mobiles; iii) l'expérimentation de la couche supérieure à la couche réseau (par exemple, la gestion de la mobilité, le multicast, les applications, etc.); iv) l'infrastructure du réseau de taille moyenne; et v) le réseau de taille grande en fonction de nœuds mobiles.

A.3 La mobilité d'un nœud multicast dans PMIPv6

A.3.1 Optimisation de la continuité de service dans un domaine PMIPv6

La solution de base a été récemment adoptée pour soutenir la mobilité de l'auditeur dans PMIPv6. Néanmoins, elle ne traite pas des problèmes d'optimisation et de performance tels que le temps d'interruption de service, les surcharges de tunnel, et le routage non optimal, etc. En ce qui concerne le temps d'interruption de service, nous proposons une méthode basée sur la combinaison des mécanismes de transfert de contexte multicast et de fonction de suivi explicite pour minimiser le temps d'interruption. Commençant par l'analyse du temps de l'interruption, les expériences sont ensuite effectués pour comparer différentes approches reposant sur un banc d'essai près au réel. Les résultats numériques et expérimentaux montrent que grâce à l'utilisation de transfert de contexte multicast, le temps d'interruption peut être réduit de manière significative. En ajustant le comportement du MLD pour les routeurs, nous pouvons également obtenir un résultat similaire, mais arrive une dramatique augmentation de la signalisation liée au multicast. Particulièrement, le problème sera plus grave avec un grand nombre d'auditeurs. En outre, grâce au transfert de contexte multicast le temps de congés (leave latency) est minimisé. Par conséquent, le protocole de transfert de contexte en général peut être considéré dans les solutions proposées. A noter que la fonction de transfert de contexte et la fonction de suivi explicite mises en œuvre peuvent être utilisées dans notre banc d'essai, ainsi que dans un vrai banc d'essai. Notre banc d'essai peut être servi comme un banc d'essai proche du réel, qui peut fournir des résultats réalistes à faible coût pour l'expérimentation de la mobilité multicast dans un domaine PMIPv6.

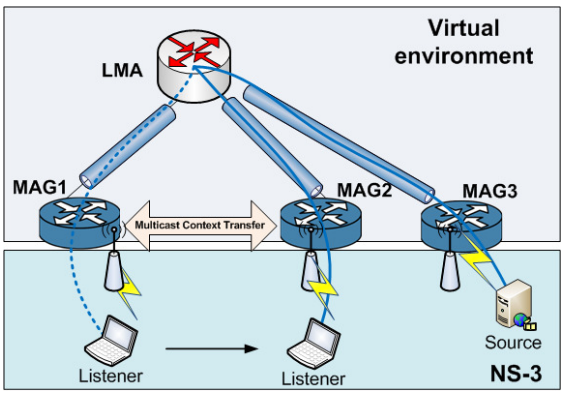


Figure A.5 – Le déploiement d'un banc d'essai proche au réel.

Pour réduire le temps d'interruption, l'objectif est de réduire le temps nécessaire au nouveau MAG (nMAG) pour obtenir des informations d'abonnement multicast actives du MN pendant handover. Alors que le nMAG peut s'abonner à des flux courants (à l'avance) et transmet les paquets multicast au MN dès que possible. Pour ce faire, des informations d'abonnement sont échangées entre le pMAG et le nMAG. En outre, cette solution est indépendante de la technologie de la couche 2 et plus facile à déployer que les propositions existantes. Le transfert de contexte multicast est également mis au point conformément à la norme pour le protocole de transfert de contexte [159]. En outre, la solution proposée ne met pas de charge supplémentaire sur le LMA, ce qui rend notre solution meilleure en comparaison avec la solution M-LMA en termes d'évolutivité.

A.3.2 Equilibrage de charge du flux multicast dans les réseaux PMIPv6

La croissante de la pénétration des appareils mobiles, tels que les tablettes et les téléphones intelligents génère un grand nombre de trafic de données, en particulier le trafic vidéo sur les réseaux mobiles [6, 1]. Dans ce contexte, il est fréquent d'avoir un grand nombre de périphériques associés au LMA dans un domaine PMIPv6 donc facilement faire le LMA un goulot d'étranglement et un point de défaillance unique. Par conséquent, la qualité des sessions en cours pourrait être dégradée (par exemple, une augmentation du délai de la file d'attente et une augmentation du perte de paquets). En conséquence, les opérateurs des réseaux mobiles peuvent avoir besoin de déployer plusieurs LMAs dans un grand domaine PMIPv6, de sorte que le trafic peut être réparti entre les LMAs [76]. Pourtant, il est fort possible que certains LMAs deviennent surchargés alors que les autres sont sous-utilisés. Par conséquent, l'équilibrage de charge (LB) entre les LMAs est nécessaire. Du fait que le multicast IP devrait être largement déployé dans un proche avenir pour faire face à une énorme demande de trafic multimédia. Ainsi que, le contenu de la vidéo mobile a généralement des débits beaucoup plus élevés que les autres types de contenu. Le service multicast devrait donc jouer un facteur crucial dans la mise charge sur le LMA. Cependant, son rôle a été négligé dans toutes les propositions existantes. Par conséquent, l'utilisation de service multicast dans les mécanismes LB existants peut conduire à plusieurs problèmes à la fois de LB (la dégradation de l'efficacité) et de service multicast (par exemple, le problème de la convergence et l'interruption de service).

Pour ces raisons, nous introduisons un mécanisme d'équilibrage de charge (en fonction de multicast), qui prend le service multicast en compte. L'idée clé est que par la séparation du mécanisme d'équilibrage de charge multicast à partir de l'unicast, la solution proposée permet de mieux répartir la charge entre les LMAs dans runtime, ainsi que d'améliorer l'efficacité de l'utilisation des ressources.

Dans plus de détails, deux approches différentes, à savoir l'approche proactive multicast (ou MAG-initié) et l'approche réactive multicast (ou LMA-initié) sont considérées. Dans le premier cas, le mécanisme LB sera appelé lorsqu'un MN démarre une nouvelle session multicast pour sélectionner un LMA approprié à servir cette session. Dans ce dernier cas, le mécanisme LB sera exécuté quand un LMA est surchargé en sélectionnant une session de multicast pour passer à un LMA moins chargée. Il peut être fait grâce à une extension de proxy MLD pour supporter de multiples interfaces « en amont » [167]. Dans ce cas, une seule instance de proxy est déployée à MAG avec plusieurs interfaces « en amont » étant configurées vers différents LMAs. En conséquence, le MN peut recevoir le trafic multicast à partir d'un LMA moins chargé, en obtenant le trafic unicast à partir de sa LMA. Par conséquent, la solution proposée ne modifie pas les sessions multicast/unicast en cours.

A.3.3 Mobilité dans les réseaux hétérogènes

La mobilité dans les réseaux hétérogènes sera illustrée via un cas d'utilisations: le service de recharge de véhicule électrique (EVCS). Il y a plusieurs raisons pour choisir ce cas d'utilisation. Tout d'abord, le véhicule électrique (EV) est un choix prometteur pour le transport personnel dans un proche avenir. Deuxièmement, l'idée de connexion des véhicules prend de l'ampleur. En outre, un nœud mobile (ou un véhicule électrique dans ce contexte) peut être relié à l'infrastructure via différentes technologies sans fil / filaires dans différentes étapes. Ainsi, compte tenu multicast dans le véhicule électrique est une étape pour permettre de déployer système de divertissement à l'EV, qui devient de plus en plus populaire. En outre, le multicast IP peut également être utilisé pour mettre à jour le

logiciel des systèmes embarqués.

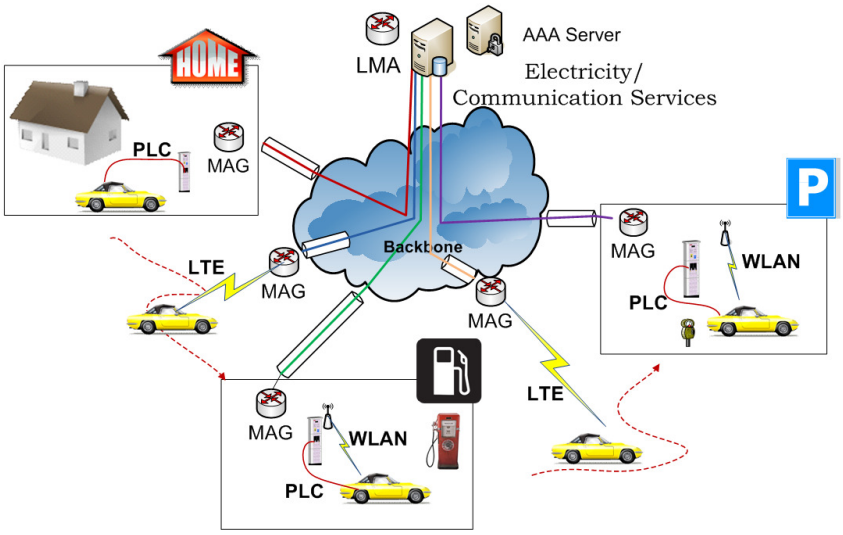


Figure A.6 – Les cas d'utilisation de service EVCS.

Comme indiqué dans [184], la condition essentielle pour obtenir des avantages énergétiques et économiques de Smart-Grid et de véhicules électriques est d'atteindre un ordonnancement optimal de la charge des véhicules électriques et le stockage de l'électricité par les EVs. Ainsi, il est important pour les opérateurs du Grid de surveiller les données nécessaires (comme la consommation d'énergie et la demande) et d'attribuer et de router des véhicules vers les stations de recharge appropriées pour appuyer leurs politiques de tarification nécessaires. Cette négociation ne peut être menée à la station de charge, mais doit être effectuée pendant la conduite. L'EV doit donc communiquer avec l'infrastructure de charge [185]. Dans ce contexte, plusieurs technologies d'accès (par exemple, WLAN, LTE, et PLC) doivent être utilisés lors des différentes phases de l'EVCS, comme LTE pendant la conduite, WLAN en approchant une station de charge, et PLC en étant amarré à une station de recharge. Ces technologies de communications hétérogènes doivent être transparentes pour l'utilisateur, la gestion de réseau et pour l'EVCS afin de maintenir le contexte de service.
Nous vous proposons une solution de EVCS à la fois point de vue de l'utilisateur et de l'opérateur de Grid. Pour l'utilisateur, il offre un service omniprésent et transparent à différents scénarios (à la maison, à une station de charge et à un parking), ce qui rend le chargement d'un EV aussi simple que possible. Il contribue également à l'operateur du réseau de gérer efficacement la consommation de l'utilisateur et la demande sur le Grid, surtout quand un grand nombre de véhicules électriques est considéré. De la nature centralisée de service de Smart-Grid, une solution de la gestion de la mobilité centralisée basée sur le réseau, par exemple, PMIPv6 est le plus appropriée pour fédérer les services de charge segmentés et faire l'expérience de charge transparente de la mobilité des EVs ainsi que la technologie de communication utilisée par chaque phase du EVCS. En utilisant PMIPv6, le service prend en charge la mobilité des EVs, les handovers verticaux et horizontaux entre les différentes technologies de communication. Pourtant, la conservation de l'adresse IPv6 dans PMIPv6 reste un problème dans un tel contexte, et nous fournissons une solution en s'appuyant sur une approche de l'interface logique pour cacher la modification de l'interface vers la pile IPv6 (du point de vue de la couche IP). Le concept d'EVCS et la performance du PMIPv6 pour l'EVCS ont été validés à l'encontre de référence de la norme IEEE 1646. Un banc d'essai proche au réel, qui est une combinaison des machines réelles et virtuelles, a

été déployé pour réduire le coût du matériel et de fournir d'expérience flexible. Un lien réel PLC fournis par les partenaires du projet VELCRI est utilisé pour obtenir des résultats réalistes.

A.3.4 La mobilité inter-domaine : du point de vue du DMM

Comme mentionné précédemment, en profitant de la gestion de la mobilité basée sur le réseau, PMIPv6 permet à la mobilité IP pour déplacer les clients sans leur participation. PMIPv6 apporte plusieurs avantages par rapport à la gestion de la mobilité basée sur le client comme MIPv6. Cependant, PMIPv6 échoue à soutenir la mobilité inter-domaine. Cela signifie que, même si un MN se déplace vers un autre domaine PMIPv6, la continuité de la session ne peut être maintenue.
Afin de soutenir la mobilité inter-domaine, plusieurs solutions ont été proposées, par exemple, l'intégration de MIPv6 et PMIPv6 (H-PMIP) [192]; et I-PMIP [193]. Pourtant, elles ont des limitations telles que le routage sous-optimal, les surcharges de signalisation et la latence de handover. Surtout, en raison du manque de granularité sur le service de gestion de la mobilité, la mobilité est toujours disponible même pour les sessions qui ne nécessitent pas de support de gestion de la mobilité (par exemple, les sessions qui sont lancées et terminées alors que le nœud mobile connecté au même domaine).
Basé sur le concept DMM, nous introduisons un support à la mobilité inter-domaine, appelé D-PMIP. Ainsi, cette proposition apporte certains avantages : (i) les ancres de mobilité sont placées près de MN; et (ii) le service de la mobilité n'est disponible que pour les sessions qui nécessitent vraiment la continuité du service. Une fois que le MN entre son domaine PMIPv6, il obtient un préfixe. Basé sur le préfixe attribué, le MN configure son adresse IPv6. Le MN peut ensuite utiliser cette adresse pour initier et maintenir les sessions de façon standard alors qu'il reste attaché à ce domaine. Lorsque le MN change son domaine, il obtient un autre préfixe et configure une nouvelle adresse basée sur ce préfixe. Cette adresse peut être utilisée pour mettre en place les nouvelles sessions. Jusqu'à ce que les sessions précédentes ne soient pas fermées, les anciennes adresses doivent être maintenues. Ainsi, un tunnel est construit entre le LMA d'ancrage et le LMA actuel à rediriger les paquets entre deux LMAs.
Basé sur le concept DMM, deux solutions possibles pour la mobilité inter-domaine sont considérées, à savoir la solution de partie distribuée (DP-PMIP) et la solution d'entier distribuée (DF-PMIP). La première solution repose sur une base de données commune pour le plan de contrôle, alors que dans la dernière la fonction de la mobilité est répartie dans les deux plans : le plan de contrôle et le plan de données. Ainsi, deux solutions permettent à des paquets de données à être acheminés via une manière quasi-optimale en mettant les points d'ancrage de mobilité plus proche du MN tandis que le plan de contrôle peut être placé n'importe où dans le réseau. Les résultats numériques montrent que la solution DP-PMIP donne des meilleures performances que les solutions existantes (par exemple, MIPv6, H-PMIP et I-PMIP) en termes de latence, de coût de signalisation et d'utilisation du tunnel.

A.4 La mobilité d'un nœud multicast dans DMM

Comme indiqué précédemment, le multicast IP peut être activé dans DMM en déployant la fonction proxy MLD à MAR. Pour le nouveau flux, le trafic multicast est transmis directement à partir de l'infrastructure multicast via le MAR courant. Pour le flux après le handover, le trafic est tunnelé du MAR où le flux est initié au MAR courant par le tunnel de la mobilité entre eux. Ainsi, le point d'ancre de mobilité multicast (MMA) est associé

à la phase initiale du flux multicast (identique à l'ancre de mobilité unicast) : le MAR où le flux est initiée. Le flux multicast sera ancré au MMA initialement attribué au cours de sa vie. Par conséquent, même lorsque le MN se déplace loin de son point d'ancre, le trafic de multicast traverse encore l'ancre. En conséquence, il provoque plusieurs problèmes au flux multicast en cours, comme l'interruption de service, le routage non-optimal, le délai de bout-en-bout et la duplication de paquets. Ces problèmes deviennent graves lorsqu'on considère les services sensibles à l'interruption et aux délais. En outre, même les ancres de mobilité sont distribuées, des ancres sont plus surchargées que les autres [200].
Dans cette section, nous soutenons principalement la nécessité d'un mécanisme de sélection dynamique de l'ancre de mobilité multicast (DMMA). D'un point de vue du service, il contribue à satisfaire les exigences en termes de l'interruption du service et le délai, en particulier lorsqu'on considère les services en temps réel. Il fournit un mécanisme permettant de mieux répartir la charge entre MARs. En outre, d'autres problèmes telles que la duplication de paquets et le laisser latence (perte de ressources) peuvent être réduits. Le DMMA prend en compte non seulement le contexte du service, mais aussi le contexte de la mobilité du nœud et le contexte du réseau, permettant un support par flux. En d'autres termes, chaque flux multicast peut être traité différemment selon différents contextes.

A.4.1 La mobilité de l'auditeur dans DMM

En ce qui concerne l'interruption de service, quand un auditeur multicast se déplace de pMAR à cMAR, il peut provoquer une interruption de service perceptible pour les flux en cours. En conséquence, le transfert de contexte multicast est nécessaire pour éviter une grande interruption causée par les procédures relatives au service multicast (environ 5 s dans le cas normal, et de 2,5 s dans le meilleur des cas) [16]. Ce délai est beaucoup plus long que le temps d'interruption de tolérance maximum pour les services normaux, comme spécifié dans [162] est de 500 ms. Même avec le transfert de contexte, il est incapable de répondre à l'exigence en termes d'interruption pour le service sensible à l'interruption lorsque le délai cMAR-aMAR est grand [22, 129]. C'est parce que le trafic multicast doit passer par l'aMAR, qui joue le rôle de point d'ancrage de multicast (MMA). En outre, puisque le trafic de multicast traverse toujours l'aMAR, il entraîne souvent une route plus longue. Particulièrement, considérant un grand domaine, il peut provoquer un délai de bout en bout élevé. Ce problème devient plus sérieux lorsque le service sensible au délai est considéré.
En cas de mobilité, l'utilisation du tunnel pour le flux multicast peut entraîner le problème de la convergence. Puisque le but de DMM est de déplacer les ancres de mobilité du coeur vers la périphérie du réseau, le nombre de points d'ancrage dans un domaine DMM sera beaucoup plus que celui dans un domaine PMIPv6. En conséquence, le problème de la convergence est supposé être bien plus sévère que celui dans PMIPv6. En utilisant une extension de proxy MLD pour supporter de multiples interfaces « en amont » [167], le problème de la convergence peut être évité.
Pour souligner ces problèmes, nous considérons différents candidats pour le MMA comme l'aMAR (le mode par défaut), le pMAR, le cMAR (le subscription native), ou un MMA commun (COMMA) qui sert comme un seul MMA pour le domaine (comme dans [117]). Différentes approches MMA_aMAR, MMA_pMAR, MMA_cMAR et MMA_COMMA sont considérées, en conséquence. Nous considérons également l'impact du déploiement de proxy MLD avec plusieurs interfaces sur ces problèmes.
La signalisation lorsqu'un auditeur effectue un handover dans DMM est décrite dans la figure A.7. Les opérations sont décrites brièvement comme suivants. La base de données de mobilité centrale (CMD), comme un LMA prolongé, stocke les préfixes du MN, ses

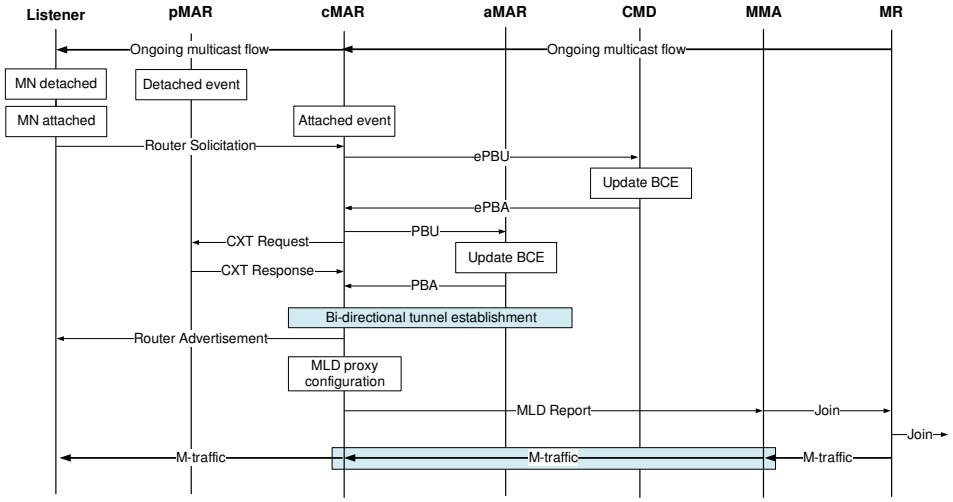


Figure A.7 – La signalisation quand un auditeur exécute un handover.

points d'ancrage (aMAR) et son emplacement actuel (cMAR). En cas de handover, le cMAR alloue un nouveau préfixe de réseau pour ce MN. Le cMAR envoie alors un PBU au CMD pour l'enregistrement de nouveau préfixe ainsi que récupère les adresses de MARs d'ancrage des sessions en cours. Ce message comprend le MN_ID et le préfixe alloué au courant. En regardant le tableau de BCE, le CMD met à jour l'entrée correspondante au MN_ID à l'emplacement actuel du MN. Le CMD répond alors par un PBA prolongé, y compris la liste des adresses précédentes et les préfixes correspondants. À la réception de ce message, le cMAR échange les messages PBU / PBA avec les aMARs afin de mettre à jour l'emplacement actuel du MN. Ainsi, le tunnel bidirectionnel est établi entre le cMAR et chaque aMAR, si nécessaire. En parallèle, les messages de transfert de contexte sont échangés entre le cMAR et le pMAR permettant le cMAR d'obtenir l'abonnement multicast active du MN. Pour chaque flux, le cMAR configure une interface « en amont » vers le MMA (si nécessaire), et envoie un rapport MLD au MMA à se joindre au flux multicast. Le MMA, après avoir rejoint l'arbre de distribution, transmet les paquets multicast au cMAR via le tunnel entre eux. Enfin, ils atteignent le MN.

A.4.2 Analyse Quantitative

Ce paragraphe présente l'analyse quantitative des différentes approches concernant différents paramètres tels que l'interruption de service, le délai de bout en bout, le coût de signalisation et la perte de paquets.

A.4.2.1 Le modèle du réseau et les métriques pour la performance

Le modèle de référence La figure A.8 présente une topologie de référence et les distances en saut entre les entités pour l'analyse de performance. A noter que l'intersection MR (IMR) est un router qui possède déjà un état d'acheminement pour le groupe. On définit alors l'échelle du réseau ψ qui est le ratio entre le nombre de sauts entre deux MAR adjacents (h_{mm}) et le nombre de sauts entre le MAR et le CMD (h_{cd}) .

$$\psi = \frac{h_{mm}}{h_{cd}}. \tag{A.1}$$

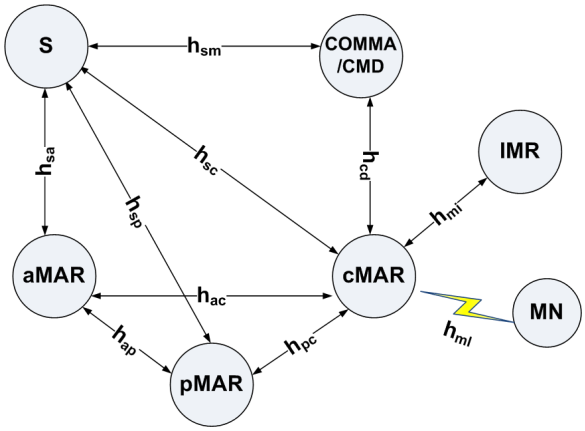


Figure A.8 – Une topologie de référence du réseau.

En règle générale, le nombre moyen de sauts entre deux MAR adjacents est inférieur à celui entre un MAR et une entité centralisée. Cela signifie que $\psi \leq 1$. Dans ce document, nous allons étudier l'impact de l'échelle du réseau sur les métriques de la performance en variant la valeur de ψ sur un intervalle [0,1].

Les messages liés à l'analyse de performance Dans notre analyse, différents messages sont utilisés. Pour un souci de simplicité, nous supposons qu'il existe un seul flux continu. L_{RS}, L_{RA}, L_{PBU}, L_{PBA}, L_{ePBU}, L_{ePBA}, L_{M-Req}, L_{M-Res}, L_{C-Req}, L_{C-Res}, L_{MLD-R}, L_{Join}, L_{MP}, L_T est la taille du message Router Solicitation (RS), Router Advertisement (RA), PBU, PBA, PBU étendu, PBA étendu, request de transfert de contexte, réponse de transfert de contexte, demande de configuration de canal, réponse de configuration de canal, Rapport MLD, PIM Rejoignez, paquet multicast, l'en-tête de tunnel; respectivement.

Le modèle de délai Dans cette thèse, on adopte le modèle de délai de transmission de paquets dans [134] dans lequel la transmission de paquets se compose la durée de transmission et le temps de propagation. Ainsi, le délai de transmission d'une liaison filaire peut être calculé comme

$$d_{wd}(l,h) = h(\frac{l}{BW_{wd}} + D_{wd}), \tag{A.2}$$

Où h est la distance en saut entre deux nœuds, l est la taille du paquet, BW_{wd} est la bande passante de liaison filaire et D_{wd} est la latence du liaison filaire.
Contrairement à la transmission filaire qui peut être considéré comme fiable, la liaison sans fil n'est pas fiable. Le délai de transmission sans fil est donc calculé comme [134]

$$d_{wl}(l) = \frac{1}{1-q}(\frac{l}{BW_{wl}} + D_{wl}), \tag{A.3}$$

où q est la probabilité d'échec de liaison sans fil, BW_{wl} est la bande passante et D_{wl} est la latence de liaison sans fil.

Le modèle de mobilité Dans ce document, nous considérons le cas où le MN se déplace toujours de MAR à MAR comme s'ils étaient déployés linéaire (l'utilisateur est en train de s'éloigner du premier MAR et jamais s'attache vers un MAR précédemment visité). Il représente le pire des cas. Ainsi, nous avons $h_{ac} = h_{ap} + h_{pc}$.

Soit N_{mar} représente le nombre moyen de MARs impliqués dans le transfert du trafic de données vers / depuis un MN. Dans notre contexte, N_{mar} est également le nombre de handovers. On obtient donc

$$h_{ac} = N_{mar} h_{mm}, \tag{A.4}$$

$$h_{pc} = h_{mm}. \tag{A.5}$$

Dans notre analyse, la valeur basse de N_{mar} représente le nœud avec la faible mobilité ou le scénario dans lequel le flux est à court durée. La valeur plus élevée de N_{mar} correspond à la forte mobilité ou le scénario dans lequel le flux est à long terme.

A.4.2.2 La modélisation analytique

Ce paragraphe développe un modèle d'analyse en ce qui concerne différents paramètres de performance. Dans cette analyse, nous considérons le cas normal et le cas où le proxy MLD supportant la capacité de multiples d'interfaces en amont. Nous soulignons ensuite les impacts et les avantages de l'utilisation de plusieurs interfaces sur ces métriques.

Le temps d'interruption du service Le temps d'interruption ($SD(.)$) est définie comme une période où un auditeur est incapable de recevoir les paquets multicast. En supposant que le temps associé au traitement des messages dans les entités de réseau (par exemple, le temps de traitement de PBU et de mise à jour de cache dans MAR) est inclus dans la valeur totale de chaque variable. Ensuite, le temps d'interruption est (voir la figure A.7).

$$\begin{aligned} SD(.) = T_{L2} + d_{wl}(L_{RS}) + d_{wd}(L_{ePBU}, h_{cd}) + d_{wd}(L_{ePBA}, h_{cd}) + max\{d_{wd}(L_{PBA}, h_{ac}) \\ + d_{wd}(L_{PBU}, h_{ac}), d_{wd}(L_{M-Req}, h_{pc}) + d_{wd}(L_{M-Res}, h_{pc})\} \\ + max\{d_{wl}(L_{MP}), T_M(.) + d_{wl}(L_{MP})\}, \end{aligned} \tag{A.6}$$

où T_{L2} est la durée de handover de la couche 2, $T_M(.)$ est le temps nécessaire pour le cMAR d'adhérer et obtenir le premier paquet après le handover.
En cas MMA_cMAR, le cMAR doit obtenir le trafic à partir de l'IMR qui a déjà un état d'acheminement pour ce groupe. Ainsi

$$T_M(cMAR) = \begin{cases} \overline{w}_{mr} \quad \text{if } h_{mi} = 0, \\ (h_{mi}+1)\overline{w}_{mr} + d_{wd}(L_{MLD-R}) + d_{wd}(L_{MP}) + d_{wd}(L_{Join}, h_{mi}-1) \\ +d_{wd}(L_{MP}, h_{mi}-1) \quad \text{if } h_{mi} \geq 1. \end{cases}$$

où $\overline{w}_m$ est le délai dans lequel un MR (et un proxy MLD) doit rejoindre un flux multicast à chaque routeur intermédiaire dans l'Internet [104].
En cas MMA_pMAR, le pMAR a eu l'état pour ce flux. Nous avons

$$T_M(pMAR) = 2\overline{w}_{mr} + d_{wd}(L_{MLD-R} + L_T, h_{pc}) + d_{wd}(L_{MP} + L_T, h_{pc}). \tag{A.7}$$

En cas MMA_aMAR, il y a deux possibilités : le cas normal (cas 1, correspond au mode par défaut), et le cas où le proxy MLD supportant plusieurs interfaces « en amont » est déployé dans MARs. Dans ce dernier cas, dans le pire des cas, l'aMAR doit rejoindre le canal multicast, conduisant à un délai supplémentaire. Soit p_a représentent la probabilité que cette situation se produit. En conséquence, $T_M(.)$ est calculé comme

$$T_M(aMAR) = (1-p_a)T_M(aMAR-c1) + p_a T_M(aMAR-wc), \tag{A.8}$$

où

$$T_M(aMAR-c1) = 2\overline{w}_{mr} + d_{wd}(L_{MLD-R} + L_T, h_{ac}) + d_{wd}(L_{MP} + L_T, h_{ac}), \tag{A.9}$$

$$T_M(aMAR-wc)=\begin{cases}T_M(aMAR-c1) & \text{if } h_{mi}=0,\\ T_M(aMAR-c1)+d_{wd}(L_{MLD-R})+d_{wd}(L_{MP})+d_{wd}(L_{Join},h_{mi}-1)\\ +(h_{mi}+1)\overline{w}_{mr}+d_{wd}(L_{MP},h_{mi}-1) & \text{if } h_{mi}\geq 1.\end{cases}$$

Il est à noter que $T_M(aMAR-c1)$ représente le temps d'interruption dans le mode par défaut, quand $T_M(aMAR)$ montre l'impact de l'utilisation de proxy avec plusieurs interfaces sur le temps d'interruption. En conséquence, $SD(aMAR)$ peut être considéré comme un compromis entre l'interruption de service et le problème de la convergence.
Dans le cas MMA_COMMA, nous avons

$$T_M(COMMA)=2\overline{w}_{mr}+d_{wd}(L_{MLD-R}+L_T,h_{cd})+d_{wd}(L_{MP}+L_T,h_{cd}). \tag{A.10}$$

Le délai de bout en bout Le délai de bout en bout ($E2E(.)$) est le délai de transmission de paquets de la source à l'auditeur. Dans le MMA_cMAR, le cMAR reçoit le trafic multicast directement à partir de l'infrastructure multicast. Par conséquent, le délai de bout-en-bout est donné par

$$E2E(cMAR)=d_{wd}(L_{MP},h_{sc})+d_{wl}(L_{MP}). \tag{A.11}$$

Dans le cas MMA_aMAR, le paquet multicast est acheminé depuis la source vers le cMAR via l'aMAR, représentant le mode par défaut. Nous avons

$$E2E(aMAR)=d_{wd}(L_{MP},h_{sa})+d_{wd}(L_{MP}+L_T,h_{ac})+d_{wl}(L_{MP}). \tag{A.12}$$

En cas MMA_pMAR, le MAR reçoit toujours le trafic de son pMAR dans le cas normal. Par conséquent, le délai de bout-en-bout est donné comme suit

$$E2E(pMAR{-}c1)=d_{wd}(L_{MP},h_{sa})+d_{wd}(L_{MP}+L_T,h_{ap})+d_{wd}(L_{MP}+L_T,h_{pc})+d_{wl}(L_{MP}). \tag{A.13}$$

En cas d'utilisation de proxy avec plusieurs interfaces, nous supposons que p_p est la probabilité que le MAR obtient le trafic multicast d'une interface « en amont ». Ainsi, $1-p_p$ est la probabilité que le MAR obtient le trafic multicast de son pMAR. Le délai dans le cas MMA_pMAR est donc donné par

$$\begin{aligned}E2E(pMAR)&=d_{wl}(L_{MP})+[d_{wd}(L_{MP},h_{sa})+N_{mar}d_{wd}(L_{MP}+L_T,h_{mm})]p_p^{N_{mar}-1}\\ &+\sum_{i=1}^{N_{mar}-1}[d_{wd}(L_{MP},h_i)+(N_{mar}-i)d_{wd}(L_{MP}+L_T,h_{mm})]p_p^{N_{mar}-i-1}(1-p_p),\end{aligned} \tag{A.14}$$

où h_i est la distance en saut de la source vers le i^{ime} MAR dans le chemin de déplacement du MN (de l'aMAR au cMAR), par exemple, $h_{N_{mar}-1}=h_{sp}$.
Considérant le MMA_COMMA, le délai de bout en bout est exprimé sous la forme

$$E2E(COMMA)=d_{wd}(L_{MP},h_{sm})+d_{wd}(L_{MP}+L_T,h_{cd})+d_{wl}(L_{MP}). \tag{A.15}$$

L'analyse du coût Dans ce paragraphe, le coût de signalisation ($SC(.)$), le coût de livraison de paquets ($PC(.)$) et le coût de tunnelisation ($TC(.)$) sont étudiés. Le coût de signalisation (per handover) est le frais général de signalisation pour soutenir le handover y compris les procédures relatives au multicast. Il peut être calculé comme

$$SC(.)=SC_{LU}+SC_M(.), \tag{A.16}$$

où SC_{LU}, $SC_M(.)$ est le coût pour la mise à jour de l'emplacement et les procédures relatives au multicast, respectivement. Le coût de signalisation est calculé comme le produit de la taille du message, la distance et le coût de transmission d'une unité dans une liaison filaire/sans fil (α pour le liaison filaire et β pour la liaison sans fil). SC_{LU} est donc donné par

$$SC_{LU} = \beta(L_{RS} + L_{RA}) + \alpha(L_{ePBU}h_{cd} + L_{ePBA}h_{cd}) + \alpha(L_{PBU}h_{ac} + L_{PBA}h_{ac}). \quad (A.17)$$

$SC_M(.)$ est calculé par

$$SC_M(cMAR) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R} + L_{Join}h_{mi}). \quad (A.18)$$

$$SC_M(pMAR) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{pc}). \quad (A.19)$$

$$SC_M(aMAR) = (1 - p_a)SC_M(aMAR - c1) + p_aSC_M(aMAR - wc), \quad (A.20)$$

où

$$SC_M(aMAR - c1) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{ac}), \quad (A.21)$$

$$SC_M(aMAR - wc) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{ac} + L_{MRD-R} + L_{Join}h_{mi}). \quad (A.22)$$

$$SC_M(COMMA) = \alpha(L_{M-Req}h_{pc} + L_{M-Res}h_{pc} + L_{MLD-R}h_{cd}). \quad (A.23)$$

Le coût de livraison représente le coût de livraison des paquets multicast pour le MN par unité de temps. Soit S_c, λ_p représentent la durée moyenne des séances au cMAR et le taux d'arrivée des paquets, respectivement. Encore, le coût dans le MMA_aMAR correspond au mode par défaut. Le coût est exprimé sous la forme

$$PC(cMAR) = S_c\lambda_p(\alpha L_{MP}h_{sc} + \beta L_{MP}). \quad (A.24)$$

$$PC(aMAR) = S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha(L_{MP} + L_T)h_{ac} + \beta L_{MP}]. \quad (A.25)$$

En cas MMA_pMAR, dans le cas normal, le MAR reçoit toujours le trafic multicast de son pMAR. Ainsi, le coût de livraison de paquets est donné comme suit

$$PC(pMAR - c1) = S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha(L_{MP} + L_T)(h_{ap} + h_{pc}) + \beta L_{MP}]. \quad (A.26)$$

En utilisant le proxy avec multiples interfaces, le coût de livraison est calculé comme étant

$$\begin{aligned} PC(pMAR) &= S_c\lambda_p\beta L_{MP} + S_c\lambda_p[\alpha L_{MP}h_{sa} + \alpha N_{mar}(L_{MP} + L_T)h_{mm}]p_p^{N_{mar}-1} \\ &+ S_c\lambda_p \sum_{i=1}^{N_{mar}-1} [\alpha L_{MP}h_i + \alpha(N_{mar} - i)(L_{MP} + L_T)h_{mm}]p_p^{N_{mar}-i-1}(1 - p_p). \end{aligned} \quad (A.27)$$

En cas MMA_COMMA, le coût de livraison de paquets est

$$PC(COMMA) = S_c\lambda_p[\alpha L_{MP}h_{sm} + \alpha(L_{MP} + L_T)h_{cd} + \beta L_{MP}]. \quad (A.28)$$

En ce qui concerne le coût de tunnelisation, il est défini comme le coût supplémentaire de la tête de tunnel. En MMA_cMAR, le trafic multicast est reçu directement à partir de l'infrastructure multicast, il n'y a donc pas de coût de tunnelisation. Au contraire, dans les cas MMA_aMAR, MMA_pMAR et MMA_COMMA le trafic est routé via le tunnel aMAR-cMAR, pMAR-cMAR, et cMAR-COMMA, respectivement. A noter que le coût de tunnelisation dans le cas MMA_aMAR correspond au mode multicast par défaut. Le coût

de tunnelisation est donc calculé comme

$$TC(cMAR) = 0. \tag{A.29}$$

$$TC(aMAR) = \alpha S_c \lambda_p (L_{MP} + L_T) h_{ac}. \tag{A.30}$$

$$TC(pMAR) = \alpha S_c \lambda_p (L_{MP} + L_T) h_{mm} \sum_{i=0}^{N_{mar-1}} (N_{mar} - i) p_p^{N_{mar-i-1}} (1 - \theta p_p). \tag{A.31}$$

où

$$\theta = \begin{cases} 0 & \text{if } i = 0, \\ 1 & \text{if } i \geq 1. \end{cases}$$

$$TC(COMMA) = \alpha S_c \lambda_p (L_{MP} + L_T) h_{cd}. \tag{A.32}$$

Le coût de signalisation en général, est un facteur important qui influence l'évolutivité du réseau. Cependant, en tant que le plan de données et le plan de contrôle ne sont plus couplés, dans le cas où une grande quantité de trafic est générée dans le réseau, le coût de livraison de paquets et le coût de tunnelisation jouent le rôle plus important.

La perte de paquets Pendant le handover, les paquets peuvent être perdus. Le nombre de paquets perdus est proportionnel à la durée de l'interruption du service, et le taux d'arrivée des paquets. En conséquence, le nombre de paquets perdus est donné par

$$\varphi_p(.) = \lambda_p SD(.). \tag{A.33}$$

A.4.2.3 Les résultats numériques

Ce paragraphe présente les résultats numériques basés sur l'analyse donnée dans le paragraphe précédent. Les valeurs des paramètres par défaut sont présentées dans le tableau A.1, dans lequel L_{PBU}, L_{PBA}, L_{ePBU}, L_{ePBA}, L_{M-Req}, L_{M-Res}, L_{C-Req} et L_{C-Res} sont extraites de l'implémentation réelle de PMIPv6 [155] et de fonction de transfert de contexte [161], tandis que les autres sont de [73, 69, 177, 161]. Il est à noter que le $SD(aMAR-c1)$, $E2E(aMAR)$, $SC(aMAR-c1)$, $PC(aMAR)$ et $TC(aMAR)$ correspondent au mode par défaut dans notre analyse.

Table A.1 – Paramètres pour l'analyse de la performance.

Paramètre	**Valeur**	**Paramètre**	**Valeur**	**Paramètre**	**Valeur**
T_{L2}	50ms	BW_{wd}	100Mbps	BW_{wl}	11 Mbps
D_{wd}	2ms	D_{wl}	10ms	q	0.35
$\overline{w}_{mr}$	10 ms	h_{mm}	3 sauts	h_{cd}	12 sauts
h_{mi}	2 sauts	h_{sa}	16 sauts	h_{sp}	16 sauts
h_{sc}	16 sauts	h_{sm}	16 sauts	S_c	60 s
λ_p	10 paquets/s	α	1	β	5
p_p	0.9	p_a	0.5	L_{RS}	52 octets
L_{RA}	80	L_{PBU}	84	L_{PBA}	92 octets
L_{ePBU}	84 octets	L_{ePBA},	128 octets	L_{M-Req}	86 octets
L_{M-Res}	104 octets	L_{C-Req}	92 octets	L_{C-Res}	112 octets
L_{MLD-R}	96 octets	L_{Join}	110 octets	L_{MP}	200 octets
L_T	40 octets				

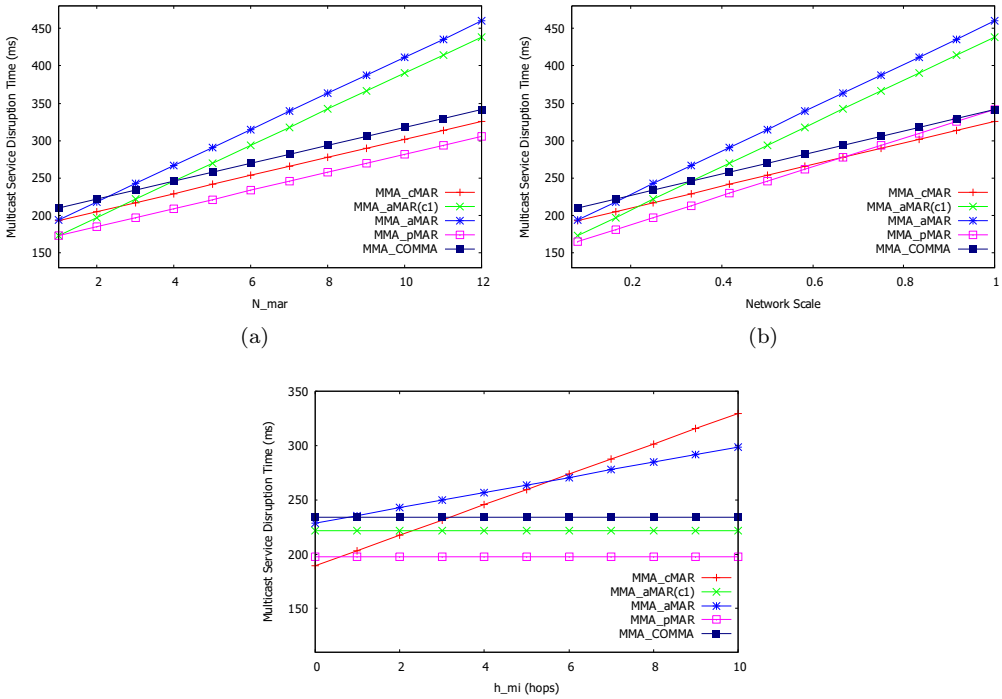


Figure A.9 – Le temps d'interruption comme une fonction de : (a) N_{mar}, (b) ψ, (c) h_{mi}.

Le temps d'interruption de service multicast La figure A.9a montre le temps d'interruption de service quand N_{mar} est variée sur une intervalle de 1 à 12. Il apparaît clairement que l'approche MMA_pMAR donne une meilleure performance que les autres. Lorsque N_{mar} est faible (moins de 5), toutes les approches satisfont à l'exigence en termes d'interruption pour les services en temps réel (inférieur à 300 ms). Lorsque N_{mar} est relativement grande, l'interruption de service en cas MMA_aMAR est significativement augmentée. Nous étudions aussi l'impact de l'échelle du réseau (ψ) sur le temps d'interruption. Dans ce cas, N_{mar} est réglée à une valeur de 3. D'une manière générale, l'impact de ψ est similaire à celui de N_{mar}. Surtout, Fig. A.9b montre qu'il existe une zone où le MMA_cMAR surpasse le MMA_pMAR (lorsque $\psi \geq 0.62$).
La figure A.9c indique le temps d'interruption lorsque h_{mi} est variée sur une intervalle de 0 à 10 sauts. Une petite valeur de h_{mi} indique un scénario de forte densité d'auditeur et une valeur élevée de h_{mi} représente un scénario de faible densité d'auditeur. Le temps d'interruption dans le MMA_pMAR est plus faible que dans les autres (sauf si $h_{mi} = 0$ indiquant le cas où le trafic multicast est déjà disponible au MR « en amont » du cMAR). Comme la valeur de h_{mi} augmente, le temps d'interruption dans le MMA_pMAR, MMA_aMAR (c1) et MMA_COMMA est maintenu constant alors que celui dans les autres cas est considérablement augmenté. Par conséquent, la différence entre les approches est augmentée. En outre, le temps d'interruption dans MMA_cMAR dépend fortement de la valeur de h_{mi}. En d'autres termes, il ne peut pas être garantie à l'approche MMA_cMAR. En outre, dans MMA_aMAR, il augmente de manière significative comparé à celui dans le cas MMA_aMAR (c1) à la suite de l'utilisation du proxy avec plusieurs interfaces.

En conclusion, l'approche MMA_pMAR est généralement bien adaptée pour les services sensibles à l'interruption. Ainsi, l'augmentation du temps d'interruption, qui est causée par les multiples interfaces, peut être considérée comme un compromis entre le temps

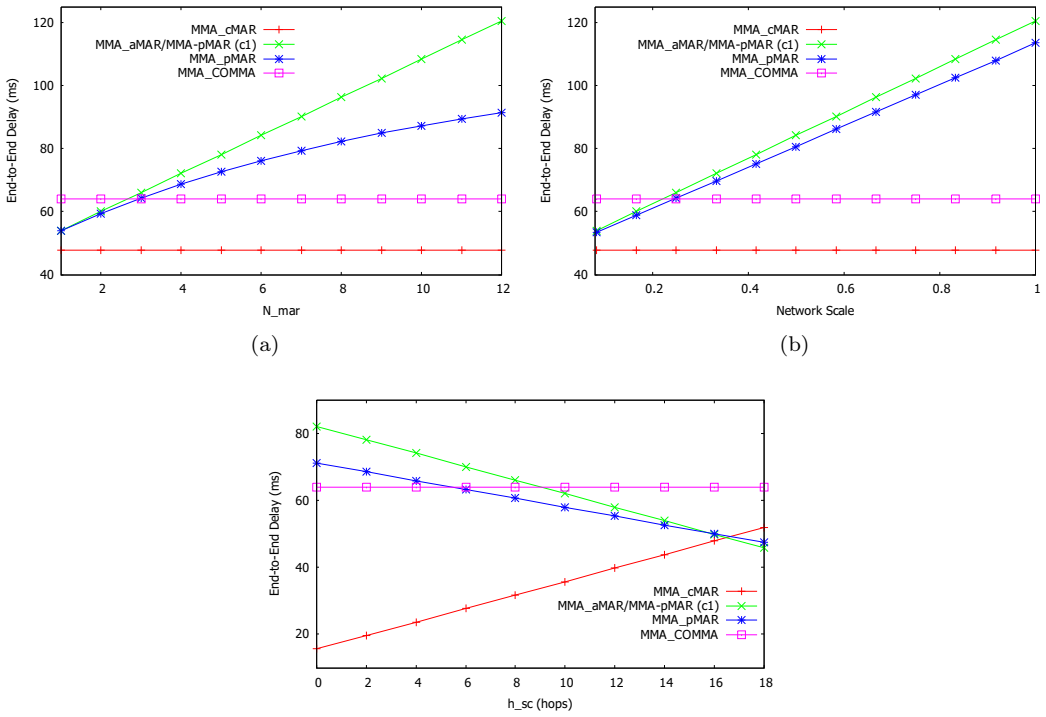
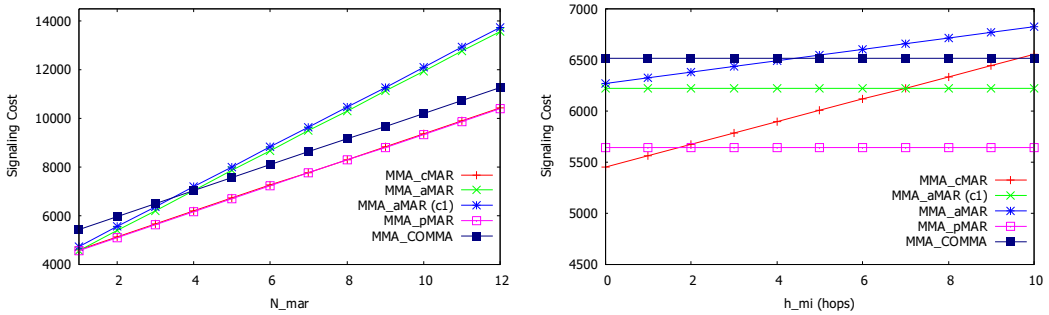


Figure A.10 – Le délai de bout en bout en fonction de : (a) N_{mar}, (b) ψ, (c) h_{sc}.

d'interruption et le problème de la convergence.

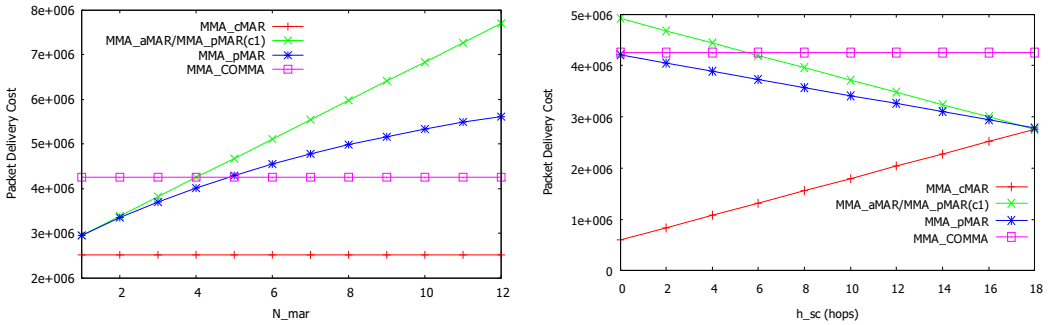
Le délai de bout en bout Maintenant, nous étudions l'impact de N_{mar} sur le délai de bout-en-bout. La figure A.10a montre le délai par rapport au nombre de handovers N_{mar}. Comme N_{mar} augmente (h_{ca} augmente) le délai en cas MMA_aMAR et MMA_pMAR augmente rapidement, tandis que celui dans MMA_cMAR et MMA_COMMA est maintenu constant. A noter que le délai dans MMA_cMAR est maintenu en dessous de la valeur de 50 ms. Cela signifie que MMA_cMAR satisfait à la exigence stricte en termes de délai de bout-en-bout. Le délai dans MMA_pMAR (c1) est supérieur à celui dans le MMA_pMAR à la suite de l'utilisation de multiples interfaces « en amont ». Comme on peut le voir sur la figure A.10b. En général, l'échelle du réseau a un impact similaire sur le délai de bout en bout que N_{mar}. La différence majeure est que l'augmentation de la ligne MMA_pMAR dans la figure A.10b est plus rapide que celle dans la figure A.10a.
Ensuite, N_{mar} est réglé à une valeur de 6 (correspondant aux flux à moyen / long terme et aux nœuds à moyen / haute mobilité), tandis que la valeur de h_{sc} est variée. A ce stade, nous supposons que $h_{sa} + h_{sc}$ est une valeur fixe, par exemple, 18 sauts et $h_{sp} = h_{sc}$. Ce scénario est utilisé pour illustrer le cas où la source est très proche de l'aMAR (côté droit de la figure A.10c) ou très proche du cMAR (côté gauche de la figure A.10c). Comme on peut le voir sur la figure A.10c, même lorsque la source est très proche de l'aMAR, l'approche MMA_cMAR donne une meilleure performance en termes de délai de bout en bout que les autres. Ainsi, l'impact du tunnel de la mobilité sur le délai est évident. En conclusion, le cMAR est généralement bien adapté pour les flux sensibles aux délais.



(a) (b)

Figure A.11 – Le coût de signalisation comme une fonction de: (a) N_{mar}, (b) h_{mi}.

Le coût de signalisation La figure A.11 montre le coût de signalisation en fonction de N_{mar} et h_{mi}. En général, le coût de signalisation augmente lorsque N_{mar} augmente. Sur la figure A.11a, le coût de signalisation dans le cas MMA_cMAR et MMA_pMAR est inférieur à celui dans les autres cas. Quand N_{mar} est assez petite, le coût de signalisation en cas MMA_COMMA devient plus élevé. Dans le cas contraire, le coût en cas MMA_aMAR devient plus élevé. Comme on peut le voir sur la figure A.11b (quand h_{mi} est variée), le MMA_pMAR surpasse les autres quand h_{mi} est supérieur à 2.



(a) (b)

Figure A.12 – Le coût de livraison de paquets en termes de: (a) N_{mar}, (b) h_{sc}.

Le coût de livraison de paquets Similaire au délai de bout en bout, le coût de livraison de paquets (en fonction de N_{mar}) en cas MMA_cMAR et MMA_COMMA est maintenu constant tandis que dans le cas MMA_aMAR et MMA_pMAR est fortement augmenté. La figure A.12b montre le coût de livraison en fonction de h_{sc} quand $h_{sa} + h_{sc}$ est fixé (18 sauts). Il apparaît clairement que le coût dans le cas MMA_cMAR est nettement inférieur à celui dans les autres, même lorsque la source est très proche de l'aMAR. En outre, nous pouvons observer que ce coût en cas MMA_pMAR (c1) est supérieur à celui de MMA_pMAR en raison de multiples interfaces.

Le coût de tunnelisation En ce qui concerne le coût de tunnelisation, la figure A.13 montre le coût de tunnelisation en fonction de N_{mar}. Le MMA_cMAR n'introduit pas des surcharges de tunnel, alors que le coût de tunnelisation dans le MMA_COMMA est fixé. D'autre part, il est significativement augmenté quand N_{mar} augmente en cas MMA_aMAR

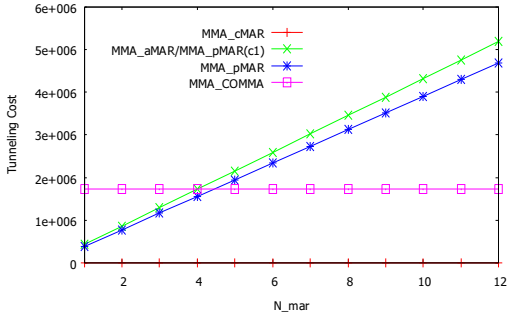


Figure A.13 – Le coût de tunnelisation comme une fonction de N_{mar}.

et MMA_pMAR. Encore une fois, en appliquant les multiples interfaces, le coût de tunnelisation en cas MMA_pMAR augmente légèrement.

A.4.2.4 Conclusion de la partie d'analyse quantitative

De l'analyse de la performance et des résultats numériques, nous concluons qu'aucune des approches est toujours meilleure que les autres. Par exemple, le MMA_pMAR est généralement un bon choix lorsqu'on considère l'interruption de service. Le MMA_cMAR, en revanche, est un choix préféré en ce qui concerne le délai de bout en bout. Les autres approches peuvent être les plus appropriées, cependant, dans une situation spécifique. L'analyse de performance donne aussi une idée de l'utilisation d'un MMA commun (COMMA) qui sert comme un point d'ancrage seule pour le service multicast pour tous les nœuds dans le domaine, donc reflétant le déploiement PMIPv6. Bien que cette approche présente une performance acceptable, par exemple, quand N_{mar} et ψ sont petites, COMMA pose un goulot d'étranglement et un point de panne unique. COMMA n'est pas non plus un bon choix quand un contenu local est disponible. Par conséquent, la comparaison entre le MMA_COMMA et le mode par défaut donne l'idée de la performance de DMM en ce qui concerne PMIPv6 concernant le service multicast.
Essentiellement, la performance des méthodes dépend de différents facteurs tels que le nombre de handovers (N_{mar}, qui peut être considérée comme une fonction de la vitesse et du rayon de sous-réseau), l'échelle de réseau (ψ), la position de la source (h_{sc}, h_{sa}) et la densité de l'auditeur (h_{mi}). Ce sont les raisons pour lesquelles un MMA fixe n'est pas une bonne stratégie. En outre, les utilisateurs mobiles quotidiens consacrent jusqu'à 62 % de leur temps à la maison et au travail (en général, l'emplacement typique) [202]. Ainsi, dans certains cas, l'emplacement typique serait également un bon candidat. Même les ancres de mobilité sont distribuées, certaines d'entre elles sont surchargées plus que les autres [200]. En conséquence, un support par flux de multicast doit être fourni.

A.4.3 La sélection dynamique de l'ancre multicast

Dans ce paragraphe, un mécanisme de sélection dynamique de l'ancre de mobilité multicast sera introduit. Sur la base des contextes collectés, le MMA sera sélectionné de façon dynamique afin de répondre à un ensemble des exigences. D'un point de vue du service, il contribue à satisfaire les exigences en termes de l'interruption de service et le délai, en particulier lorsqu'on considère des services en temps réel. Il fournit également un mécanisme permettant de mieux répartir la charge entre MARs. D'autres problèmes telles que la duplication de paquets et le laisser la latence (perte de ressources) peuvent être réduits. La sélection de MMA prend en compte non seulement le contexte de service multicast, mais

aussi le contexte de la mobilité du nœud et le contexte de réseau, ainsi permettant une support multicast par flux. En d'autres termes, chaque flux multicast peut être traité différemment selon differents contextes. La sélection de MMA peut être fait dynamiquement quand un flux est initié ou lorsque l'auditeur effectue un handover grâce au proxy MLD supportant plusieurs interfaces en amont.
Pour sélectionner dynamiquement le MMA approprié, des contextes différents doivent être pris en compte comme le contexte de service multicast, le contexte de la mobilité du MN, et le contexte de réseau. Chaque contexte peut être affecté à un numéro de priorité. Par exemple, une valeur plus faible indique que le contexte est plus important. A ce stade, similaire au mode par défaut, quand un auditeur initie un flux multicast, le cMAR servira comme le MMA pour ce flux (le trafic multicast sera reçu directement à partir de l'infrastructure multicast). Cela signifie que la sélection MMA dans la phase initiale sera laissée pour les travaux au futur. Pour un flux de handover, le trafic multicast peut être reçu de l'aMAR, le pMAR, le cMAR, ou même un MAR dans lequel le canal multicast est déjà disponible, ou un MAR moins chargé afin de répondre à un ensemble des exigences.
Notre solution n'est pas seulement pour les problèmes de l'interruption de service et de délai de bout en bout, mais aussi pour autres problèmes liées au service multicast. Ainsi, elle peut offrir des avantages tels que :

- *Une solution complète* pour la plupart des problèmes de l'auditeur liées à la mobilité (y compris l'interruption de service, le problème de convergence, le laisser de latence, le gaspillage des ressources, le routage sous-optimal et la perte de paquets);

- *La route optimale* : Les flux multicast seront acheminés dans un mieux chemin, car ils ne passent pas toujours par leur ancre de mobilité.

- *Evitant du problème de convergence du tunnel* : Cette solution peut résoudre complètement le problème de la convergence;

- *L'utilisation dynamique de tunnel de mobilité* : L'utilisation de tunnel de la mobilité pour les sessions multicast en cours est activée dans les cas appropriés, par exemple, pour un contenu à distant, ou un canal avec des exigences de délai très strict;

- *Gestion efficace du tunnel* : Dans un environnement DMM, il est impossible d'effectuer une pré-établir tous les tunnels entre MARs puisque le nombre de MARs est censé être grand. En permettant au proxy MLD avec multiples interfaces en amont, il peut causer la gestion complexe de tunnel (par exemple, l'entretien et la vie du tunnel). Ainsi, la solution proposée, qui est basée sur le module de gestion de la mobilité multicast, peut aider à résoudre ce problème;

- *Répartition de la charge de flux multicast* : Puisque la sélection MMA prend la charge actuelle du MAR en compte, elle permet de meilleur répartir la charge de trafic multicast entre MARs.

- *La gestion centralisée des canaux multicast* : L'entité centrale (Multicast Control Entity, ou MCE) recueille et gère les contextes considérés (par exemple, les canaux multicast et leur portée (locale ou distante)), améliorant le contrôle des fournisseurs de réseau;

- *Possibilité d'être appliquée à la mobilité de la source multicast*;

- *Compatibilité avec la mobilité unicast.*

A.4.3.1 Les contextes considérés

Le contexte du service multicast Lorsque les services sont sensibles à l'interruption ou à la perte de paquets, le temps d'interruption de service doit être minimisé. Par exemple, il devrait être inférieur à 300ms pour un service en temps réel, tandis que 500 ms pour un service normal [162]. Pour le service sensible au délai de bout en bout, un long tunnel de mobilité ce qui peut entraîner un haut retard, doit être évité. La recommandation UIT-T G.114 [204] suggère que si le temps de transmission unidirectionnelle de connexion peut être maintenu en dessous de 150 ms, la plupart des applications connaîtront une interactivité transparente. En outre, les flux à longue durée peuvent effectuer de nombreuses handovers tandis que les flux à courte durée semblent être lancé et terminé au même MAR sans effectuer aucun handover.

Le contexte du nœud mobile Un nœud mobile à haute mobilité effectue souvent des handovers. Si le trafic multicast est toujours acheminé par aMAR, le temps de séjour plus long, le plus grave de l'impact sera. En outre, le nombre de points d'ancrage et de tunnels peut être augmenté. Au contraire, pour le nœud de faible mobilité, le MN devrait rester à un ou plusieurs MARs la plupart du temps.

Le contexte du réseau La sélection MMA peut également être basée sur plusieurs contextes de réseau tels que la charge actuelle de MAR, la proximité géographique du MAR au MN ainsi que la politique de canal multicast. Par exemple, lorsque la charge de MAR est élevée, il peut entraîner de retard et de perte de paquets si ce MAR est sélectionné comme un point d'ancrage multicast. Dans ce cas, le moins chargé MAR (entre MARs qu'ont l'état de transmission multicast pour ce canal) peut être un candidat potentiel. La raison est que si le canal est déjà disponible au MAR sélectionné, le temps d'interruption peut être réduit au minimum (pas besoin de temps pour rejoindre le canal multicast). En outre, avec une augmentation négligeable de la charge, ce MAR peut transférer le trafic vers le cMAR [28].

A.4.3.2 La description de l'architecture de la solution proposée

Afin de collecter et gérer les contextes considérés, une entité de réseau, appelé MCE est introduite. Le MAR met régulièrement à jour le contexte de MN et la charge actuelle de MAR au MCE en utilisant une extension de PBU / PBA (ou une extension de messages Heartbeat [205]). Le MCE gère également tous les canaux multicast dans le domaine. Le contexte de service peut être définie basé sur la classe de QoS.
Résidant dans le MAR, le module de gestion de la mobilité (MUMO) prend la responsabilité de toutes les actions liées à la mobilité multicast. La structure de ce module est illustrée dans la figure A.14 et brièvement décrite comme suit :

- La fonction de gestion de groupe multicast (MGMF) réfère aux opérations de gestion de groupe et de stockage de l'information, qui est basée sur le proxy MLD avec plusieurs interfaces en amont[1]. Ce module prend également en charge la fonction explicite de suivi afin de maintenir un état du groupe de multicast par le client [51]. Elle se fait sur la base de Multicast Mobility Database (MMD), qui stocke les entrées avec les informations suivantes : i) l'identification de MN (MN_ID); l'adresse de MN; et les abonnements des MNs. En outre, il maintient une structure de compteur pour le nombre d'auditeurs par canal multicast, ce qui permet d'identifier si un nœud est le dernier abonné du groupe.

[1] Ce module peut également être invoqué la fonction de routeur multicast par exemple, MRDv6.

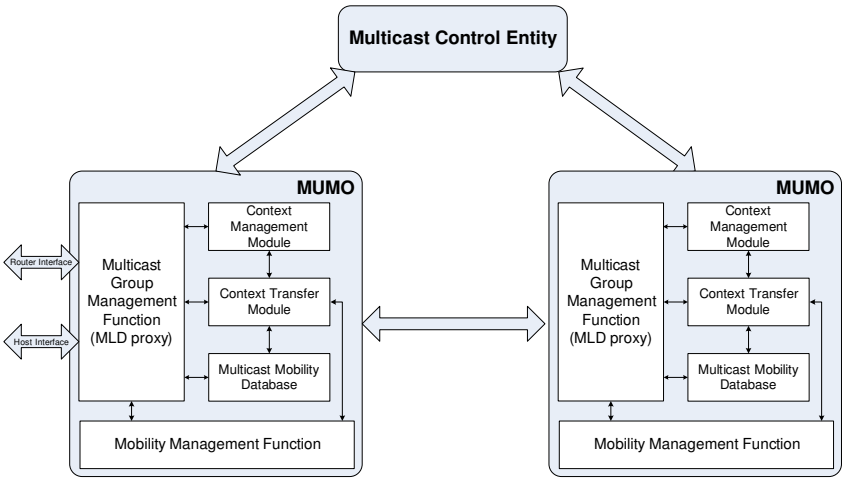


Figure A.14 – Le module de gestion de la mobilité multicast (MUMO) à MAR.

- La fonction de gestion de contexte (CMF) communique avec le MCE pour récupérer les informations de configuration de canaux, y compris l'adresse de MMA correspondant, et le type de MMA (le précédent, l'ancrage, et le MAR courant ou autre). Basé sur cette information, le proxy MLD configure ses interfaces en amont vers les MARs correspondants.
- La fonction de transfert de contexte multicast (MCTF) est responsable d'échanger des informations d'abonnement multicast de MN entre MARs. Alors que le nouveau MAR peut rejoindre le flux courant à l'avance pour minimiser le temps d'interruption.
- La fonction de gestion de mobilité (MMF) ressemble à la pile de protocole de mobilité. Elle est responsable de l'attribution et le maintien de la connectivité IP d'un MN exécutant un handover à l'intérieur du domaine DMM. En d'autres termes, il est responsable de toutes les actions liées à la gestion de mobilité.

A.4.3.3 Les opérations de la solution proposée

Les opérations de la solution sont brièvement présentées comme suit. Une fois que le MN entre dans un domaine de DMM (attache à MAR1), un préfixe est attribué à lui (dire Pref1). Le MAR1 envoie alors un message PBU y compris l'identification du MN (MN_ID) et le Pref1 au CMD pour enregistrer ce MN. Après avoir reçu le PBU, le CMD crée une BCE qui se compose du MN_ID, le Pref1, et l'adresse de MAR1 (comme aMAR) pour ce MN. En réponse, le message PBA est envoyé de CMD à MAR1 pour informer que l'emplacement de MN est mis à jour. Le MAR1 envoie un message RA y compris le Pref1 au MN. Le MN, après avoir configuré son adresse IPv6, peut adhérer à un flux multicast via le MAR courant.
En cas de handover (voir figure A.15), le cMAR alloue un nouveau préfixe pour ce MN (appelé Pref2). Le cMAR envoie alors un PBU au CMD pour le nouveau enregistrement de préfixe. Ce message comprend le MN_ID, et le Pref2. En regardant le tableau BCE, le CMD met à jour l'entrée correspondante au MN_ID à l'emplacement actuel du MN. Le CMD répond alors par un message PBA, y compris la liste des adresses des points d'ancrage, les préfixes correspondants, et l'adresse du MAR précédent. À la réception de ce message, le cMAR échange les messages PBU/PBA avec MARs d'ancrage pour mettre à jour l'emplacement actuel du MN. Ainsi, le tunnel bidirectionnel est établi entre le cMAR

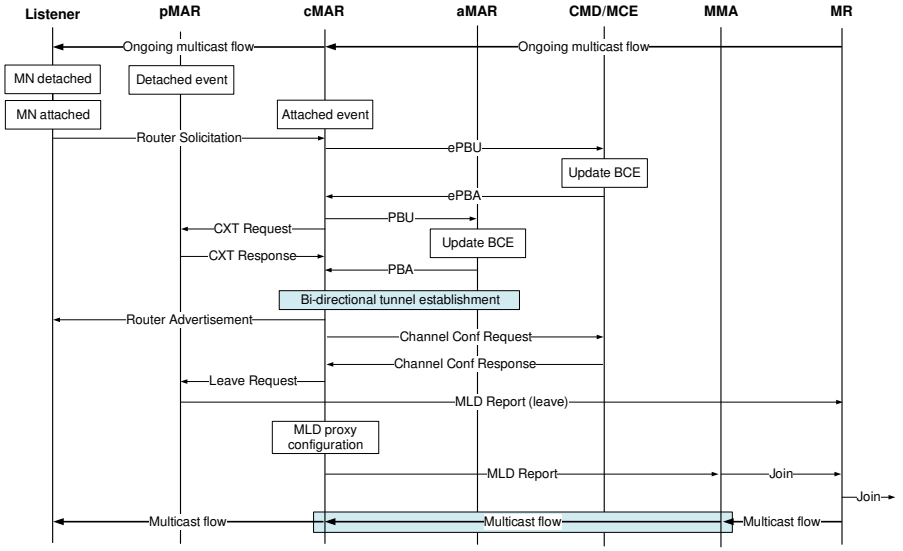


Figure A.15 – La signalisation liée au service multicast avec la fonction de transfert de contexte multicast.

et l'aMAR, si nécessaire. Le cMAR envoie alors un message RA, y compris le nouveau préfixe alloué au MN. Le MN peut donc configurer son adresse IPv6 et commencer une nouvelle communication avec le CN. En parallèle, les messages de transfert de contexte multicast sont échangés entre le cMAR et le pMAR permettant le cMAR d'obtenir les flux multicast en cours. Basé sur ces informations, le cMAR contacts avec le MCE pour obtenir les configurations de canaux qui composent les informations suivantes (par canal) : S, G, l'adresse de MMA, et un champ indiquant le rôle de MMA. Les messages PBU / PBA peuvent être étendus à transmettre la configuration de canal. Le cMAR configure une interface en amont vers le MMA, et envoie un rapport MLD au MMA pour rejoindre le canal multicast en cours. Après avoir rejoint l'arbre de transmission multicast (si nécessaire), le MMA transmet les paquets multicast au cMAR, et ils ont finalement atteint le MN. Si le cMAR ne reçoit pas le trafic multicast du pMAR, il demandera le pMAR pour arrêter la transmission du flux. Merci à la fonction explicite de suivi, le pMAR s'arrête la transmission du flux si le MN est le dernier membre de ce flux. Ainsi, il réduit le temps de latence et le gaspillage des ressources.

A.4.3.4 L'implémentation de la solution proposée

Une première version du DMMA était disponible grâce au projet Medieval [161, 206, 23]. Dans ce mode de réalisation, le module CMF exécute de façon simple : lorsque le MN agit comme un auditeur, le cMAR joue toujours le rôle du MMA. Au contraire, l'aMARs agit comme le MMA lorsque le MN joue le rôle d'une source. Cependant, les procédures pour l'acquisition des contextes considérés sont encore en cours de développement. Le module MMF est aussi en cours de développement basé sur la mise en œuvre de l'OAI PMIPv6. Les autres modules comme le MGMF et le MCTF sont déjà disponibles. Dans la prochaine étape, la mise en œuvre complète du module CMF sera déployée. Des expériences seront ensuite effectuées basé sur un banc d'essai proche d'un réseau réel.

A.5 Conclusion et Perspectives

Le volume de données dans les réseaux mobiles est en plein essor principalement dû au succès des smartphones et des tablettes. Basé sur le fait que le trafic de l'Internet mobile sera dominé par la vidéo, l'évolutivité et l'efficacité de la bande passante de routage multicast permettent le multicast IP jouera un rôle plus important. Cependant, quand considérant le multicast IP dans un environnement mobile sans fil, il soulève plusieurs problèmes telles que l'interruptions de service, le délai de bout-en-bout, la duplication de paquets, le routage non-optimal et le gaspillage de ressources.
Pour résoudre ces problèmes, cette thèse propose des solutions dans les environnements PMIPv6 et DMM. Grâce à cette thèse, les objectifs suivants sont atteints :

- *Identifier les enjeux et les défis de la mobilité d'un nœud multicast et des métriques pour évaluer le mécanisme pour la mobilité d'un nœud multicast*
- *Proposer une méthode expérimentale pour atteindre les résultats réalistes à faible coût* : La méthode expérimentale est proposé comme une combinaison des techniques de la virtualisation et de la simulation. Un banc d'essai PMIPv6 a été donc mis en œuvre.
- *Présenter une méthode efficace pour optimiser la continuité de service en PMIPv6 et déployer un banc d'essai proche d'un réseau réel pour la mobilité d'un nœud multicast* : La solution proposée est basée sur le transfert de contexte multicast et la fonction de suivi explicite permettant au nouveau MAG pour obtenir les informations d'abonnement de MN à l'avance, ce qui réduit l'interruption de service.
- *Proposer un mécanisme d'équilibrage de charge des flux multicast dans PMIPv6* : La solution proposée permet de mieux répartir la charge entre LMAs à améliorer l'évolutivité et la fiabilité du système.
- *Introduire une solution pour le handover d'un nœud avec multiples interfaces dans des réseaux hétérogènes* : L'interface logique est utilisé en tant que la couche abstraite pour masquer le changement de l'interface physique de la pile IP. Merci à ce mécanisme, le MN n'est pas conscient de la mobilité du point de vue du service multicast.
- *Présenter un support à la mobilité inter-domaine pour les réseaux PMIPv6 et un support de base pour la mobilité de l'auditeur dans un environnement inter-domaine.*
- *Proposer un mécanisme de sélection dynamique de l'ancre de mobilité multicast (DMMA) dans l'environnement DMM*: Le DMMA non seulement supporte les services pour satisfaire l'exigence stricte en termes d'interruption et de délai de bout en bout, mais offre également des avantages tels que l'évitement du problème de la convergence, la gestion efficace du tunnel, le routage optimal, la réduction du gaspillage de ressources et la répartition de la charge.

Les bénéficie des solutions proposées Une partie du mécanisme DMMA a été mis en œuvre dans le projet MÉDIÉVAL. Ce projet vise à fournir une architecture pour améliorer l'Internet mobile actuel et fournir des applications vidéo mobiles de manière plus efficace. Une solution multi-couche a été développée dans laquelle deux services typiques liés au multicast sont considérés comme le Mobile TV et le PBS. En ce qui concerne le support de la mobilité de nœud multicast, une solution à la fois pour l'auditeur et la source dans DMM a été fournie. Dans le cadre de la solution globale, le module de mobilité de multicast qui gère le soutien à la mobilité IP pour les flux multicast a été mis en œuvre. En plus d'informations, le transfert de contexte de multicast et la fonction explicite de suivi sont utilisés pour accélérer le processus d'acquisition de souscription du MN à réduire le temps d'interruption. Pour l'auditeur, le paquet multicast est toujours reçu directement

de l'infrastructure multicast au MAR courant. Pour la source, le paquet multicast est acheminé à partir du MAR courant à celui d'ancrage par le tunnel de mobilité.
Dans le projet VELCRI, la solution pour un handover sur des réseaux hétérogènes est une partie du système de communication (y compris la communication véhicules-au-Grid et la communication Grid-aux-véhicules) pour fournir le service de charge pour le véhicule électrique. Le système de communication permet à l'EV à toujours être relié au Smart Grid en utilisant différentes technologies dans les différentes phases telles que LTE tout en conduisant, WLAN en approchant une station de recharge, et PLC tout en étant amarré à une station de recharge.
Dans le projet SYSTUF, le DMMA sera utilisé pour fournir le service multicast pour les utilisateurs sur les transports publics, par exemple dans le tram et le métro. Dans plus de détails, le but du projet est de définir et de mettre en œuvre de nouveaux services à haut débit et un système de communication entre le sol et les véhicules en mouvement pour améliorer la qualité des transports urbains. Le DMMA sera étudié dans un scénario de forte mobilité.

Perspectives Avec la volonté de soutenir les services multicast IP dans un environnement mobile sans fil, cette thèse propose des solutions pour les problèmes liés à la mobilité d'un nœud multicast. Toutefois, puisqu'il y a plusieurs sujets définis, plusieurs aspects ne peuvent pas être analysés dans les détails, ce qui peuvent potentiellement être améliorés. Par exemple, alors que l'objectif de cette thèse a été jusqu'ici sur la mobilité de l'auditeur de multicast, la même idée peut être appliquée à la mobilité de la source.
Un autre sujet, qui serait considéré, est la mobilité du nœud. Autres modèles de mobilité seraient appliqués pour étudier l'impact de modèle de mobilité sur la performance de la solution. Il peut être fait en utilisant le modèle de mobilité existant dans NS-3.
Comme la solution DMMA n'a été validée que par l'analyse mathématique, un banc d'essai DMM est en cours de déploiement. En outre, la prédiction de mobilité peut être utilisé pour améliorer la performance de DMMA qui permet de sélectionner le point d'ancre de mobilité de multicast adapté non seulement lors de l'exécution d'un handover, mais aussi au moment où le flux multicast est initié.
L'intérêt croissant pour la technologie LTE par les opérateurs apporte le service Multicast/Broadcast Multimedia Service (MBMS) retour à l'ordre du jour pour soutenir l'augmentation exponentielle des services de distribution multimédia sur les réseaux cellulaires dans les prochaines années. Comme nous ne considérons pas la technologie d'accès sans fil spécifique, la mobilité d'un nœud multicast serait considéré dans l'architecture 3GPP.
A l'avenir, des milliards de véhicules seront connectés aux réseaux, qui créent de nouveaux défis et opportunités pour les opérateurs de réseau. Par conséquent, le mécanisme DMMA doit être envisagé, par exemple, pour les utilisateurs dans les véhicules à grande vitesse.
Enfin, nous devons mettre notre solution dans la relation avec d'autres technologies comme le Software Defined Networking (SDN), l'Internet of Thing (IoT) et le Cloud Computing. Par exemple, la technique SDN peut changer le réseau de base en permettant un déploiement distribué optimisé des instances virtualisées de passerelles mobiles. Cela pourrait faire beaucoup plus souple le façon de traiter les paquets et les flux IP. En outre, depuis les applications de IoT y compris l'ITS attirent de grand intérêt récemment, le support de la mobilité dans l'IoT aussi gagné beaucoup de l'élan. D'autre part, les avantages du Cloud Computing continuent de prendre de l'élan significatif. Comme les applications en cours d'exécution sur le Cloud sont des médias riches, ou des applications de collaboration, le multicast IP peut offrir des avantages pour les utilisateurs, ainsi que pour les opérateurs [208]. En outre, la répartition de l'infrastructure Cloud Computing entre les différents opérateurs de réseau influence également le scénario de développement de DMM [209].

Appendix B
List of Publications

The results obtained in this dissertation have been published (submitted) in:

1. T.-T. Nguyen and C. Bonnet, "Considerations of IP Multicast for Load Balancing in Proxy Mobile IPv6 Networks", Accepted for publication in Computer Network, Elsevier, Jul 2014.
2. T.-T. Nguyen, R. Costa, and C. Bonnet, "Experimental evaluation of wireless mo- bile networks: from methodology to a testbed", Submitted to Wireless Networks, Springer, May 2014.
3. T.-T. Nguyen and C. Bonnet, "On the Efficiency of Dynamic Multicast Mobility Anchor Selection in DMM: Use Cases and Analysis", ICC, Jun 2014.
4. T.-T. Nguyen and C. Bonnet, "Load Balancing Mechanism for Proxy Mobile IPv6 Networks: An IP Multicast Perspective", ICNC 2014, CNC workshop, Feb 2014.
5. T.-T. Nguyen, C. Bonnet, and J. Härri, "Proxy mobile IPv6 for electric vehicle charging service: Use case and analysis", PIMRC, Sep 2013.
6. T.-T. Nguyen and C. Bonnet, "Efficient multicast content delivery over a distributed mobility management environment", VTC2013-Fall, Sep 2013.
7. T.-T. Nguyen and C. Bonnet, "DMM-based Inter-domain Mobility Support for Proxy Mobile IPv6", WCNC, Apr 2013.
8. T.-T. Nguyen and C. Bonnet, "Performance Optimization of Multicast Content Delivery in a Mobile Environment based on PMIPv6", WCNC, Apr 2013.
9. T.-T. Nguyen and Christian Bonnet, "Optimizing Multicast Content Delivery over Novel Mobile Networks", ICNS, Mar 2013.
10. S. Figueiredo, C. Guimarães, R.-L Aguiar, T.-T. Nguyen, L. Yadin, N. Carapeto, and C. Parada, "Broadcasting User Content over Novel Mobile Network", ICC, Jun 2013.
11. S. Figueiredo, M. Wetterwald, T.-T. Nguyen, L. Eznarriaga, N. Amram, and R.-L. Aguiar, "SVC multicast video mobility support in MEDIEVAL project", FUTURENET 2012, Jul 2012.
12. T.-T. Nguyen, C. Bonnet, and J. Härri, "Proxy mobile IPv6 for electric vehicle charging service: Use case and analysis", Research Report RR-12-271, 2013.
13. T.-T. Nguyen and C. Bonnet, "IP mobile multicast : problems and solutions", Research report RR-11-252, 2011.

Bibliography

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2012-2017," White Paper, Cisco Inc., Feb. 2013.

[2] S. Kurnia, H. Lee, and S. Yang, "Understanding consumers' expectations of mobile data services in australia," in *Management of Mobile Business (ICMB)*, July 2007.

[3] "Cisco vni service adoption forecast, 2012–2017'," White Paper, Cisco Inc., 2013.

[4] "Tablet demand and disruption: Mobile users come of age'," Blue Paper, Morgan Stanley, Feb. 2011.

[5] A. Smith, "Mobile access 2010," Pew Research Center, Tech. Rep., Jul. 2010.

[6] "Ericsson mobility report: On the pulse of the networked society," Ericsson, Tech. Rep., Jun. 2013.

[7] (2009, Jun.) Telefonica sees arpu decline as data grows and voice falls. [Online]. Available: http://www.mobileeurope.co.uk/News-Analysis/telefonica-sees-arpu-decline-as-data-grows-and-voice-falls

[8] H. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen. (2013, Dec.) Requirements for distributed mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-dmm-requirements-12

[9] H. A. Chan, H. Yokota, J. Xie, P. Seite, and D. Liu, "Distributed and dynamic mobility management in mobile internet: Current approaches and issues," *Journal of Communications*, vol. 6, no. 1, 2011.

[10] H. Chan. (2011, Oct.) Problem statement for distributed and dynamic mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/search/draft-chan-distributed-mobility-ps-05

[11] T. Schmidt, M. Waehlisch, and G. Fairhurst, "Multicast mobility in mobile ip version 6 (mipv6): Problem statement and brief survey," RFC 5757, Feb. 2010.

[12] I. Romdhani, M. Kellil, H.-Y. Lach, A. Bouabdallah, and H. Bettahar, "Ip mobile multicast: Challenges and solutions," *Communications Surveys Tutorials, IEEE*, vol. 6, no. 1, pp. 18–41, 2004.

[13] S. Figueiredo, M. Wetterwald, T.-T. Nguyen, L. Eznarriaga, N. Amram, and R. L. Aguiar, "SVC multicast video mobility support in MEDIEVAL project," in *FUTURENET 2012, Future Network and Mobile Summit*, Jul. 2012.

[14] C. Bonnet, T.-T. Nguyen, S. Figueiredo, D. Gomes, and C. Bernardos, "Deliverable 4.2: Ip multicast mobility solutions for video services," Medieval project, Deliverable, Jun. 2011.

[15] S. Figueiredo, D. Corujo, S. Jeon, T.-T. Nguyen, C. Bonnet, L. Marchetti, E. Demaria, M. Marchisio, T. Melia, R. Costa, F. Giust, C. Bernardos, A. de la Oliva, N. Carapeto, and C. Parada, "Dileverable 4.3: Final specification for mobility components and interfaces," Medieval project, Deliverable, Jun. 2012.

[16] T.-T. Nguyen and C. Bonnet, "Performance optimization of multicast content delivery in a mobile environment based on pmipv6," in *Wireless Communications and Networking Conference (WCNC)*, April 2013.

[17] T.-T. Nguyen, C. Bonnet, and J. Harri, "Proxy mobile ipv6 for electric vehicle charging service: Use cases and analysis," in *Personal Indoor and Mobile Radio Communications (PIMRC)*, 2013.

[18] T.-T. Nguyen and C. Bonnet, "Load balancing mechanism for proxy mobile ipv6 networks: An ip multicast perspective," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2014.

[19] ——, "On the efficiency of dynamic multicast mobility anchor selection in dmm: Use cases and analysis," in *IEEE International Conference on Communications (ICC)*, Jun 2014.

[20] ——, "Efficient multicast content delivery over a distributed mobility management environment," in *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*, 2013.

[21] ——, "Dmm-based inter-domain mobility support for proxy mobile ipv6," in *Wireless Communications and Networking Conference (WCNC)*, April 2013.

[22] ——, "Optimizing multicast content delivery over novel mobile networks," in *ICNS 2013, 9th International Conference on Networking and Services*, Mar. 2013.

[23] S. Figueiredo, C. Guimarães, R. L. Aguiar, T.-T. Nguyen, N. Carapeto, and C. Parada, "Broadcasting user content over novel mobile networks," in *ICC 2013, IEEE International Conference on Communications*, Jun. 2013.

[24] T.-T. Nguyen and C. Bonnet, "Considerations of ip multicast for load balancing in proxy mobile ipv6 networks," Accepted for publication in Computer Networks, Elsevier, Jan. 2014.

[25] T.-T. Nguyen, R. Costa, and C. Bonnet, "Experimental evaluation of wireless mobile networks: from methodology to a testbed," Submitted to Wireless Networks, Springer, May 2014.

[26] S. E. Deering, "Multicast routing in internetworks and extended lans," in *Symposium Proceedings on Communications Architectures and Protocols*, ser. SIGCOMM '88, 1988.

[27] S. Deering, "Host extensions for ip multicasting," RFC 1112, Aug. 1989.

[28] B. Williamson, *Developing IP Multicast Networks, Volume I.* Cisco Press, Oct. 1999.

[29] H. Eriksson, "Mbone: The multicast backbone," *Commun. ACM*, vol. 37, no. 8, pp. 54–60, Aug. 1994.

[30] Ipv6 multicast address space registry. [Online]. Available: http://http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

[31] A. El-Sayed, V. Roca, and L. Mathy, "A survey of proposals for an alternative group communication service," *Network, IEEE*, vol. 17, no. 1, pp. 46–51, 2003.

[32] Y.-h. Chu, S. G. Rao, and H. Zhang, "A case for end system multicast (keynote address)," in *Proceedings of the 2000 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, 2000.

[33] "Lte broadcast: A revenue enabler in the mobile media era," White Paper, Ericsson, Feb. 2013.

[34] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet group management protocol, version 3," RFC 3376, Oct. 2002.

[35] R. Vida and L. Costa, "Multicast listener discovery version 2 (mldv2) for ipv6," RFC 3810, Jun. 2004.

[36] D. Waitzman, C. Partridge, and S. Deering, "Distance vector multicast routing protocol," RFC 1075, Nov. 1988.

[37] J. Moy, "Multicast extensions to ospf," RFC 1584, Mar. 1994.

[38] A. Ballardie, "Core based trees (cbt) multicast routing architecture," RFC 2201, Sep. 1997.

[39] ——, "Core based trees (cbt version 2) multicast routing," RFC 2189, Sep. 1997.

[40] A. Adams, J. Nicholas, and W. Siadak, "Protocol independent multicast - dense mode (pim-dm): Protocol specification (revised)," RFC 3973, Jan. 2005.

[41] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol independent multicast - spare mode (pim-sm): Protocol specification (revised)," RFC 4601, Aug. 2006.

[42] B. Fenner, H. He, B. Haberman, and H. Sandick, "Internet group management protocol (igmp)/multicast listener discovery (mld)-based multicast forwarding (igmp/mld proxying)," RFC 4605, Aug. 2006.

[43] B. Quinn and K. Almeroth, "IP Multicast Applications: Challenges and Solutions," RFC 3170, Sep. 2001.

[44] A. Benslimane, *Multimedia Multicast on the Internet*. John Wiley & Sons Ltd, Jan. 2007.

[45] R. Rümmler, A. D. Gluhak, and H. Aghvami, *Multicast in Third-Generation Mobile Networks: Services, Mechanisms and Performance*. John Wiley & Sons Ltd, Mar. 2009.

[46] S. Bhattacharyya, "An overview of source-specific multicast (ssm)," RFC 3569, Jul. 2003.

[47] H. Holbrook and B. Cain, "Source-specific multicast for ip," RFC 4607, Aug. 2006.

[48] H. Holbrook, B. Cain, and B. Haberman, "Using internet group management protocol version 3 (igmpv3) and multicast listener discovery protocol version 2 (mldv2) for source-specific multicast," RFC 4604, Aug. 2006.

[49] W. Fenner, "Internet group management protocol, version 2," RFC 2236, Nov. 1997.

[50] S. Deering, W. Fenner, and B. Haberman, "Multicast listener discovery (mld) for ipv6," RFC 2710, Oct. 1999.

[51] H. Asaeda. (2013, Dec.) Igmp/mld-based explicit membership tracking function for multicast routers. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-pim-explicit-tracking-09

[52] C. Makaya and P. Samuel, "An architecture for seamless mobility support in ip-based next-generation wireless networks," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 2, pp. 1209–1225, 2008.

[53] Z. Zhu, R. Wakikawa, and L. Zhang, "A survey of mobility support in the internet," RFC 6301, Jul. 2011.

[54] I. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-ip-based wireless systems," *Wireless Communications, IEEE*, vol. 11, no. 4, pp. 16–28, 2004.

[55] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, "Mobility and handoff management in vehicular networks: A survey," *Wirel. Commun. Mob. Comput.*, vol. 11, no. 4, pp. 459–476, Apr. 2011.

[56] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00, 2000.

[57] M. Atiquzzaman and A. Reaz, "Survey and classification of transport layer mobility management schemes," in *Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2005.

[58] E. Wedlund and H. Schulzrinne, "Mobility support using sip," in *ACM International Workshop on Wireless Mobile Multimedia (WOWMOM)*, 1999.

[59] H. Schulzrinne and E. Wedlund, "Application-layer mobility using sip," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 4, no. 3, pp. 47–57, Jul. 2000.

[60] D. Damic, *Introducing L3 network-based mobility management for mobility-unaware IP hosts*. Springer Netherlands, 2007, pp. 195–205.

[61] D. Saha, A. Mukherjee, I. Misra, and M. Chakraborty, "Mobility support in ip: A survey of related protocols," *IEEE Network*, vol. 18, pp. 34 – 40, 2004.

[62] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

[63] H. Soliman, "Mobile ipv6 support for dual stack hosts and routers," RFC 5555, Jun. 2009.

[64] P. Bertin, S. Bonjour, and J.-M. Bonnin, "Distributed or centralized mobility?" in *Proceedings of the 28th IEEE Conference on Global Telecommunications, GLOBECOM*, 2009.

[65] F. Giust, A. De La Oliva, C. J. Bernardos, and R. Da Costa, "A network-based localized mobility solution for distributed mobility management," in *Wireless Personal Multimedia Communications (WPMC)*, 2011, pp. 1–5.

[66] J.-H. Lee, J.-M. Bonnin, P. Seite, and H. Chan, "Distributed ip mobility management from the perspective of the ietf: motivations, requirements, approaches, comparison, and challenges," *Wireless Communications, IEEE*, vol. 20, no. 5, pp. 159–168, 2013.

[67] T. Condeixa and S. Sargento, "Dynamic mobile ip anchoring," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 3607–3612.

[68] H. Ali-Ahmad, M. Ouzzif, P. Bertin, and X. Lagrange, "Distributed dynamic mobile ipv6: Design and evaluation," in *Wireless Communications and Networking Conference (WCNC)*, 2013.

[69] ——, "Distributed mobility management: Approaches and analysis," in *Communications Workshops (ICC), 2013 IEEE International Conference on*, 2013.

[70] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in ipv6," RFC 3775, Jun. 2004.

[71] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, "Routing optimization security in mobile ipv6," *Computer Networks*, vol. 50, no. 13, pp. 2401 – 2419, 2006.

[72] C. Makaya and P. Samuel, "An analytical framework for performance evaluation of ipv6-based mobility management protocols," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 3, pp. 972–983, 2008.

[73] J.-H. Lee, J.-M. Bonnin, I. You, and T.-M. Chung, "Comparative handover performance analysis of ipv6 mobility management protocols," *Industrial Electronics, IEEE Transactions on*, vol. 60, no. 3, pp. 1077–1088, 2013.

[74] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical mobile ipv6 mobility management (hmipv6)," RFC 5380, Oct. 2008.

[75] R. Koodli, "Mobile ipv6 fast handovers," RFC 5568, Jul. 2009.

[76] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile ipv6," RFC 5213, Aug. 2008.

[77] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, "The network access identifier," RFC 4282, Dec. 2005.

[78] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy mobile ipv6," RFC 5949, Sep. 2010.

[79] K. Hong and S. Lee, "Dynamic multi-step paging scheme in pmipv6-based wireless networks," *Wireless Networks*, vol. 18, no. 1, pp. 33–44, Jan. 2012.

[80] J.-H. Lee, T.-M. Chung, S. Pack, and S. Gundavelli, "Shall we apply paging technologies to proxy mobile ipv6?" in *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture*, ser. MobiArch '08, 2008, pp. 37–42.

[81] J.-E. Kang, D.-W. Kum, Y. Li, and Y.-Z. Cho, "Seamless handover scheme for proxy mobile ipv6," in *Wireless and Mobile Computing, Networking and Communications (WIMOB)*, Oct 2008.

[82] G. Kim, "Low latency cross layer handover scheme in proxy mobile ipv6 domain," in *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, ser. Lecture Notes in Computer Science, vol. 5174, 2008.

[83] L. Magagula and H. Chan, "Ieee802.21 optimized handover delay for proxy mobile ipv6," in *Military Communications Conference (MILCOM)*, Nov 2008.

[84] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, and A. Dutta, "Localized routing for proxy mobile ipv6," RFC 6705, Sep. 2012.

[85] A. Rasem, C. Makaya, and M. St-Hilaire, "O-pmipv6: Efficient handover with route optimization in proxy mobile ipv6 domain," in *Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2012.

[86] G. Giaratta, "Interactions between pmipv6 and mipv6: Scenarios and related issues," RFC 6612, May 2012.

[87] N. Neumann, J. Lei, X. Fu, and G. Zhang, "I-pmip: An inter-domain mobility extension for proxy-mobile ip," in *IWCMC*, Jun. 2009.

[88] Z. Ma, K. Wang, and F. Zhang. (2012, Jan.) Network-based inter-domain handover support for pmipv6'. Internet draft. [Online]. Available: https://tools.ietf.org/html/draft-ma-netext-pmip-handover-02

[89] "3rd generation partnership project (3gpp); technical specification group services and system aspects; network architecture (release 12)," TS, 3GPP TS 23.002, Dec. 2012.

[90] J. L. P. Seite, P. Bertin. (2013, Feb.) Distributed mobility anchoring. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-seite-dmm-dma-07

[91] F. G. CJ. Bernardos, A. de la Oliva. (2013, Jul.) A pmipv6-based solution for distributed mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-bernardos-dmm-pmip-02

[92] ——. (2013, Jul.) An ipv6 distributed client mobility management approach using existing mechanisms. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-bernardos-dmm-cmip-00

[93] T. Nguyen and C. Bonnet, "Dmm-based inter-domain mobility support for proxy mobile ipv6," in *Wireless Communications and Networking Conference (WCNC)*, 2013.

[94] J. Korhonen, T. Savolainen, and S. Gundavelli. (2013, Jul.) Local prefix lifetime management for proxy mobile ipv6. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-korhonen-dmm-local-prefix-01

[95] T. Melia and S. Gundavelli. (2013, Oct.) Logical interface support for multi-mode ip hosts. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-netext-logical-interface-support-08

[96] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (nemo) basic support protocol," RFC 3963, Jan. 2005.

[97] R. Droms, P. Thubert, F. Dupont, W. Haddad, and C. Bernardos, "Dhcpv6 prefix delegation for network mobility (nemo)," RFC 6276, Jul. 2011.

[98] N. Montavont and T. Noel, "Handover management for mobile nodes in ipv6 networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 38–43, Aug 2002.

[99] X. Pérez-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, Oct. 2003.

[100] J.-H. Lee, T.-M. Chung, and S. Gundavelli, "A comparative signaling cost analysis of hierarchical mobile ipv6 and proxy mobile ipv6," in *Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep 2008.

[101] J.-H. Lee, T. Ernst, and T.-M. Chung, "Cost analysis of ip mobility management protocols for consumer mobile devices," *Consumer Electronics, IEEE Transactions on*, vol. 56, no. 2, pp. 1010–1017, May 2010.

[102] T. G. Harrison, C. L. Williamson, W. L. Mackrell, and R. B. Bunt, "Mobile multicast (mom) protocol: Multicast support for mobile hosts," in *Annual ACM/IEEE International Conference on Mobile Computing and Networking*, ser. MobiCom '97, 1997.

[103] C. Lin and K.-M. Wang, "Mobile multicast support in ip networks," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2000.

[104] S.-J. Yang and S.-H. Park, "A dynamic service range-based multicast routing scheme using rsvp in mobile ip networks," in *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE*, vol. 4, 2001, pp. 2395–2399 vol.4.

[105] H.-S. Shin, Y.-J. Suh, and D.-H. Kwon, "Multicast routing protocol by multicast agent in mobile networks," in *Parallel Processing, 2000. Proceedings. 2000 International Conference on*, 2000.

[106] C. Jelger and T. Noel, "Multicast for mobile hosts in ip networks: progress and challenges," *Wireless Communications, IEEE*, vol. 9, no. 5, pp. 58–64, Oct 2002.

[107] G. A. Leoleisa, G. N. Prezerakosb, and I. S. Venierisa, "Seamless multicast mobility support using fast mipv6 extensions," *Computer Communications*, vol. 29, no. 18, pp. 3745 – 3765, 2006.

[108] T. Schmidt, M. Waehlisch, R. Koodli, G. Fairhurst, and D. Liu. (2013, Dec.) Multicast listener extensions for mipv6 and pmipv6 fast handovers. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-multimob-fmipv6-pfmipv6-multicast-02

[109] D.-H. Kwon, W.-J. Kim, Y.-S. Kim, W.-S. Im, and Y.-J. Suh, "Design and implementation of an efficient multicast support scheme for fmipv6," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006.

[110] T. Schmidt and M. Wählisch, "Morphing distribution trees—on the evolution of multicast states under mobility and an adaptive routing scheme for mobile ssm sources," *Telecommunication Systems*, vol. 33, no. 1-3, pp. 131–154, 2006.

[111] O. Christ, T. Schmidt, and M. Wahlisch, "Towards seamless handovers in ssm source mobility an evaluation of the tree morphing protocol," in *Next Generation Mobile Applications, Services and Technologies (NGMAST)*, Sep 2008.

[112] H. Lee, S. Han, and J. P. Hong, "Efficient mechanism for source mobility in source specific multicast," in *Information Networking (ICOIN), 2006 International Conference on*, 2006.

[113] Z. Kovácsházi and R. Vida, "Host identity specific multicast," in *Third Intenational Conference on Networking and Services, ICNS*, jun 2007.

[114] L. Wang, S. Gao, H. Zhang, T. Schmidt, and J. Guan, "Mobile multicast source support in pmipv6 networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 152, 2013.

[115] H. Asaeda, H. Liu, and Q. Wu, "Tuning the behavior of the internet group management protocol (igmp) and multicast listener discovery (mld) for routers in mobile and wireless networks," RFC 6636, May 2012.

[116] L. Contreras, C. Bernardos, and I. Soto. (2013, Dec.) Pmipv6 multicast handover optimization by the subscription information acquisition through the lma (sial). Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-multimob-handover-optimization-07

[117] J. Zuniga, L. Contreras, C. Bernardos, S. Jeon, and Y. Kim, "Multicast mobility routing optimizations for proxy mobile ipv6," RFC 7028, Sep. 2013.

[118] T. Schmidt, S. Gao, H. Zhang, and M. Waehlisch. (2014, Jan.) Mobile multicast sender support in proxy mobile ipv6 (pmipv6) domains. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-multimob-pmipv6-source-07

[119] T. Schmidt, M. Waehlisch, and S. Krishnan, "Base deployment for multicast listener support in proxy mobile ipv6 (pmipv6) domains," RFC 6224, Apr. 2011.

[120] H.-K. Zhang, S. Gao, T. C.Schmidt, B. hao Feng, and L.-L. Wang. (2013, Jul.) Multi-upstream interfaces igmp/mld proxy. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-zhang-pim-muiimp-01

[121] Y. Li, W. Chen, L. Su, D. Jin, and L. Zeng, "Proxy mobile ipv6 based multicast listener mobility architecture," in *Wireless Communications and Networking Conference (WCNC)*, 2009, pp. 1–6.

[122] M. Gohar, S. I. Choi, and S.-J. Koh, "Fast handover using multicast handover agents in pmipv6-based wireless networks," in *Information Networking (ICOIN), 2011 International Conference on*, 2011, pp. 367–372.

[123] J.-H. Lee, T. Ernst, D.-J. Deng, and H.-C. Chao, "Improved pmipv6 handover procedure for consumer multicast traffic," *Communications, IET*, vol. 5, no. 15, pp. 2149–2156, 2011.

[124] L. Contreras, C. Bernardos, and I. Soto, "On the efficiency of a dedicated lma for multicast traffic distribution in pmipv6 domains," in *5th ERCIM Workshop in eMobility*, Jun. 2011.

[125] S. Jeon, N. Kang, and Y. Kim, "Mobility management based on proxy mobile ipv6 for multicasting services in home networks," *Consumer Electronics, IEEE Transactions on*, vol. 55, no. 3, pp. 1227–1232, August 2009.

[126] J. Guan, H. Zhou, C. Xu, H. Zhang, and H. Luo, "The performance analysis of the multicast extension support for proxy mipv6," *Wireless Personal Communications*, vol. 61, no. 4, pp. 657–677, 2011.

[127] L. Wang, H. Zhou, Y. Qin, J. Guan, H. Zhang, and I. You, "Design and analysis of efficient multicast sender mobility scheme for proxy mobile ipv6," in *MobiWorld Workshop, IEEE Consumer Communications and Networking Conference, CCNC*, Jan. 2014.

[128] S. Figueiredo, S. Jeon, and R. L. Aguiar. (2013, Oct.) Ip multicast use cases and analysis over distributed mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-sfigueiredo-multimob-use-case-dmm-03

[129] S. Figueiredo, S. Jeon, and R.-L. Aguiar, "Use-cases analysis for multicast listener support in network-based distributed mobility management," in *Personal Indoor and Mobile Radio Communications (PIMRC)*, Sep 2012.

[130] S. Jeon, S. Figueiredo, and R. Aguiar, "A channel-manageable ip multicast support framework for distributed mobility management," in *Wireless Days (WD), 2012 IFIP*, Nov 2012.

[131] J.-H. Lee and T.-M. Chung, "How much do we gain by introducing route optimization in proxy mobile ipv6 networks?" *annals of telecommunications*, vol. 65, no. 5-6, pp. 233–246, 2010.

[132] Y. Fang, "Movement-based mobility management and trade off analysis for wireless mobile networks," *IEEE Trans. Comput*, pp. 791–803, 2003.

[133] H. Li, Y. Cheng, C. Zhou, and W. Zhuang, "Minimizing end-to-end delay: A novel routing metric for multi-radio wireless mesh networks," in *INFOCOM 2009, IEEE*, April 2009, pp. 46–54.

[134] J. McNair, I. Akyildiz, and M. Bender, "An inter-system handoff technique for the imt-2000 system," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1, 2000, pp. 208–216 vol.1.

[135] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling.* Wiley-Interscience, may 1991.

[136] E. Nourbakhsh, J. Dix, P. Johnson, R. Burchfield, S. Venkatesan, N. Mittal, and R. Prakash, "Assert: A wireless networking testbed," *LNCS*, vol. 46, pp. 209–218, 2011.

[137] S. Kurkowski, T. Camp, and M. Colagrosso, "Manet simulation studies: the incredibles," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9(4), p. 50– 61, Oct. 2005.

[138] S. Mehta, N. Ullah, H. Kabir, N. Sultana, and K. S. Kwak, "A case study of networks simulation tools for wireless networks," in *Proc. Third Asia International Conference on Modelling & Simulation (AMS'09)*, May 2009, pp. 661 – 666.

[139] K. Pawlikowski, H.-D. Jeong, and J.-S. Lee, "On credibility of simulation studies of telecommunication networks," *Communications Magazine, IEEE*, vol. 40, no. 1, pp. 132–139, 2002.

[140] M. Weigle, "Improving confidence in network simulations," in *Simulation Conference, 2006. WSC 06. Proceedings of the Winter*, 2006, pp. 2188–2194.

[141] D. Cavin, Y. Sasson, and A. Schiper, "On the accuracy of manet simulators," in *POMC'02*, 2002.

[142] J. Montavont, E. Ivov, and T. Noel, "Analysis of mobile ipv6 handover optimizations and their impact on real-time communication," in *Wireless Communications and Networking Conference (WCNC)*, March 2007.

[143] L. X. et al., "Virtual wifi: Bring virtualization from wired to wireless," in *Proc of the 7th ACM SIGPLAN/SIGOPS international conference on Virtual execution environments*, 2011, pp. 181–192.

[144] Y. Zaki, L. Zhao, C. Görg, and A. Timm-Giel, "Lte mobile network virtualization," *Mobile Networks and Applications (MONET), ACM Journal*, pp. 1–9, 2011.

[145] D. Menascé, "Virtualization: Concepts, applications, and performance modeling," in *In Proc. of The Computer Measurement Group's 2005 International Conference*, Dec. 2005.

[146] "Understanding full-virtualization, para-virtualization and hardware-assist," White Paper, VMware, Nov. 2007.

[147] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles*, ser. SOSP '03, 2003.

[148] J. Dike, *User Mode Linux*. Prentice Hall, 1996.

[149] W. Chen, H. Lu, L. Shen, Z. Wang, N. Xiao, and D. Chen, "A novel hardware assisted full virtualization technique," in *Young Computer Scientists (ICYCS)*, 2008.

[150] S. Singhal, G. Hadjichristofi, I. Seskar, and D. Raychaudhri, "Evaluation of uml based wireless network virtualization," in *Next Generation Internet Networks (NGI)*, Apr. 2008.

[151] T. R. Henderson, S. Roy, S. Floyd, and G. F. Riley, "Ns-3 project goals," in *Proceeding from the 2006 Workshop on Ns-2: The IP Network Simulator*, ser. WNS2 '06. New York, NY, USA: ACM, 2006.

[152] Wireshark homepage. [Online]. Available: http://www.wireshark.org/

[153] Tcpdump homepage. [Online]. Available: http://www.tcpdump.org/

[154] Tun/tap devices. [Online]. Available: http://user-mode-linux.sourceforge.net/old/UserModeLinux-HOWTO-6.html/

[155] Oai pmipv6, homepage. [Online]. Available: http://www.openairinterface.org/openairinterface-proxy-mobile-ipv6-oai-pmipv6/

[156] Pmipv6 implementation in ns-3, homepage. [Online]. Available: http://code.google.com/p/pmip6ns3/

[157] Mpi for distributed simulation. [Online]. Available: http://www.nsnam.org/docs/release/3.11/models/html/distributed.html

[158] A. Alvarez, R. Orea, S. Cabrero, X. G. Pañeda, R. García, and D. Melendi, "Limitations of network emulation with single-machine and distributed ns-3," in *International ICST Conference on Simulation Tools and Techniques*, ser. SIMUTools '10, 2010.

[159] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, "Context transfer protocol (cxtp)," RFC 4067, Jul. 2005.

[160] R. Gerhards, "The syslog protocol," RFC 5424, Mar. 2009.

[161] L. M. et al., "Deliverable d4.4: Final operational mobility architecture," Medieval project, Deliverable, Dec. 2012.

[162] "3rd generation partnership project (3gpp); requirements for evolved utra (e-utra) and evolved utran (e-utran) (release 9)," TR, 3GPP TR 25.913, Dec. 2009.

[163] J. Korhonen, S. Gundavelli, H. Yokota, and X. Cui, "Runtime local mobility anchor (lma) assignment support for proxy mobile ipv6," RFC 6463, Feb. 2012.

[164] J. Korhonen and V. Devarapalli, "Local mobility anchor (lma) discovery for proxy mobile ipv6," RFC 6097, Feb. 2011.

[165] H. Kong, S. Oh, M. Kim, and H. Choo, "Load balancing of local mobility anchors in proxy mobile ipv6 networks," in *Proceedings of the Second Asia-Pacific Symposium on Internetware*, ser. Internetware '10, 2010, pp. 16:1–16:5.

[166] S. Jeon, R. Aguiar, and N. Kang, "Load-balancing proxy mobile ipv6 networks with mobility session redirection," *Communications Letters, IEEE*, vol. 17, no. 4, pp. 808–811, April 2013.

[167] H.Zhang, S. Gao, T. C.Schmidt, B. hao Feng, and L.-L. Wang. (2013, Jul.) Multiple upstream interfaces igmp/mld proxy'. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-zhang-pim-muiimp-01

[168] M.-S. Kim and S. Lee, "Load balancing and its performance evaluation for layer 3 and ieee 802.21 frameworks in pmipv6-based wireless networks," *Wirel. Commun. Mob. Comput.*, vol. 10, no. 11, pp. 1431–1443, Nov. 2010.

[169] F. Xia, B. Sarikaya, J. Korhonen, S. Gundavelli, and D. Damic, "Radius support for proxy mobile ipv6," RFC 6572, Jun. 2012.

[170] S. Krishnan, S. Gundavelli, M. Liebsch, H. Yokota, and J. Korhonen. (2012, Oct.) Update notifications for proxy mobile ipv6. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-krishnan-netext-update-notifications-01

[171] R. Jain, "Throughput fairness index: An explanation," in *ATM Forum/99-0045*, Feb. 1999.

[172] Iperf, homepage. [Online]. Available: http://sourceforge.net/projects/iperf/.

[173] Mint, homepage. [Online]. Available: http://mc-mint.sourceforge.net/.

[174] D. Smith, "Ip tv bandwidth demand: Multicast and channel surfing," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007.

[175] T. G. Yonas Tsegaye, "Ospf convergence times," Master Thesis, Chalmers University of Technology, Goteborg, Sweden, 2012.

[176] "Example: Configuring ospf timers." [Online]. Available: http://www.juniper.net/techpubs/en_US/junos11.4/topics/topic-map/ospf-timers.html

[177] S. Yang and S. Park, "A dynamic service ranged-based multicast routing scheme using rsvp in mobile networks," in *INFOCOM 2001. 20th IEEE International Conference on Computer Communications. IEEE*, 2001.

[178] J. Zuniga, L. Contreras, C. Bernardos, S. Jeon, and Y. Kim, "Multicast mobility routing optimizations for proxy mobile ipv6," RFC 7028, Sep. 2013.

[179] D. Schlesinger and M. Girardot, "Smart and connected passenger vehicles: Pervasive connectivity will fundamentally change the automotive landscape," Cisco Internet Business Solutions Group (IBSG), 2010.

[180] A. Mai and D. Schlesinger, "Connected vehicles: From building cars to selling, personal travel time well-spent," Cisco Internet Business Solutions Group (IBSG), 2010.

[181] Wardsauto, "World vehicle population tops 1 billion units'." [Online]. Available: http://wardsauto.com/ar/world_vehicle_population_110815

[182] M. Kearney, "Ev charging infrastructure deployment: Policy analysis using a dynamic behavioral spatial model," Master Thesis, MIT, 2011.

[183] "Transport greenhouse gas emissions: Country data 2010," International Transport Forum, Tech. Rep., 2010.

[184] "Smart grids and electric vehicles: Made for each other?" International Transport Forum, Tech. Rep., Apr. 2012.

[185] S. Galli, A. Scaglione, and Z. Wang, "Power line communication and the smart grid," in *SmartGridComm*, 2010.

[186] F. Nouvel, P. Maziero, and J. Prevotet, "Wireless and power line communication in vehicle," in *Design, Automation & Test in Europe*, 2009.

[187] S. Barmada, M. Raugi, M. Tucci, and T. Zheng, "Plc in a full electric vehicle: Measurements, modelling and analysis," in *ISPLC*, 2010.

[188] L. M. et al, "Deliverable 4.1: Light ip mobility architecture for video services: initial architecture," Medieval project, Deliverable, Jun. 2011.

[189] T.-T. Nguyen, C. Bonnet, and J. Härri, "Proxy mobile ipv6 for electric vehicle charging service: Use case and analysis," EURECOM, Tech. Rep. RR-12-271, May 2013.

[190] T. Melia and S. Gundavelli. (2013, Oct.) Logical interface support for multi-mode ip hosts'. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-netext-logical-interface-support-08

[191] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, pp. 3604–3629, 2011.

[192] G. Giaratta, "Interactions between pmipv6 and mipv6: Scenarios and related issues," RFC 6612, May 2012.

[193] N. Neumann, J. Lei, X. Fu, and G. Zhang, "I-pmip: An inter-domain mobility extension for proxy-mobile ip," in *IWCMC*, June 2009.

[194] Z. Ma, K. Wang, and F. Zhang. (2012, Jan.) Network-based inter-domain handover support for pmipv6'. Internet draft. [Online]. Available: https://tools.ietf.org/html/draft-ma-netext-pmip-handover-02

[195] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik, and D. Famolari, "Ieee 802.21: Media independent handover: Features, applicability, and realization," *Communications Magazine, IEEE*, vol. 47, no. 1, pp. 112–120, January 2009.

[196] D. Forsberg, "Secure distributed aaa with domain and user reputation," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, June 2007.

[197] M. Crawford and B. Haberman, "Ipv6 node informatioin query," RFC 4620, Aug. 2006.

[198] Y. Fang, I. Chlamtac, and Y.-B. Lin, "Channel occupancy times and handoff rate for mobile computing and pcs networks," *Computers, IEEE Transactions on*, vol. 47, no. 6, pp. 679–692, Jun 1998.

[199] Y. Min-hua, Y. Lv-yun, L. Yu, and Z. Hui-min, "The implementation of multicast in mobile ip," in *Wireless Communications and Networking (WCNC)*, March 2003.

[200] H. Ali-Ahmad, D. Moses, H. Moustafa, P. Seite, and T. Condexia. (2013, Jul.) Mobility anchor selection in dmm: Use-case scenarios'. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-aliahmad-dmm-anchor-selection-01

[201] "3rd generation partnership project (3gpp); technical specification group services and system aspects; policy and charging control architecture (release 12)," TS, 3GPP TS 23.203, Sep. 2013.

[202] "Ibsg connected life market watch: Fixed location usage, consumers living connected lives," White Paper, Cisco Internet Business Solutions Group, Oct. 2012.

[203] D. Liu, J. Zuniga, P. Seite, H. Chan, and C. Bernardos. (2014, Feb.) Distributed mobility management: Current practices and gap analysis'. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-dmm-best-practices-gap-analysis-03

[204] "Itu-t recommendation g. 114: General characteristics of international telephone connections and international telephone circuits: One-way transmission time," ITU-T G.114, May 2003.

[205] V. Devarapalli, H. Lim, N. Kant, and S. Krishnan, "Heartbeat mechanism for proxy mobile ipv6," RFC 5847, Jun. 2010.

[206] N. A. et al., "Deliverable d6.4: Second periodic testing report," Medieval project, Deliverable, Jul. 2013.

[207] J. Asghar, I. Wijnands, S. Krishnaswamy, A. Karan, and V. Arya. (2013, Oct.) Explicit rpf vector'. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-pim-explicit-rpf-vector-03

[208] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - protocols and formats for cloud computing interoperability," in *International Conference on Internet and Web Applications and Services (ICIW)*, 2009.

[209] D. Liu, H. Chan, and H. Deng. (2014, Mar.) Cloud based mobile core network problem statement. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-liu-dmm-deployment-scenario-01