Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática,
2013

Jonathan Gabriel Oliveira Carvalho

Mobilidade Distribuída em Ambientes Dinâmicos

Universidade de Aveiro Departamento de
Electrónica, Telecomunicações e Informática,
2013

Jonathan Gabriel
Oliveira Carvalho

Distributed Mobility in Dynamic Environments

Universidade de Aveiro Departamento de
2013 Electrónica, Telecomunicações e Informática,

Jonathan Gabriel Oliveira Carvalho

Distributed Mobility in Dynamic Environments

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requesitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Professora Susana Sargento e Professor André Zúquete, Professores do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

o júri / the jury

presidente / president

Prof. Dr. Paulo Miguel Nepomuceno Pereira Monteiro
Professor Associado da Universidade de Aveiro (por delegação da Reitora da Universidade de Aveiro)

vogais / examiners committee

Prof. Dr. Teresa Maria Sá Ferreira Vazão Vasques
Professora Associada do Instituto Superior Técnico, Universidade Técnica de Lisboa

Prof. Dr. Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro (Orientator)

agradecimentos / acknowledgements

A dedicação, da mesma forma que o amor, exige uma certa dose de suave disciplina.

Grato pelo apoio incondicional daqueles que tornaram possível este trabalho.

Resumo

As redes de telecomunicações sem fios convencionais têm implementada uma estrutura hierárquica específica que em muitos casos lida com entidades centralizadas para garantirem continuidade de sessão e acessibilidade nas comunicações IP. Neste contexto, a gestão de mobilidade exige que haja uma âncora central e estática para permitir que os nós móveis se encontrem acessíveis quando conectados nas diferentes redes. Porém, este elemento central é suscetível a falhas introduzindo maiores atrasos, exigindo uma maior gestão da sinalização, sendo mais vulnerável a ataques o que pode causar problemas no sistema. Por estas razões, à medida que as redes móveis se tornam cada vez menos hierárquicas, a gestão da mobilidade baseada em modelos centralizados torna-se menos optimizada. Para melhorar a gestão de mobilidade tendo em consideração as exigências evolutivas da rede, têm vindo a ser propostas soluções para distribuir as âncoras, colocando-as mais perto do utilizador final com o objetivo de tornar a rede menos hierárquica, descentralizando o processo de gestão de mobilidade de uma forma dinâmica pelos nós da rede. Desta forma, a mobilidade distribuída em ambientes dinâmicos melhora a escalabilidade, acessibilidade e evita pontos centrais de falhas e engarrafamentos. Neste contexto, são idealizados e implementados três cenários de redes veiculares usando dois modelos de gestão de mobilidade, um centralizado e outro distribuído. Os resultados mostram que o protocolo de gestão de mobilidade distribuído apresenta melhores resultados em termos de perda de pacotes, atraso médio por pacote, custo de dados e custo de sinalização quando comparado com o protocolo de gestão de mobilidade centralizado.

O rápido crescimento de nós móveis tem levado ao aumento do consumo de tráfego de dados e, atualmente, estes estão equipados com múltiplas interfaces que, em muitos casos, utilizam diferentes tecnologias de acesso à rede. No entanto, a continuidade de sessão de um determinado serviço deve ser garantido, independentemente da tecnologia de acesso utilizada. Consequentemente, há uma preocupação em transformar a arquitetura da rede em modelos menos hierárquicos para lidar com o comportamento dos utilizadores e com a evolução do consumo de tráfego de dados móveis. Desta forma, é especificado um esquema de gestão de mobilidade distribuída com suporte a múltiplas interfaces para manter continuidade de sessões quando os nós móveis mudam de rede ou interface. Este mecanismo de mobilidade foi avaliado e testado num cenário real, demonstrando a capacidade de manter as sessões ativas em cenários com múltiplas interfaces melhorando a experiência do utilizador, dando como exemplo cenários de perda de ligação, ligação a outras redes e ligar/desligar uma interface.

Abstract

Conventional networks have implemented a specific hierarchical structure, which in many cases deals with centralized mobility anchoring models to ensure IP session continuity. In this context, mobility management demands the existence of a centralized and static anchor point to allow reachability to mobile nodes connected to distinct networks. However, such centralized element is a single point of failures, introducing longer delays and higher management signalling. It may be more vulnerable to attacks, causing problems in the system. For this reason, mobility management addressed to centralized models is a satisfactory and non-optimal solution when mobile networks become less hierarchical. In order to improve mobility management to meet the requirements in mobile network evolution, there have been proposed solutions to distribute the anchor points closer to the end-user. This way, distributed and dynamic mobility anchoring improves scalability and availability, avoiding single points of failure and bottlenecks, as well as enabling transparent mobility support. In this framework, it is idealized and implemented a set of Vehicular scenarios using two different types of mobility management models, one centralized and another distributed. The results shows that the distributed mobility management protocol provides better results in terms of data loss, average data delay, data cost and signalling cost, when compared with the centralized mobility management protocol.

The rapid growth of mobile nodes has lead to the increase of mobile data traffic consumption, and they are currently equipped with multiple network interfaces, which in many cases use different access technologies simultaneously. Therefore, session continuity of a certain user's services should be guaranteed independently of the access network technology. Consequently, there is a fundamental change in the network architectures, which is adopting flatten model to cope with users' behaviour and the evolution of the mobile data traffic consumption. Thus, it is specified a distributed mobility management scheme with multihoming support to provide continuity to active sessions when mobile nodes roam between networks/interfaces. This mobility mechanism is evaluated and tested in a real environment, demonstrating the capability to provide uninterrupted sessions for multihomed scenarios, such as the addition/removal of a link, likewise the capability to improve user experience.

Contents

Contents **i**

List of Figures **v**

List of Tables **ix**

Acronyms **x**

1 Introduction **1**

1.1 Motivation . . . 1

1.2 Objectives . . . 2

1.3 Organization . . . 3

1.4 Contributions . . . 4

2 State of the Art **5**

2.1 Introduction . . . 5

2.2 Problem Statement . . . 5

2.3 Requirements For Internet Mobility Support . . . 6

2.4 Mobility Management Overview . . . 7

2.4.1 Session Initiation Protocol (SIP) . . . 8

2.4.2 Mobile Stream Control Transmission Protocol (M-SCTP) . . . 9

2.4.3 Solutions based on Mobile Internet Protocol . . . 10

2.4.3.1 Mobile Internet Protocol (MIP) . . . 10

2.4.3.2 Fast Handover for Mobile IP (FMIP) . . . 12

2.4.3.3 Hierarchical Mobile IP (HMIP) . . . 13

2.4.3.4 Proxy Mobile Internet Protocol (PMIP) . . . 14

2.4.3.5 Distributed Mobility Management Approaches . . . 16

2.4.3.6 Distributed Mobility Anchoring (DMA) . . . 16

2.4.3.7 Dynamic Mobile IP Anchoring (DMIPA) . . . 18

2.4.3.8 Summary . . . 18

2.4.4 WiMAX Mobility Management . . . 20

2.4.5 Long Term Evolution Mobility Management . . . 21

2.4.6 Summary . . . 22

2.5 Multihoming . . . 23

2.6 Vehicular Ad-doc Networks (VANETs) . . . 25

2.6.1 Vehicular Network Architectures . . . 26

2.6.2 Characteristics of Vehicular Networks . . . 27

2.6.3 Business and Technical Problems 27
2.6.3.1 Routing and Dissemination 27
2.6.3.2 Security 28
2.6.3.3 Mobility Management and IP Configuration 28
2.6.3.4 Distribution of Applications 28
2.6.3.5 Business Models 29
2.7 Conclusion 29

3 Evaluation of MIPv6 and DMIPA performance in Vehicular scenarios 31
3.1 Introduction 31
3.2 MIPv6 and DMIPA 32
3.3 Available Network Simulators 35
3.4 Available Vehicular Mobility Simulators 37
3.5 Network Topology implemented in NS-3 38
3.6 SUMO 39
3.7 Network Topology and Deployed Scenarios 42
3.8 Evaluation, Results and Analysis 43
3.8.1 Evaluation of MIPv6 and DMIPA performance: Short Highway Scenario 45
3.8.2 Evaluation of the Data Packet Loss Cause 50
3.8.3 Evaluation of Long Highway Scenario 54
3.8.4 Evaluation of DMIPA performance: City Scenario 58
3.8.5 Evaluation of MIPv6 and DMIPA performance: City Scenario 61
3.9 Overall Discussion, Analysis and Conclusions 67

4 Proof of Concept in Distributed and Dynamic Mobility Management 69
4.1 Introduction 69
4.2 DMIPA Without Multihoming Support 69
4.2.1 Use-case Scenarios Description 69
4.3 DMIPA With Multihoming Support 72
4.3.1 Multihoming Overview and Specifications 72
4.3.2 Use-case Scenarios Description 75
4.4 Testbed Description 77
4.5 Implementation Description 79
4.6 Testbed Evaluation, Results and Analysis 79
4.6.1 Testing the Limitations of the Testbed: Part 1 79
4.6.2 Testing the Limitations of the Testbed: Part 2 81
4.6.2.1 Evaluating the UDP sessions in Test A and Test B 83
4.6.2.2 Evaluating the TCP sessions in Test A and Test B 84
4.6.3 Evaluating the performance of DMIPA with multihoming support in Scenario C 86
4.6.4 Evaluating the performance of DMIPA with multihoming support in Scenario D 88
4.6.5 Evaluating the performance of DMIPA with multihoming support in Scenario E 93
4.7 Challenges 94
4.8 Overall Discussion, Analysis and Conclusions 95

5 Conclusion and Future Work 97

5.1 Conclusions 97

5.2 Future Work 98

Bibliography 101

List of Figures

2.1 Mobility Management Approaches from the TCP/IP Stack point of view. . . 8
2.2 MIPv4 operational example without Route Optimization protocol. 11
2.3 MIPv6 operational example (with RO). 12
2.4 HMIPv6 operational example. 14
2.5 Architecture of PMIPv6. 15
2.6 Architecture of DMA. 17
2.7 DMA operational example. 17
2.8 a) DMIPA operational example. 19
2.9 b) DMIPA operational example. 19
2.10 WiMAX intra-ASN handover procedure. 20
2.11 LTE architecture. 22
2.12 Use-case scenario. 25
2.13 C2C-CC Reference Architecture [1]. 26

3.1 MIPv6 Architecture Overview. 32
3.2 MIPv6 Operational Mode and Exchanged Messages (without RO). 33
3.3 DMIPA Architecture Overview. 34
3.4 DMIPA Operational Mode and Exchanged Messages. 36
3.5 Short Highway. 39
3.6 Long Highway. 39
3.7 City. 40
3.8 Crossroads Example. 41
3.9 Bus Stop Example. 41
3.10 Example of the network deployed in NS-3. 42
3.11 Deployment scenario - Short Highway. 43
3.12 Deployment scenario - Long Highway. 43
3.13 Deployment scenario - City. 44
3.14 Signalling Cost in the Short Highway scenario. 46
3.15 MIPv6 Data Packets in the Short Highway scenario. 46
3.16 DMIPA (4 DMARs) Data Packets in the Short Highway scenario. 47
3.17 Data Cost in the Short Highway scenario. 47
3.18 Data Loss in the Short Highway scenario. 48
3.19 Average Data Delay in the Short Highway scenario. 48
3.20 Average Sessions per MN in the Short Highway scenario. 49
3.21 Average Number of IP per MN in the Short Highway scenario. 49
3.22 Binding Update Time in the Short Highway scenario. 50

3.23 Signalling Cost in the Short Highway scenario (Applications with lower Packet Rate). 51
3.24 MIPv6 Data Messages in the Short Highway scenario (Applications with lower Packet Rate). 51
3.25 DMIPA (4 DMARs) Data Messages in the Short Highway scenario (Applications with lower Packet Rate). 52
3.26 Data Cost in the Short Highway scenario (Applications with lower Packet Rate). 52
3.27 Data Loss in the Short Highway scenario (Applications with lower Packet Rate). 53
3.28 Data Delay in the Short Highway scenario (Applications with lower Packet Rate). 53
3.29 Average Sessions per MN in the Short Highway scenario (Applications with lower Packet Rate). 54
3.30 Average Number of IP per MN in the Short Highway scenario (Applications with lower Packet Rate). 54
3.31 Binding Update Time in the Short Highway scenario (Applications with lower Packet Rate). 55
3.32 Signalling Cost in the Long Highway scenario. 55
3.33 Data Cost in the Long Highway scenario. 56
3.34 Data Loss in the Long Highway scenario. 57
3.35 Average Data Delay in the Long Highway scenario. 57
3.36 Average Session per MN in the Long Highway scenario. 58
3.37 Average Number of IPs per MN in the Long Highway scenario. 58
3.38 Binding Update Time in the Long Highway scenario. 59
3.39 Signalling Cost in the City scenario. 59
3.40 Data Cost in the City scenario. 60
3.41 Data Loss in the City scenario. 60
3.42 Average Data Delay in the City scenario. 61
3.43 Average Session per MN in the City scenario. 61
3.44 Average Number of IPs per MN in the City scenario. 62
3.45 Binding Update Time in the City scenario. 62
3.46 Comparing Signalling Cost of MIPv4 and DMIPA (4 DMARs) in the City scenario. 63
3.47 Comparing Data Cost of MIPv6 and DMIPA (4 DMARs) in the City scenario. 63
3.48 Comparing Data Loss of MIPv6 and DMIPA (4 DMARs) in the City scenario. 64
3.49 Comparing the Average Data Delay of MIPv6 and DMIPA (4 DMARs) in theu City scenario. 64
3.50 Comparing the Average Session per MN of MIPv6 and DMIPA (4 DMARs) in the City scenario. 65
3.51 Comparing the Average Number of IPs per MN of MIPv6 and DMIPA (4 DMARs) in the City scenario. 65
3.52 Comparing the Binding Update Time of MIPv6 and DMIPA (4 DMARs) in the City scenario. 66

4.1 Common Scenario in DMIPA topology (without multihoming support). . . . 70
4.2 Scenario A. 71
4.3 Scenario B. 71
4.4 Example of handover between interfaces connected to the same DMAR. . . . 73
4.5 Example of handover between interfaces connected to different DMARs. . . . 74

4.6 Example of handover between interfaces connected to different ARs. 74
4.7 Scenario C. 75
4.8 Scenario D. 76
4.9 Scenario E. 76
4.10 Testbed. 77
4.11 Bitrate at 250 packets per second. 80
4.12 Bitrate at 1000 packets per second. 80
4.13 Delay at 250 packets per second. 81
4.14 Delay at 1000 packets per second. 81
4.15 Packet Loss at 250 packets per second. 82
4.16 Packet Loss at 1000 packets per second. 82
4.17 Bitrate for UDP sessions with a constant packet rate of 125 pps (Test A). . . 83
4.18 Bitrate for the UDP sessions with different packet rate (Test B). 83
4.19 End-to-End Packet Delay for UDP sessions with a constant packet rate of 125 pps (Test A). 84
4.20 End-to-End Packet Delay for the UDP sessions with different packet rate (Test B). 84
4.21 Packet Loss Results for UDP sessions with a constant packet rate of 125 pps (Test A). 85
4.22 Packet Loss Results for the UDP sessions with different packet rate (Test B). 85
4.23 Bitrate for TCP sessions with a constant packet rate (Test A). 85
4.24 Bitrate for the TCP sessions with different packet rate (Test B). 86
4.25 End-to-End Packet Delay for TCP sessions with a constant packet rate (Test A). 86
4.26 End-to-End Packet Delay for the TCP sessions with different packet rate (Test B). 87
4.27 Bitrate of UDP Sessions in Scenario C. 87
4.28 Delay of UDP Sessions in Scenario C. 88
4.29 Packet Loss of UDP Sessions in Scenario C. 88
4.30 Bitrate of TCP Sessions in Scenario C. 89
4.31 Delay of TCP Sessions in Scenario C. 89
4.32 Bitrate of UDP Sessions (Reference Model - Scenario A). 89
4.33 Bitrate of UDP Sessions (Matching Model - Scenario D). 90
4.34 Delay of UDP Sessions (Reference Model - Scenario A). 90
4.35 Delay of UDP Sessions (Matching Model - Scenario D). 90
4.36 Bitrate of TCP Sessions (Reference Model - Scenario A). 91
4.37 Bitrate of TCP Sessions (Matching Model - Scenario D). 91
4.38 Delay of TCP Sessions (Reference Model - Scenario A). 92
4.39 Delay of TCP Sessions (Matching Model - Scenario D). 92
4.40 Bitrate of TCP Sessions (Reference Model - Scenario B). 93
4.41 Bitrate of TCP Sessions (Matching Model - scenario E). 93
4.42 Delay of TCP Sessions (Reference Model - Scenario B). 94
4.43 Delay of TCP Sessions (Matching Model - Scenario E). 94

List of Tables

4.1 Matching between Use-case and Testbed scenarios. 78

Acronyms

1G First Generation of Mobile Telecommunications Technology

3G Third Generation of Mobile Telecommunications Technology

3GPP Third Generation Partnership Project

4G Fourth Generation of Mobile Telecommunications Technology

AODV Ad Hoc On Demand Distance Vector

AP Access Point

AR Access Router

ASA Anchor Set Acknowledgement

ASN Access Service Network

ASU Anchor Set Update

AU Application Unit

BA Binding Acknowledgement

BS Base Station

BU Binding Update

BWA Broadband Wireless Access

C2C Car-to-Car

C2C-CC Car-to-Car Communication Consortium

C2I Car-to-Infrastructure

CoA Core-of Address

CN Correspondent Node

DHCP Dynamic Host Configuration Protocol

DMA Distributed Mobility Anchoring

DMAR Data Mobility Access Router

DMIPA Dynamic Mobile IP Anchoring

DMM Distributed Mobility Managment

D-ITG Distributed Internet Traffic Generator

eNodeB evolved NodeB

FA Foreign Agent

FBSS Fast Base Station Switching

FMIPv6 Fast Handover for Mobile IP version 6

FN Foreign Network

GloMoSim Global Mobile Information System Simulator

GPRS General Packet Radio Service

GTP GPRS Tunneling Protocol

HoA Home Address

HA Home Agent

HHO Hard Handover

HMIP Hierarchical Mobile Internet Protocol

HMIPv6 Hierarchical Mobile Internet Protocol version 6

HN Home Network

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IT Institute of Telecommunications

ITS Intelligent Transportation System

LCoA Local Care-of Address

LMA Local Mobility Anchor

LTE Long-Term Evolution

MAC Media Access Control

MAG Mobile Access Gateway

MAP Mobility Anchor Point

MAR Mobility capable Access Router

MDHO Macro Diversity Handover

MIP Mobile Internet Protocol

MIPv6 Mobile Internet Protocol version 6

MIPv4 Mobile Internet Protocol version 4

MME Mobility Management Entity

M2M Machine-to-Machine

MN Mobile Node

MS Mobile Station

MSF Mobility Support Flag

M-SCTP Mobile Stream Control Transmission Protocol

NAR New Access Router

NGN Next Generation Networks

NS-2 Network Simulator 2

NS-3 Network Simulator 3

OBU On-Board Unit

OLSR Optimized Link State Routing

OPNET OPNET Modeler Suite Network Simulator

OSI Open Systems Interconnection

PAR Previous Access Router

PBA Proxy Binding Acknowledgement

PBU Proxy Binding Update

PDA Personal Digital Assistant

PDCP Packet Data Convergence Protocol

PMIPv6 Proxy Mobile IPv6

PTPd Precision Time Protocol daemon

QoE Quality of Experience

QuelNet QualNet Communications Simulation Platform

QoS Quality of Service

RA Router Advertisements

radvd Router Advertisement Daemon

RAN (Radio Access Network

RCoA Regional Care-of Address

RS Router Solicitation

RSU Road Side Unit

SBC Single Board Computer

SCTP Stream Control Transmission Protocol

SHO Soft Handover

SIP Session Initiation Protocol

SUMO Simulation of Urban MObility

TCP Transmission Control Protocol

UDP User Datagram Protocol

UE User Equipment

UMTS Universal Mobile Telecommunications System

USB Universal Serial Bus

VANET Vehicular Ad Hoc Network

VoIP Voice over Internet Protocol

WiMAX Worldwide Interoperability for Microwave Access

Chapter 1

Introduction

1.1 Motivation

Global mobile data traffic grew more than fifty percent in 2012 and will increase at a considerable annual growth rate of sixty six percent from 2012 to 2017 [2]. Moreover, it is expected that the increasing usage of smartphones will cause the continuous increase of mobile data traffic in 2013. Therefore, the proliferation of high-end handsets, tablets and laptops on mobile networks is a major generator of traffic, but smartphones and other device categories such as Machine-to-Machine (M2M) nodes will account for a significant part of the traffic in the next few years.

Diversification of mobile devices has experienced an exponential growth, and according to Cisco [2], they are the main contributors to increase the traffic in mobile networks worldwide. Those mobile devices are constantly increasing in sophistication, becoming more powerful in terms of access technologies, supporting any services at any interface, enabling end-users to have a wide mobility. With the world evolving towards more subscriber-centric and user-centric Future Internet architecture models, mobility is an important key feature which relies on end-user movement patterns. However, mobility is no longer limited to the idea of a device moving among networks, changing its point-of-attachment, but it will extend from terminals to subscribers, content and applications, affected by a large range of factors, such as subscriber experience and resource efficiency.

Focussing on user-centric models, mobility management must have intrinsic the concept of session continuity. From this point of view, session continuity is an essential requirement, which provides transparent and seamless ongoing sessions between access locations and access technologies. This means that any end-user moving through the network, changing the access point (and perhaps changing access technology - interface), shall be able to maintain session continuity without significant degrading of Quality of Experience (QoE). Such demands have to be supported by today's world heterogeneous networks that use different access technologies to meet large dynamic environments with non-deterministic mobility patterns. Nowadays, mobility management is an indispensable mechanism of mobile networks. However, traditional mobility management approaches for all-IP networks have in common a strong centralized model. They are based on a static Mobility Anchor Point (MAP). MAP is the element responsible to guarantee the mobility management process of a Mobile Node (MN), namely location and handover management from both data and control planes. Despite being an important element in the mobility architectures, the centralized entity may not be suitable for large flatten networks, being a single point of failure, congestion and bottlenecks.

Schemes based on centralized architectures cause scalability, robustness and availability issues. Moreover, those issues cause performance limitations in dynamic environments with a large set of mobile devices with different wireless technologies. There have been proposed solutions to solve the majority of the problems about using centralized architectures, which rely on distributing anchor points in network nodes, closer to the end-user, providing enhancements to the mobility management. Hence, there is a trend to flattening the network by allowing a dynamic distribution of mobility management functionalities across the access nodes.

The Distributed Mobility Managment (DMM) working group in IETF [3] does not specify any mobility management scheme with multihoming support, nor any specifications on how this should properly work in real situations. However, the literature already contains several proposals for distributing mobility, including the one of our research group [4].

Nevertheless, mobility management remains an area of study that needs an intensive contribution of the scientific community which already understood the impact of users' mobility, where the desire to maintain high quality of communication and active mobile multimedia services across the network depends on both human mobility behaviour and network solutions deployed.

1.2 Objectives

The work to be developed under this Master Dissertation is related to both distributed mobility management and dynamic multihoming support schemes in wireless environments. These schemes improve the mobility management mechanism and therefore it is essential to evaluate each parameter concerning the architectures and scenarios under study.

Furthermore, it is described a distributed mobility management scheme based on mechanisms that manage Internet Protocol (IP) addresses, mobility anchors, IP tunnels and routing rules, in order to provide session continuity in multihomed scenarios without compromising effectiveness and performance.

The objectives of this work are the following described:

- Evaluation of the distributed mobility management protocol defined by our research group in vehicular networks;
- Implementation and evaluation of a distributed mobility management protocol defined by our group in real scenarios;
- Proof of concept of a distributed mobility management concept with multihoming support in real scenarios.

The first objective in evaluation of the distributed mobility management protocol is to study the performance of Dynamic Mobile IP Anchoring (DMIPA) protocol in vehicular environments, and the second is to compare it with Mobile Internet Protocol version 6 (MIPv6), a centralized mobility management protocol which is deployed in today's networks. For this purpose, it is used a network simulator and a traffic mobility generator.

Then, it is performed an evaluation of DMIPA in a real network, using a real testbed, where a mobile node changes its point-of-attachment and communicates with the correspondent node using only one interface.

In order to prove the capability of DMIPA to provide multihoming support in real scenarios, it is used the same testbed where the mobile node uses multiple interfaces.

To achieve the main objectives of this work, it was necessary to perform the following tasks:

- Study the existent mobility management protocols, the multihoming concept and the most recent developments of vehicular networks;
- Development of a network topology using the network simulator NS-3;
- Design different vehicular scenarios taking into account the advantages of the tools available in Simulation of Urban MObility (SUMO);
- Development of a real testbed to perform the evaluation of distributed mobility management and multihoming;
- Design use-case scenarios which address the distributed mobility management with multihoming support;
- Perform the required simulations and tests; evaluate, analyse and compare the results, concluding about the performance of the distributed mobility management protocol developed by our research group in vehicular networks as well as in real environments.

1.3 Organization

The present document is organized as follow:

Chapter 2 introduces an overview of the problem statement and the evolution of mobility management in today's technologies. It studies the current architectures and protocols that deal with IP mobility management, i.e., hierarchical and centralized architectures. Solutions founded on decentralized models and the capability of providing multihoming mechanisms will also be the focus our study. Furthermore, this chapter explains the current state of Vehicular Ad Hoc Networks (VANETs) and the key concepts and topologies of such networks. Besides, it mentions existent mobility protocols and its importance for Vehicular scenarios, highlighting the main challenges and problems to be solved.

Chapter 3 describes the IP mobility management protocol that will be the subject of our study. It will be given a brief introduction of the implementation platform simulation Network Simulator 3 (NS-3). Then, it provides a detailed description of the vehicular scenarios implemented and the modifications performed in order to achieve the requirements of the evaluation of distributed mobility in vehicular networks. Finally, it is analysed and compared the results regarding the following parameters: signalling cost, data cost, data loss, average data delay, average number of sessions per MN, average number of IPs per MN and mobility handover time.

Chapter 4 presents the work done on the testbed of distributed mobility and multihoming, detailing the activities addressed to test the theoretical assumptions about distributed and dynamic mobility management with and without multihoming support. Moreover, are described the technical considerations and challenges faced throughout the deployment of use-case scenarios. Then, it shows the results regarding bitrate, end-to-end packet delay and packet loss.

Chapter 5 concludes all the work done so far and reviews the results concerning assumptions and requirements. This chapter presents future work and possible improvements to be considered.

1.4 Contributions

As a major contribution to the research on vehicular networks, the work developed under this Master Dissertation results into two scientific papers.

The first one, entitled “Distributed Mobility Management in Dynamic Environments: V2I Networks” [5], refers to the study of MIPv6 and DMIPA in vehicular environments. In this work, it is idealized and implemented a set of vehicular scenarios, where the performance of both mobility management protocols is evaluated.

The second scientific paper, entitled “Dynamic Offload Anchoring with IP Mobility” [4], evolves a distributed mobility management scheme, called DMIPA, to provide session continuity in multihoming scenarios. Therefore, the scheme under study is evaluated in a real scenario and it is demonstrated the ability to move sessions between networks and interfaces through the adequate mobility processes.

In order to report the new results and disseminate the information to the large community of scientists, these two papers are under development and will be submitted in November, the first one in an international conference, IEEE ICC 2014, and the second one in an international journal, the Mobile Networks and Applications (MONET) by Springer.

Chapter 2

State of the Art

2.1 Introduction

This chapter is focussed on studying and analysing the mobility management based solutions for Internet Networks available today, while it is explained the multihoming concept and how much it is important to combine both mechanisms to achieve a total mobility management experience. An explanation of the current state of art in VANETs is also given.

First of all, it is defined the problem statement and associated requirements for Internet mobility and management. Then, the reader is submitted to a general review of the existent solutions adopted from a different TCP/IP stack perspective. It describes with detail the characteristics of mobility management according to network structures and today's technologies. Moreover, it will investigate the advantages and disadvantages of the various concepts for mobility management according to the different layers of the TCP/IP protocol stack.

Multihoming is a mechanism to increase network reliability. Thus, it is directly involved with the mobility management concept which aims to maintain the ongoing sessions. This chapter also studies the multihoming goals and the present solutions.

Finally, the demand for highly dynamic mobility in vehicular networks introduces significant challenges which require novel mobility management approaches. Therefore, these types of networks and the mobility management solutions require a new area of study. This chapter analyses the concepts of vehicular networks and the related mobility management approaches.

2.2 Problem Statement

Over the recent decades, the number of wireless access technologies and the number of mobile computing devices has experienced an exponential growth. Hence, there is a paradigm shift to move towards a new mobile world in which users communicate with each other using powerful mobile devices. These mobile devices are equipped with a wide range of radio access technologies with continuously expanding capabilities, and they are becoming available for everyone, calling for high interoperability between systems and services [6]. Moreover, the continued growth of Internet triggered the need for network access using TCP/IP anywhere and anytime. Then, the Internet becomes one of the premier technological success, changing the paradigm of publication, advertising and personal communication.

Unfortunately, the base protocols upon which the Internet has been developed and its current architecture are not suitable to support the emerging demand on dynamic mobility. The IP protocol combines routing information with host identification in a globally unique IP address. Hence, if a host moves to a new network, it would require to configure a new IP address in order to indicate the proper new point-of-attachment to the Internet routers.

However, some transport protocols, such as Transmission Control Protocol (TCP), use the IP address internally to manage connection state for sessions, being operated on the mobile device. Consequently, if a host roams to another network, and therefore, it changes its IP address, the TCP will not be able to keep the connection status for the active sessions. The lack of mobility management protocols are unable to handle the mobile devices to maintain the current active sessions when moving to other networks.

Therefore, if connections are to be maintained as the nodes move from one network to another, protocol modifications and new proposals are required.

2.3 Requirements For Internet Mobility Support

In order to provide Internet mobility management support and management, which refers to guaranteeing session continuity, when an IP-based device changes its topological point-of-attachment, it is required to fulfil the following requirements [7]:

- Handover Management: In order to provide seamless communication and session continuity when the mobile devices move to a different network, a fundamental mechanism, called handover management is required. The main goal is to minimize service disruption during handover procedure.

- Location Management: Managing location information of mobile nodes is an important issue and involves: identification of the mobile node current location and maintenance of the tracking of location changes.

- Multihoming: With a wide diversity of wireless access technologies being deployed to provide access to the Internet, the future mobile environment will be purely heterogeneous, where mobile devices will have multiple interfaces with different wireless access technologies. So, there is a need to provide multihoming support to the mobile nodes by allowing them to access the Internet through multiple interfaces simultaneously, selecting and switching links dynamically.

- Applications: The mobility management should be transparent without requiring modifications to services and applications. Then, the network needs to be able to support the current services and applications.

- Security: When providing Internet mobility support, security is an important aspect to be considered. Therefore, the mobility solutions must provide a total protection to avoid, as example, stealing of legitimate addresses, lost of privacy, identity spoofing and others.

It is also listed some of the performance requirements that are most relevant for Internet mobility: handover latency, packet loss, signalling overhead and throughput.

Concluding, to deploy a complete and useful Internet mobility, such requirement should be addressed as much as possible. The following section presents existent solutions adopted from a different TCP/IP stack perspective.

2.4 Mobility Management Overview

The latest evolution and successful deployment of several wireless network technologies pose a strong demand to develop a framework for co-existence of heterogeneous wireless networks within IEEE 802.11 g/n/p, Worldwide Interoperability for Microwave Access (WiMAX), Third Generation of Mobile Telecommunications Technology (3G) and Long-Term Evolution (LTE) (so-called Fourth Generation of Mobile Telecommunications Technology (4G)) and others. One of the most important technical/design challenges of today's networks is to provide seamless mobility that can guarantee transparency in service continuity for multi-mode mobile devices, such as wireless laptops, cellular phones and Personal Digital Assistants (PDAs) . Mobility can be classified into five types: **terminal mobility**, which is the ability of a mobile host to move through IP subnets, while still accessible for incoming requests and keeping sessions across subnet changes; **personal mobility** refers to the ability of addressing an user that can be located at different terminals, accessing services from anywhere (e.g. instant messaging); **session mobility** that aims to maintain actual sessions when the mobile device changes its point-of-attachment (e.g. real-time call redirect); **service mobility** specifies the capability of accessing retrieval services even when moving and changing terminals or services providers (e.g. web); and **roaming** sustains relocation across large areas, covering multiple administrative domains [8].

Nevertheless, all these types of mobility have to be managed through specific mechanisms to provide the desired mobility and guarantee the necessary Quality of Service (QoS) and QoE.

Mobility management can be analysed from different perspectives according to TCP/IP protocol stack. Mobility affects the TCP/IP protocol stack in such a way that it can be decoupled in the different stack layers:

- Application Layer: New applications and adaptations
- Transport Layer: Traffic congestion and flow control
- Network Layer: Addressing and routing issues
- Link Layer: Media access and handoff problems
- Physical Layer: Transmission errors and interference

The traditional TCP/IP stack was designed for fixed computer networks and, for that reason, this architecture has some limitations for Internet mobility support. These limitations are described in [7], covering the limitations of Link layer, IP address, lack of Cross-Layer Awareness and Corporation and Limitation of Applications.

Over the past few years, it has been proposed several solutions attempting to provide novel mobility management. Such solutions tend to reference one of the protocol stack layers to improve mobility management, as illustrated in Figure 2.1.

In this section it will be describe the most important proposals. It starts with a brief explanation about Session Initiation Protocol (SIP) which is an application-layer control protocol for initiating interactive communication sessions between users, and ends with mobility managements approaches at Layer 2 of the TCP/IP protocol stack, like WiMAX and LTE. It is highlighted the fact that proposals at Layer 3 (TCP/IP Network Layer) are the most relevant for this work, therefore sub-chapter 2.4.3 delivers an in-depth analysis of the mobility management issue in IP-based mobile communication networks.

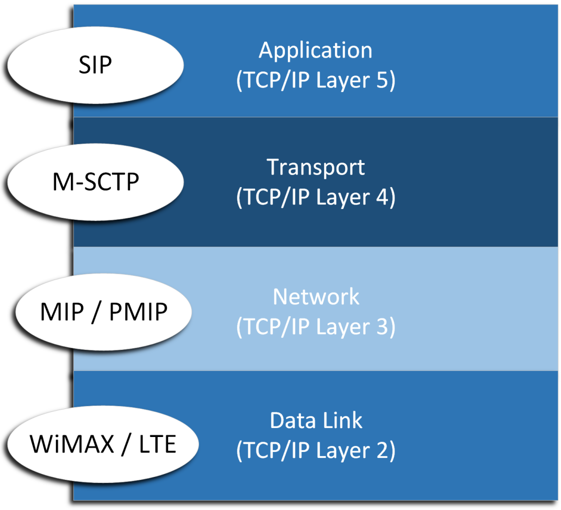

Figure 2.1: Mobility Management Approaches from the TCP/IP Stack point of view.

2.4.1 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) [9] is a control protocol deployed at the application layer, where sessions can be created, modified and terminated according to users' requirements. Such sessions can include Internet telephone calls (e.g. voice), multimedia conferences (e.g. video) and multimedia distribution (e.g. chat, interactive games, and virtual reality). This protocol does not depend on the transport-protocols' fundamental bases, so it is capable of running on TCP, User Datagram Protocol (UDP), as well as on Stream Control Transmission Protocol (SCTP) [10]; it works without any influence of the session type that is being established.

SIP coexists with many Internet applications that require the establishment and management of a session, where association participants exchange data between them. As a clear trend, participants move across the networks, change their endpoints and communicate in several different media, which in most of the cases emerge concerns about mobility support and session continuity. To avoid the described issues, SIP and other protocols work together by enabling Internet endpoints to discover each other by making agreements on a characterization of a shared session. It enables creation of an infrastructure of network host, named proxy server to which Internet endpoints can send requests: registrations, invitations to sessions and others.

The SIP protocol has mechanisms to handle the three types of mobility: terminal mobility, session mobility and personal mobility. The first one refers to support for an user equipment to move between different IP subnets while still being reachable for incoming requests, and while keeping sessions continuity. It uses dissimilar mechanisms in order to provide session continuity at the three stages: before a call, during a call and to recover from network partitions. Session mobility can be supported by SIP using the following three methods:

- Method number one assumes that server provides and manages IP addresses and ports to the involved entities. The server has the responsibility to report information about IPs and ports to each party by means of “Invite” requests.
- Third-party call control is the second method where the mapping between session re-

quests and destination is controlled by a third element placed between the participants. Although it provides good session isolation, this method has the drawback of keeping a third element involved in the session, as it manages the request to change and terminate the session from participants.

- "Refer" method is the last one. The third-party is only useful when negotiation by regular "Invite" exchange is needed. Thus, when a participant wants to transfer the session to a new destination, the third-party controls the mobility by receiving a "Refer" message and sending an "Invite" message to the new destination.

SIP protocol [9] [11] has the capability to support personal mobility, which means, this mechanism is based on the use of an unique personal identify which enables the end-user to access subscribed services in any terminal and in any location. As such, the end-user can be found independent of location and network device.

Concluding, the use of application-layer signalling protocol, SIP, to maintain active sessions removes the requirement of tunnelling at the network layer to handle mobility. However, it is possible to support mobile IP, such as MIPv6, and SIP simultaneously, using policy tables. Without them, the use of two different addresses (Home Address (HoA) and Core-of Address (CoA)), may be a problem due to the combination of these two protocols. SIP can be installed easily and is often chosen by mobile applications to get mobility before it reaches the network layer, where mobile IP is generally deployed.

2.4.2 Mobile Stream Control Transmission Protocol (M-SCTP)

Stream Control Transmission Protocol SCTP [12] has been proposed as a trustable transport protocol running on top of IP. Among other services, it offers basic support for reliable transfer of user messages when two SCTP endpoints are associated. The main feature of this protocol is multihoming, which enables a single SCTP endpoint to handle multiple IP addresses within a single association. Obviously, multihoming is a key feature for IP mobility support at the transport layer, because it separates the identity of an end system from the current address to which packets are sent.

On the other hand, multihoming aims to increase association reliability in wired networks, which implies that IP addresses of all involved end systems are fixed and known in advance. In mobile environments, traditional SCTP will face serious drawbacks due to the fact that mobile host does not have a fixed and well-known IP address. As the mobile node moves across the network, its local address frequently changes, consequently the set of IP addresses must be made dynamic.

Wei Xing, Holger Karl and Adam Wolisz [13] propose an approach in which the main idea is to have at least two IP addresses per mobile host in SCTP association when two access points are available at the same time. This approach is called Mobile Stream Control Transmission Protocol (M-SCTP) [13] and it emerges as an alternative solution to IP mobility at the network layer. M-SCTP operates primarily in the case that the coverage area of an old access point is overlapping with the coverage area of the new one, to which the mobile node will perform a handoff. So, the mobile node can obtain the IP address from the new access point and use it to anticipate the handoff process, modifying the set of IP addresses that represent a connection between him and the correspondent SCTP endpoint (SCTP association). Since the main purpose is to support active sessions through subnets, M-SCTP allows the handover processes to be solved using multihoming mechanisms. However, it does not keep reachability of mobile nodes for incoming requests.

2.4.3 Solutions based on Mobile Internet Protocol

Mobility management functionalities can be implemented at different layers of the TCP/IP protocol stack. In this section, such functionalities reside in the IP network layer and in some cases, on the mobile node.

Assuming the network-based solution approach, the mobility management function resides purely in the network, thereby the IP host does not need to send IP mobility management signalling messages to the home agent. By the other hand, a solution based on host requires mobility management functions in the IP stack of the mobile node.

Following, it is described the most notable solutions to the mobility issues on the Internet Network.

2.4.3.1 Mobile Internet Protocol (MIP)

Mobile Internet Protocol (MIP) [6] is a host based standard communication protocol proposed by Internet Engineering Task Force (IETF) to solve global mobility management.

It was presented as the first solution for mobility issues in the context of Internet Protocol version 4 (IPv4) [14], defining a mechanism which enables nodes to change their point-of-attachment to the Internet, while maintaining its IP address and transport layer connections. Mobile IP introduces a new architecture and define three new functional entities: Mobile Node (MN), Home Agent (HA) and Foreign Agent (FA). The MN is a host or router that moves from an attached network to another. It maintains the IP address while change its location and continue to communicate with other Internet nodes. HA is a router on the Home Network (HN) of a MN who is in charge of tunnelling datagrams for delivery to the MN when it is in the Foreign Network (FN), and for maintaining the mobile node's current location information. As a router, the FA provides routing services to the mobile node when it registers in a visited network. Moreover, it detunnels and delivers the datagrams to the MN, coming from the MN's Home Agent. If the datagrams are sent by the MN, the FA serves as a default router for registered MNs.

Apart from these new functional elements, it is given a long-term IP address to the MN on a HN, called Home Address (HoA), which is used in many cases as a source of the sent datagrams. When the MN is visiting a FN, a topologically correct IP address is needed to communicate and indicates the MN's current location. This address is called Care-of Address (CoA) and therefore, datagrams delivered to this address can be delivered to the MN.

For establishing connections with other internet hosts, called Correspondent Nodes (CNs), the MN uses its HA, which should remain the same during the connection's lifetime. For establishing reachability for the current access point-of-attachment, the MN uses the CoA. So, the MN has to use two different IP addresses in order to enable seamless connectivity, but the coordination of these addresses has to be managed by the Mobile IP protocol, which may result in the tunnelling of received datagrams in the MN's home agent to roaming MN. The tunnelling mechanism is done by encapsulation with the purpose of making the MN accessible from its HA. Thus, the traditional IP applications can work in a dynamic and mobile environment due to the introduction of tunnelling, allowing the application continuity between hosts, while the MN roams over the network. The basic operation of Mobile Internet Protocol version 4 (MIPv4) is illustrated in Figure 2.2.

In this version of Mobile IP protocol, the mobile nodes receives Agent Advertisements messages and determines that it is on its HN or a FN. If the mobile node is attached to its HA, it operates without mobility services, exchanging datagrams with the CN. When the MN roams to a FN, it obtains a CoA determined by the FA's advertisements. At this point, the datagrams have to continue to be delivered to MN's HA, so the HA has to intercept and send them through an IP tunnel to the MN's CoA, being received at the tunnel endpoint that could be the FA or the MN itself. The datagrams sent by the MN are directly delivered to the CN using standard IP routing processes, without traversing the HA. Consequently, the communication between MN, CN and HA create a triangle routing decreasing the performance of this protocol. This situation, in which the CN's datagrams to a MN follow a path which is longer than the optimal path, because the datagrams have be forwarded to the MN via HA, can be solved by the Route Optimization protocol described at [15]. The Route Optimization provides the updating of the CN's binding cache through binding update messages which contain the CoA of the mobile node. Then, CN may tunnel the datagrams directly to the CoA, indicated in the cached mobility binding. As a result, the introduction of this feature in the MIPv4 increases the efficiency and reduces the delays and resources allocation.

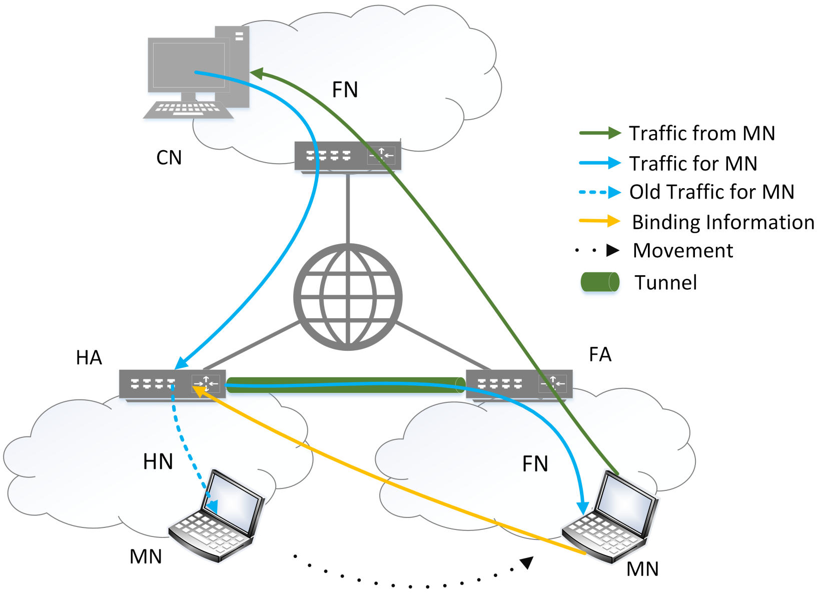

Figure 2.2: MIPv4 operational example without Route Optimization protocol.

The mobility management in the context of Internet Protocol version 6 (IPv6) [16] provides a set of features, such as extensions headers, auto-configuration services, flow-label, authentication, privacy capabilities, and others [17].

Moreover, IPv6 Neighbor Discovery [18] and Address Auto-configuration [19] allow hosts to operate in any location without any special support. It has the advantage of enabling every node with mobile capabilities, and there is no FA required, because it is designed for support mobility in its base protocol. The MIPv6's operational mode is similar to the MIPv4; however, MIPv6 avoids triangular routing allowing optimal routing. The way the packets are delivered does not need to go through the HA, and usually it will enable faster and more reliable transmission.

When the MN attaches to a new FN, it gets a CoA, and sends a Binding Update (BU) message to HA and CN. After the MN receives the Binding Acknowledgement (BA) message from CN, the communication will be made directly between them. The MN sends traffic to CN with CoA as source address in the datagram packets, meanwhile CN sends traffic to MN with CoA as destination address and with HoA as second hop in the special Routing Header field. The operational procedure of MIPv6 is illustrated on Figure 2.3.

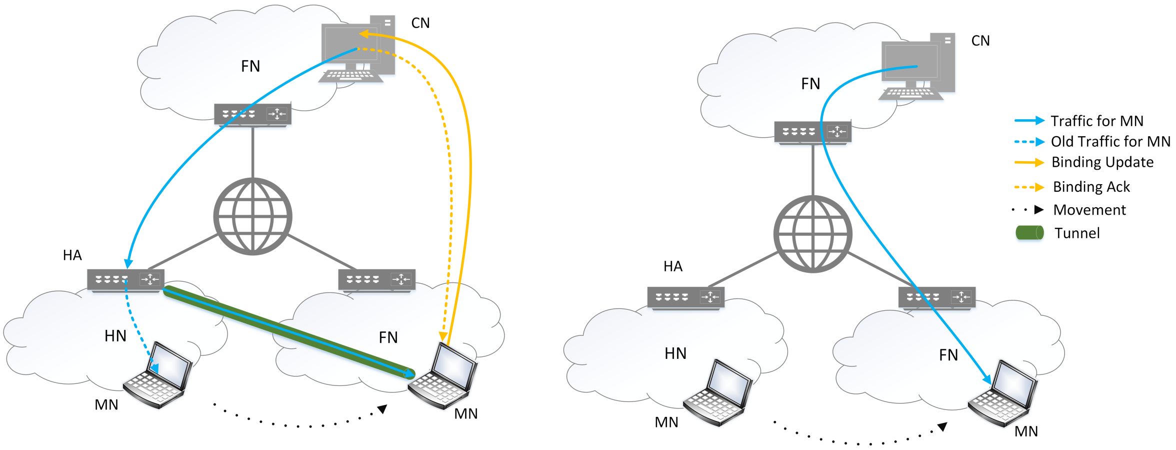

Figure 2.3: MIPv6 operational example (with RO).

Although Mobile IPv6 is a more suitable standard for IPv6 mobility, solving the major problems of MIPv4, there are still be unsolved some problems like signalling overhead, packet loss and handover latency. While the MN is registering to a subnet, it can no longer communicate through its previous subnet. Since the time to register (delay) is longer, a significant number of packets will be lost, which may result in an unacceptable quality of service for the user.

2.4.3.2 Fast Handover for Mobile IP (FMIP)

The Mobile IPv6 allows MNs to stay connected to the Internet even when moving from one Access Router (AR) to another. One of the major problems with the Mobile IP is the high handover latency. In fact, the Mobile IP handovers are slow due to the fact that the MN's IP stack has to detect the movement by listening to Router Advertisements (RA) messages, configure the new IP address through Dynamic Host Configuration Protocol (DHCP) or IPv6 address Auto-configurations mechanism, in case of IPv6. Finally, it has to send BU to HA. This procedure results in considerable delays between the moment the MN gets link layer (L2) connectivity and the moment when it can transfer data. For real-time applications, e.g. Voice over Internet Protocol (VoIP) or TCP sessions, a slow handover may indicate too many packet loss.

The Fast Handover for Mobile IP version 6 (FMIPv6)) [20] introduces IP messages necessary for its operational mode regardless of link technology to improve the handover management mechanism. The basic idea is to anticipate movements with the help of link layer and predict a possible change of subnet to prepare the network and host in advance. It means that, the MN searches for available ARs and subnets prefix information at any time, even when it is connected to the current AR using particular link layer mechanisms.

FMIPv6 works in the “predictive” operation mode: before a mobile node performs a handover, it sends a “Router Solicitation for Proxy Advertisement” message to the Previous Access Router (PAR). The PAR answers with a “Proxy Router Advertisement” message, which contains information about the new point-of-attachment. If the the New Access Router (NAR) is known by the PAR, the message specifies the new network prefix and the new access router ID. Therefore, the mobile node may form the new CoA using stateless address autoconfiguration and sends “Fast Binding Update” to PAR. Then, PAR and NAR exchange “Handover Initiate” and “Handover Acknowledge” messages to inform about QoS, access control and hearder compression, and so a “Fast Binding Acknowledgement” (FBack) will be sent by the PAR either to NAR and to the MN to ensure a successful binding. When the mobile node is connected to NAR, it sends a “Fast Neighbor Advertisement” (FNA) to initiate the packets forwarding.

FMIPv6 reduces handover latency specially when it uses the predictive mode. Moreover, it reduces the “Binding Update” latency by specifying a tunnel between the Previous CoA and the New CoA. In order to establish this tunnel, the mobile node sends a “Fast Binding Update” message to its PAR.

2.4.3.3 Hierarchical Mobile IP (HMIP)

The Hierarchical Mobile Internet Protocol (HMIP) [21] is a mobility management proposal based on Mobile Internet Protocol (MIP), and it was designed to improve service delay and reduce the amount of signalling introduced by communication between MN, its CN and its HA.

In MIPv6 [22] the frequent change of network requires new IP address configuration to route packets from one host to another, which is performed by sending “Binding Update” messages to update the binding caches every time a mobile node change its CoA. The registration requires a large number of location updates and the excessive exchange of signalling messages. To significantly improve the performance of MIPv6 minimizing signalling overhead and eliminating round trip delay from the time-critical handover period, it was proposed a solution based on a hierarchical concept, which introduces a new Mobile IPv6 node, named Mobility Anchor Point (MAP). This new entity introduces a hierarchical level which separates the local mobility from the global mobility. Thereby, MAP aims to minimize signalling load outside of the local domain, reducing handoff latency by employing a hierarchical network structure. It is essentially a local HA and can be located at any level of the hierarchical architecture, inclusive the AR level, and does not need to be placed on each subnet.

Hierarchical Mobile Internet Protocol version 6 (HMIPv6) [23] aims to improve local mobility. For that propose, it introduces two CoA for a mobile node. A Regional Care-of Address (RCoA) is obtained by the MN when it receives the MAP options, and is related to the prefix of the MAP’s subnet. On the other hand, Local Care-of Address (LCoA) is the on-link CoA configured on a MN’s interface based on the prefix advertised by its default access router. When the MN moves to another subnet inside the same MAP domain, it sends BU message to the local MAP contrary to MIPv6, in which the MN has to send the BUs either to HA and CNs. In this context, it only needs to register the new LCoA with the MAP. Then, the MAP will send back a “Binding Acknowledgement” message to the MN informing of the successful registration. It will receive all packets on behalf of the MN it is serving and will encapsulate and forward them right to the MN’s actual address. This process is illustrated at Figure 2.4.

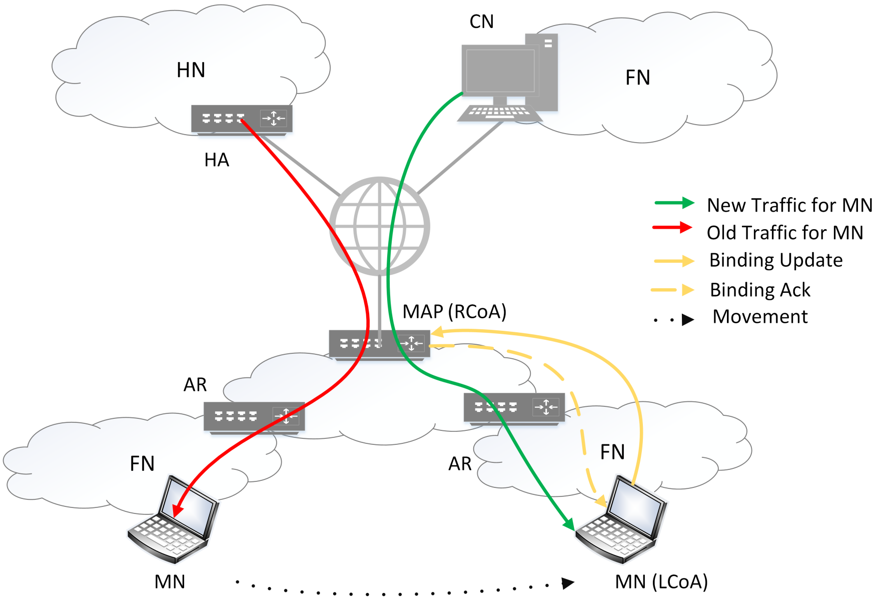

Figure 2.4: HMIPv6 operational example.

When the MN moves to a new MAP domain, both RCoA and LCoA need to be registered. This means that, RCoA does not change as long as the MN moves within a MAP domain. In consequence, the MN's mobility is transparent to the CNs communication. According to [22], which performed an intensive test of the MIPv6 and HMIPv6, considering a general case with random movements and more realistic traffic sources, i.e., VoIP, video, and TCP, they concluded that HMIPv6 reduces handoff latency, packet loss, and signalling load, having a better overall performance compared to MIPv6. Nevertheless, MAP still introduces a centralized model rising scalability and performance issues, e.g., network bottlenecks, single point of failures, attacks and non-optimal routing. Due the fast increase of mobile nodes and mobile data traffic, where users desire to keep QoE and active sessions while moving across the heterogeneous networks, the network has been designed to solve these requirements benefiting from the development of mobile architectures with fewer levels of routing hierarchy. This trend towards "Flat Networks" deals directly with communications among peers in the same geographical area, and the distributed mobility management in a truly flat mobile architecture will anchor traffic closer to the point-of-attachment of the user. Therefore, a centralized architecture is not able to address the mobile user's demands.

2.4.3.4 Proxy Mobile Internet Protocol (PMIP)

The protocols mentioned earlier, FMIPv6 and HMIPv6, are host-based solutions that require the action by the host at the IP layer (L3) similar to MIPv6 for global mobility management. These protocols allow the MN to maintain reachability when its IP address changes by updating the address mapping between the HoA and the CoA at the global MAP, or directly with the correspondent node, depending on the case. However, to update such information, the global mobility management may require a high amount of time causing packet loss because packets continue to be routed to the old local address; the increase of all signalling messages required when the mobile node moves from one AR to another reveals a disadvantage as well as location privacy. These problems and the recent developments in the network architectures and Wireless LAN infrastructures suggest to improve localized mobility management [24].

Proxy Mobile IPv6 (PMIPv6) [25] is a protocol solution that addresses the issues and requirements documented before. As a network-based mobility management protocol, it enables IP mobility for a host without requiring its participation in any exchange of signalling messages between itself and the HA. Instead, a proxy mobility agent performs the signalling with the HA being in charge of managing the mobility on behalf of the MN attached to the network. The benefits of developing a network-based mobility approach based on Mobile IPv6 is the reuse of HA functionalities as a mobility agent for all types of IPv6 nodes, and the use of the same messages format in mobility signalling. The most relevant core functional elements of the PMIPv6's architecture are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). LMA plays the role of the home agent described in MIPv6 for the MN in a Proxy Mobile IPv6 domain, while it manages the binding state of the MN. MAG does the tracking process detecting the MN's movements, and manages the mobility-related signalling of each MN that is attached to its access link. For each group of MNs, there are several LMAs serving them in a PMIPv6 domain. The architecture of this protocol is shown in Figure 2.5.

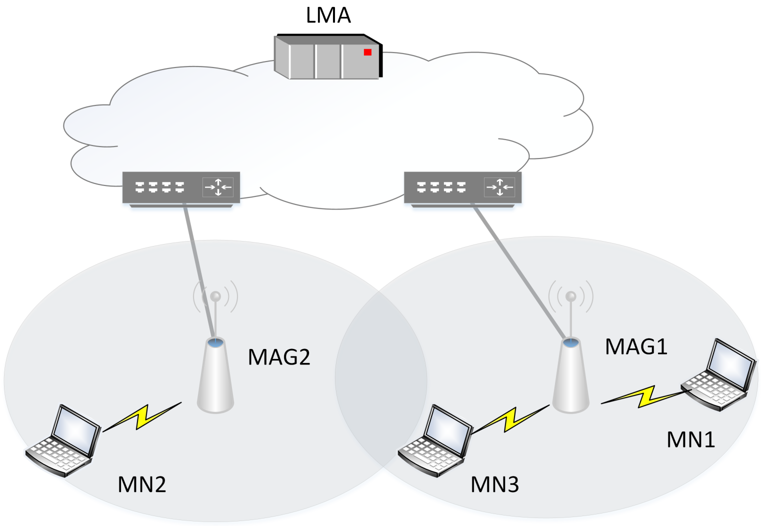

Figure 2.5: Architecture of PMIPv6.

When a MN enters in a PMIPv6 domain and before, it sends a Router Solicitation (RS) message, its attaches to an access link. Then, the MAG sends a Proxy Binding Update (PBU) message to the MN's LMA to update the current location of the MN, and receives a Proxy Binding Acknowledgement (PBA) message including the MN's HN prefix from the MN's LMA. At this point, the LMA and MAG create a Binding Cache entry and configure its endpoint of the bi-directional tunnel to the MAG and to LMA, respectively. In addition, the MAG sets up the forwarding for the MN's traffic and is able to emulate the MN's home link. At the end, the MN receives the RA message and configures its interface using statefull or stateless address configuration. The current MAG and the LMA have proper routing states for handling the traffic sent to and from the MN, and this one has at least one valid address from its HN prefix.

The PMIPv6 [25] is a well-known protocol that provides a solution for network-based mobility management. By introducing this protocol and its features, it is expected that it brings scaling benefits for localized mobility management. Furthermore, PMIPv6 may reduce the latency in IP handovers by limiting the mobility management within PMIPv6 domain. Therefore, handover performance is optimised. It also reduces the signalling overhead related to handovers since it avoids tunnelling overhead over the air and stack updates in the host [26].

2.4.3.5 Distributed Mobility Management Approaches

The available mobility management solutions, including host and network based mobility, that are derived from MIP concepts, dealing with a hierarchical structure in which mobility anchor is a centralized network entity processing MN context and data traffic encapsulation. Therefore, mobility management with centralized mobility anchoring in the traditional hierarchical mobile networks represents scalability issues and routing problems. Moreover, the present mobility anchor is a single point of failure, introducing higher signalling loads and longer delays. However, these mobility protocols enable IP session continuity by providing to the MN with an IP address or prefix that remains the same while the MN moves and attaches to different access networks. Despite these factors, a major trend in mobile networks evolution is to flat the network by confining mobility support in the access routers level. As an alternative approach, the new solutions consider an innovate manner to better adapt mobility support in the today's networks to cope with users' movements patterns and its ongoing data traffic flows.

In this context, it will be studied two distributed mobility management solutions which improve the aforementioned centralised approaches. The first solution proposes a slightly different approach from PMIPv6 by dynamically distributing the mobility management functions handling among access routers and terminals. According to [27] such solution is called Distributed Mobility Anchoring (DMA) and the main goal is to dynamically adapt mobility support when the MN performs an IP handover by applying data traffic redirection. The second one named DMIPA [28] is a host-based distributed mobility management approach where the mobility management functionalities are applied to ARs and MNs providing dynamic sessions anchoring, independently of the access technologies and Internet service provider. This protocol supports global IP mobility on flat network architectures, and has been developed in our research group.

2.4.3.6 Distributed Mobility Anchoring (DMA)

The base concept of DMA [27] [29] is to dynamically adapt the mobility support for each MN's requirements by redirecting the traffic flows that are already established when an IP handover occurs, and also to provide and restrict the mobility support functions at the access routers level, in such a way that the rest of the network does not know anything about mobility events. The architecture is depicted in Figure 2.6 and relies on a simple flat model. It adds two new entities: session database and Mobility capable Access Router (MAR). The session database is a centralized element that stores ongoing mobility sessions for the MNs. In other words, this database stores the home network prefix(es) currently allocated to the

MN and their related anchoring points. The MAR is an access router and provides mobility management functions. It has the capability of anchoring the MN's sessions and update its location.

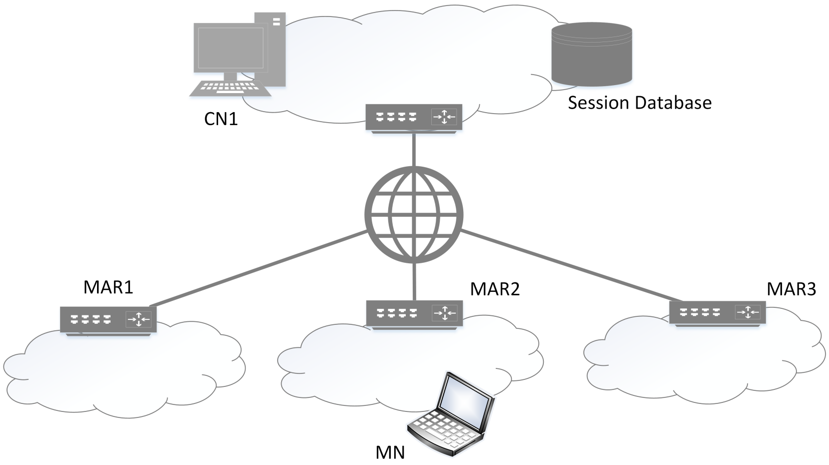

Figure 2.6: Architecture of DMA.

Initially, the MN is attached to MAR1 and initiates a communication which can be VoIP, video or data transfer with CN1. The traffic will be routed through MAR1 without requiring any specific mobility operation. When the MN moves from MAR1 to MAR3 and attaches to it, the data traffic remains anchored to MAR1 and it is established a tunnel between those MARs. Therefore, MAR1 becomes the current mobility anchor for data traffic initiated by the MN when it was attached to MAR1. If MN initiates a communication with CN2, the packets will be routed in a standard way via MAR3. In case the MN roams to another MAR, two mobile anchors come into play: the MAR1 anchoring the data traffic for communication with CN1 and MAR3 for communication with CN2.

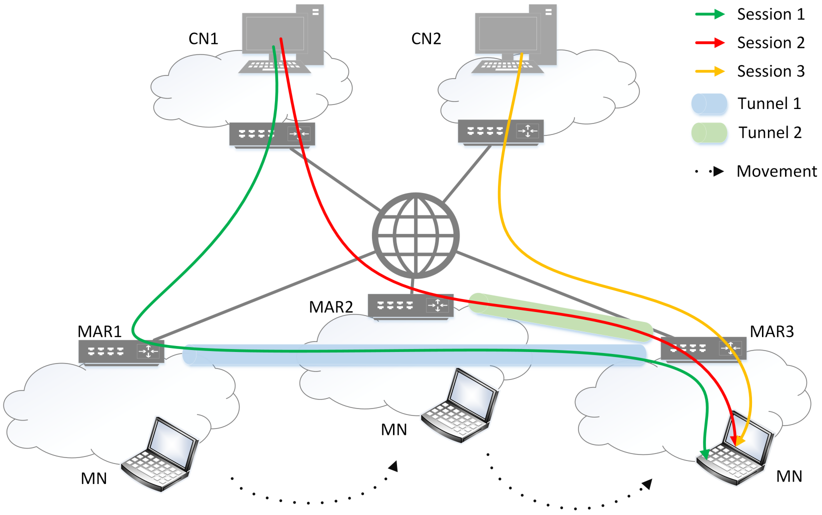

Figure 2.7: DMA operational example.

This solution provides MARs to manage the tunnelling between them, even if a MN is roaming across various MARs. Due to the fact that the home networks prefix is anchored to its mobile anchor, it is required that each MAR must advertise distinct set of prefixes per-MN.

2.4.3.7 Dynamic Mobile IP Anchoring (DMIPA)

DMIPA [28] is a new approach, based on the host, that aims to provide distributed mobility management in a flat and heterogeneous networks. Thus, the MN is able to perform global mobility in a better way. In this context, since the CN can be any node of the network, it does not need to have mobility functionalities. Therefore, allocating mobility management functions into MNs and maintaining the set of functions into mobility anchor entities achieves a more flexible and scalable mobility approach. Moreover, not every AR is prepared to support mobility management, so it is assigned mobility functionalities to the MNs to guarantee global mobility support independently of the access network and point-of-attachment. The MN plays a significant active role in the proposed approach when it is linked to an AR without mobility support, with the advantages to be agnostic to the heterogeneous network. The DMIPA's architecture is composed mainly by two entities, the MN and the Data Mobility Access Router (DMAR). The DMAR is an AR with IP mobility management functions and, together with MN,it is responsible for maintaining session continuity. As shown in Figure 2.8, if the MN is connected to DMAR1 and initiates a data traffic flow with CN1 and roams to DMAR2, the session has to be maintained along the movement. So, when the MN moves from DMAR1 to AR, which does not support any mobility functionalities, the MN has to perform the tunnelling/detunnelling and address translation itself. If the MN starts a new session with CN2, the packets are tunnelled via the DMAR1 which is the current anchor point. The anchor selection is a mechanism in charge to select the IP address of the MN that should be used for the new session. The selection of the anchor is an important factor, since this protocol deals with both DMARs and ARs and each session is anchored once in the initiation phase. Finally, the MN moves to DMAR2's network and attaches to it (Figure 2.9). In this case, DMAR1 and DMAR2 establish a tunnel to keep the ongoing sessions, and the MN is responsible to maintain a set of DMARs, thus the need of a centralized database is eliminated.

2.4.3.8 Summary

When evolving towards future heterogeneous network generations, the expectations are high in providing to the end users with session continuity and high dynamic mobility in wireless networks.

The current centralized mobility management schemes for the L3 layer may encounter scalability issues due to the creation of single point of failure and network bottleneck elements. When the mobile traffic significantly increases, these problems get worse, causing network performance problems. However, alternative schemes have been proposed to distribute the control and data path functions. These schemes, such as DMA and DMIPA, can be seen as promising approaches to improve the mobility support, maintaining the continuity of sessions, while dynamically distributing the mobility management functionalities through the access nodes and mobile nodes. The evaluation of DMIPA's benefits and evaluation comparison with MIPv6 are presented in [28]. The authors concluded that DMIPA optimizes the mobility management overall performance when compared with MIPv6.

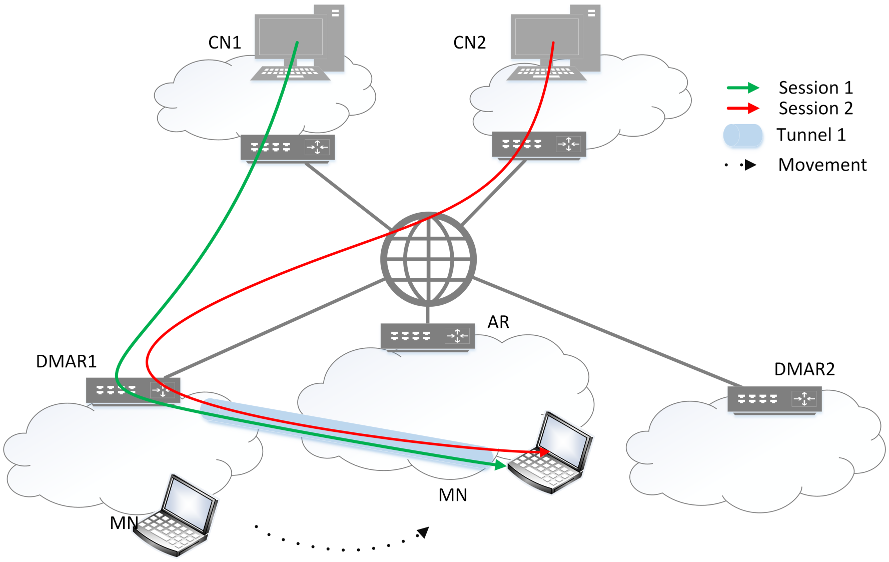

Figure 2.8: a) DMIPA operational example.

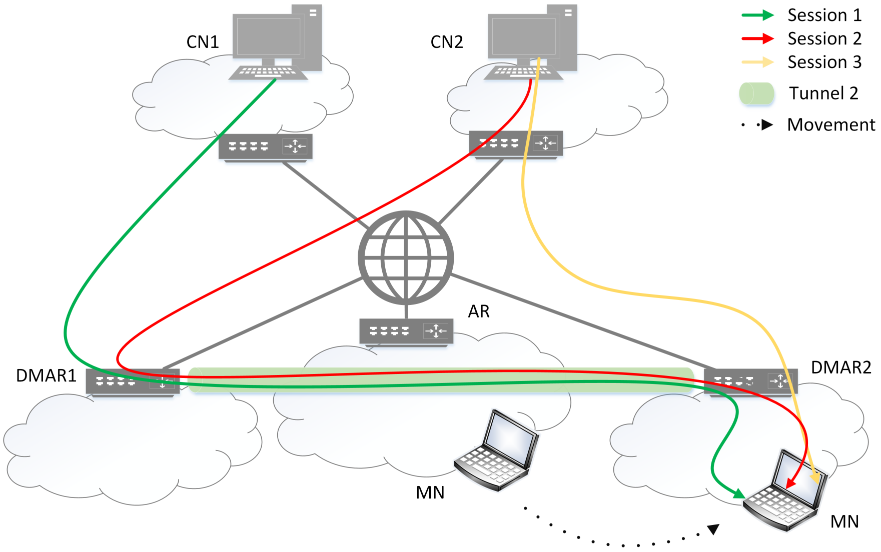

Figure 2.9: b) DMIPA operational example.

There is a paradigm shift to distribute the mobility management which results in the improvement of the network performance, allowing the end users to move dynamically, while keeping the ongoing sessions.

Distributing the mobility management functions shall be aimed as the new approach for the future of heterogeneous networks. It is important to continue exploring and evaluating these distributed mobility management schemes in order to develop a qualitative comparison focused on the performance, security, deployment, scalability, and robustness properties of each approach.

2.4.4 WiMAX Mobility Management

The increase of user mobility and the demand for data access at any time and any place have motivated the deployment of Broadband Wireless Access (BWA) technologies. It is expected that BWA will play an important role in the Next Generation Networks (NGN) [30]. The IEEE 802.16e standard [31] is a solution to BWA frequently known as mobile WiMAX that incorporates mobility management and quality of services mechanisms at the Media Access Control (MAC) layer to guarantee seamless mobility services for data, video and voice. Mobile WiMAX adds significant enhancements and improves scalability in both radio access technology and network architecture; therefore, it provides flexibility in network deployment and service offerings.

As defined in IEEE 802.16e, mobile WiMAX supports two handover methods: Hard Handover (HHO) and Soft Handover (SHO). In the first method (HHO), the serving network link is broken before the Mobile Station (MS) performs the handover and the target link is established. This process is commonly called "break-before-make" approach. On the other hand, before the serving network link is broken and the handover is executed, the SHO method prepares and establishes the target link ("make-before-break"). Thus, the SHO provides a complex method to maintain connectivity for the MS while it requires backbone communication between the serving and the target access technologies. Additionally, while HHO is mandatory, two types of SHO are optionally supported. They are Fast Base Station Switching (FBSS) and Macro Diversity Handover (MDHO). In both cases, a mobile user and Base Station (BS) maintain a list of BSs involved with the mobile user's handoff. However, in FBSS a mobile user only communicates with the anchor BS instead of communicating with all the BSs in the active set, as it happens with MDHO.

Figure 2.10 illustrates the handover procedure in mobile WiMAX when the MS initiates a handover between BSs located in the same Access Service Network (ASN) and a brief explanation is given below.

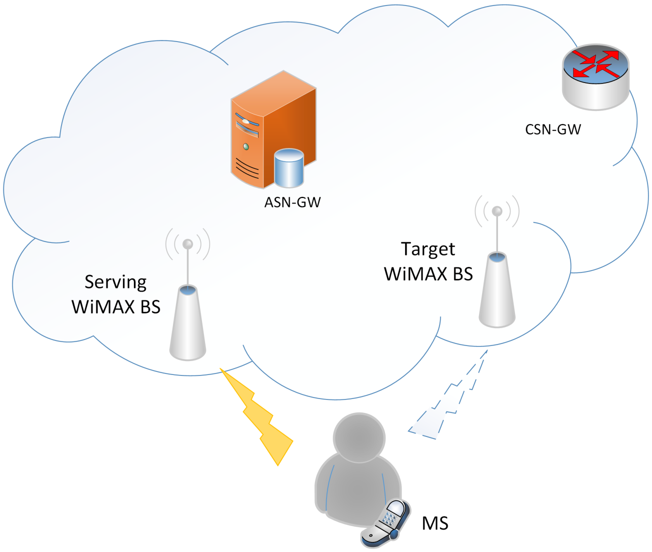

Figure 2.10: WiMAX intra-ASN handover procedure.

The MS is connected to the serving BS and receives the Mobility Neighbor Advertisement (MOB-NBR-ADV) MAC management message. Such message informs the MS that WiMAX

BS is available in the surrounding area. Then, MS initiates the handover preparation phase and sends Mobility Mobile Station Handover Request (MOB-MSHO-REQ) MAC management message to the serving BS with the list of the candidate BSs to execute the handover. Now, the serving BS is able to send Handover Request (HO-REG) backbone message to the candidate BSs, and the required QoS parameters information to fulfil the MS active services. The serving BS will receive a Handover Response (HO-RESP) backbone message from the candidate BSs indicating if the QoS resources are available or not. After the serving BS collected all the replies, it sends a Mobility Base Station Handover Responde (MOB-BSHO-RESP) MAC management message informing the MS about the recommended candidate BSs. Finally, the MS selects the target BS and notifies the serving BS about the handover using the Mobility Handover Indication (MOB-HO-IND) MAC management message, and the serving BS informs the target BS that the MS will perform handover by using the Handover Confirm (HO-CNF) backbone message. During this procedure, it is not mandatory that a managed MS retrieves new IP address configuration, thereby a MS may retain IP connectivity using network layer protocol exchange over the secondary management connection.

2.4.5 Long Term Evolution Mobility Management

Mobile communication systems revolutionized the user's behaviour and the manner they communicate with each other. Evolution of wireless technologies, especially mobile communications, have been remarkably growing in the past years. However, the concerns about mobility management along all "generations" of mobile communications (1G up to 4G) [32] have been rapidly increased, and the desire for seamless connectivity and sessions continuity triggered the interest in realizing a depth research.

Mobility Management in Long Term Evolution (LTE) [33] can be categorized into two types: intra-LTE mobility, which refers to mobility within LTE system; and inter-RAT (Radio Access Technology) mobility, which introduces mobility to other systems such as Third Generation Partnership Project (3GPP) systems (e.g. Universal Mobile Telecommunications System (UMTS)) and non-3GPP systems.

Intra-LTE mobility can be performed either over the S1 interface or over the X2 interface. When the User Equipment (UE) initiates a movement from evolved NodeB (eNodeB) to another eNodeB within the same (Radio Access Network (RAN) attached to the same Mobility Management Entity (MME), the mobility mechanism takes place over the X2 interface. If the UE moves from one eNodeB to another that belongs to a different RAN attached to different MME, then the mobility takes place over the S1 interface. This mobility procedure is also applied when two eNodeBs are not connected over an X2 interface. The inter-RAT mobility makes use of S1 interface to manage the mobility and, in the case of Packet Data Convergence Protocol (PDCP) existing in the UE and eNodeB which controls the air interface and maintains integrity protection and integrity verification of control plane data, the UE needs to re-establish its session once it moves to the target non-LTE system. In order to provide a brief explanation about the mobility procedure over X2 interface in LTE, it is important to clarify that mobility over this interface is the operational default mode in LTE if the X2 interface is available between the current and target eNodeBs. Three steps are assumed for mobility over the X2 interface: Preparation Phase, Execution Phase and Completion Phase. Initially, the current eNodeB sends a Handover Request message to the target eNodeB. When the target eNodeB receives this message, it starts to set up the required resources for the UE. Although, it is possible to set up the resources on a per-RAB basis. This method makes the handover faster and seamless because after the completion of the handover the UE will have the same RABs at the target eNodeB with the same QoS as it had on the current eNodeB. Then, the eNodeB responds with a Handover Request ACK message once it is ready and the Preparation Phase is complete. During the Executing Phase, the current eNodeB sends a handover command to the UE after it receives the Handover Request ACK. The current eNodeB starts to transfer the data to the target eNodeB while UE completes the handover procedures. Finally, at the Completion Phase, the UE sends a handoff complete message to the target eNodeB after finished the handover procedure. The target eNodeB sends a path switch request to MME/Serving-Gateway, and the GPRS Tunneling Protocol (GTP) tunnel is switched from the current eNodeB to the target eNodeB by the Serving-Gateway. Then, the target eNodeB informs the current eNodeB to release the resources used by UE on the beginning.

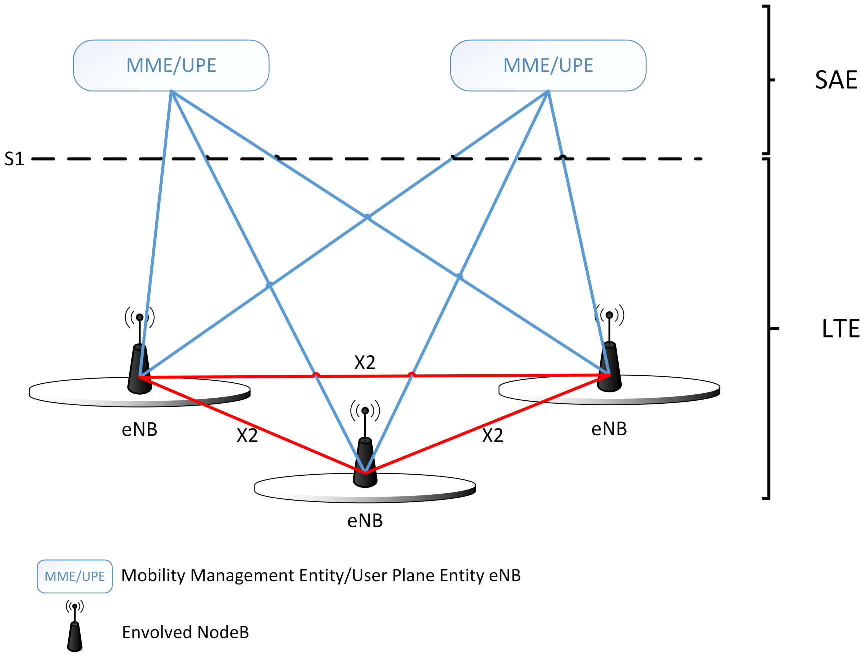

Figure 2.11: LTE architecture.

2.4.6 Summary

Currently, the mobility management of a mobile device is classified into terminal mobility, personal mobility, session mobility, service mobility and roaming. In order to improve the mobility management in today's networks, several mobility management protocols meet the users' requirements, where the social behaviour, mobility patterns and the demand for uninterrupted sessions rise great challenges to the mobility management.

Mobility management solutions address the mobility problem from different perspectives. For the TCP/IP stack protocol perspective, it was presented the most popular solutions. In one hand, mobility management schemes based on both Application and Transport layer enjoy several advantages, such as soft handoff and tunnelling avoidance. Therefore, it can be deployed without any change in the network infrastructure. On the other hand, mobility management schemes based on the IP Network layer provide transparency to the upper layers and the use of tunnelling scheme enhances scalability.

Concluding, each solution that was presented in this section focusses on solving some challenges of mobility management to guarantee seamless mobility.

2.5 Multihoming

Multihoming is the ability to have a node reachable through multiple paths. Three different situations can occur: a node has several network interfaces connected to various access networks, the subnet in which the node is located is multihomed itself, or both cases are also possible [34]. The concept of multihoming improves the reliability of network applications, and it is expected to enhance the communications' performance. For example, a MN may be simultaneously connected to a 3G cell network, 802.11p LAN and a wired Ethernet LAN. Nodes with multihomed capabilities receive configuration information from its current attached networks through DHCP (Dynamic Host Configuration Protocol) version 4 and 6, IPv6 Router Advertisements and PPP (Point-To-Point Protocol), and they have to decide which of the information to use or how to combine them. Others issues such as multiple interfaces management, addressing and naming overlaps are described by M. Blanch and P. Seite [35]. As the use of devices in high mobile and dynamic environments are more common, the introduction of multihoming will allow to solve the problems of roaming between different networks and technologies while travelling. Despite the fact that MIPv6 [16] aims to allow a MN to maintain IPv6 communication while moving across IPv6 subnets, the current solution lacks support for MNs with multiple IPv6 addresses configured at a single interface, i.e. multihomed mobile hosts. Some solutions have been proposed to extend MIPv6 for multihomed mobile hosts to provide ubiquitous, reliability and permanent access to the Internet. The work in [36] performed an analysis of multihoming in MIPv6 to define the problems in order to guarantee that future solutions will address all issues. They propose a taxonomy to classify the situations where MNs could be multihomed, and then it is used to determine the issues related to this topic. According with the number of HoAs and CoAs, it is defined five types of configurations and its multihoming goals.

- 1 HoA, 1 CoA: a scenario where the MN has two interfaces connected to different IPv6 subnets, one interface is attached to the Home Network, and the other is attached to the Foreign Network. Thereby, the MN configures a single HoA and a single CoA. As advantage of this scenario, the access is ubiquitous, the communications are reliable, the MN is able to use both interfaces at the same time, and when the MN initiates the communication, it is possible to share and balance the load through both interfaces.

- n HoAs, 1CoA: the scenario where the MN is connected to the Internet through several distinct HAs, and each operator offers a MIPv6 service to the node. In such context, the MN will have a HoA per HA. On the other hand, the home network may be multihomed if the MN has multiple prefixes on the home link. However, in both cases, the MN has to configure the CoA to all the HoAs it owns. The achievable goals are similar as described earlier (reliability, ubiquitous access, load sharing, load balancing, bicasting and preference settings).

- 1 HoA, n CoAs: if the MN's interfaces are connected to a link where multiple IPv6 prefixes are available, the MN becomes multihomed because it has several CoAs. The reason why the MN has several prefixes is that each provider announces its prefix in the visited network. Nevertheless, the MN could be connected to its Home Network using one of its interfaces. Reliability, load sharing, bicasting and preference settings are the benefits achieved by this case.

- n HoAa, n CoAa: in this case the MN is multihomed because it has multiple addresses. It can be considered a node with three interfaces, two of them connected to their home link, and the last one connected to a visited link where serveral IPv6 prefixes are available. The potential advantages are reliability, ubiquitous access, load sharing and load balancing, bicasting and some preferences settings. Note that the present scenario can be assumed as a combination of the two scenarios described above.

- n HoAs, 0 CoAs: the MN is only connected to its home link. This means that interfaces are not connected to the visited network, and therefore, the node is considered a fixed node from a multihoming point of view. This case has the equivalent goals explained above.

Although the described cases provide a set of rich goals, there are still some protocols that may not be able to guarantee the requirements expressed earlier. Some of the concerns are related to the MIPv6 itself, but others are not. The general IPv6-related issues are related to implementation that are not specific to MIPv6. They are path selection, ingress filtering, failure detection. If there are more than one path from and to the MN, the MN has to choose a source and destination address, and consequently, the interface to initiate the communication. So, when the MN has multiple available interfaces, it has to decide which flow would be transmitted to which interface, or which flow should not be used over a given interface. The interface selection mechanism has to decide which interface would be used based on users or applications policies and preferences. The selection of HoA is also an important factor, because when different HoAs are available, and before the MN sets up the communication flow with some CN, it has to select the appropriated HoA. Similarly, the MN has to select a CoA between the set of available CoAs, to use for a particular session or flow. The selection of the CoA must use internal policies to deliver its session. The path selection has another related aspect which is the ingress filtering. This technique aims to guarantee that incoming packets are actually from the networks that they are claim to be from. So, to experience multihoming, it is important to avoid ingress filtering, but the selection of path would be limited by the choice of addresses used. Furthermore, the loss of connectivity, the broken path between the MN and the HoA or the disconnected home link are issues in which IPv6 has no clearly a defined detection mechanism to solve failures. Finally, it is necessary to provide mechanisms to redirect flows from a failed path to a new path, and mechanisms to decide which of them are better to be used when multiple paths are available. Solutions for these issues are required for MNs to fulfil the advantages of being multihomed.

The PMIPv6 [25] supports multihoming [37], since the MN may have different prefixes provided by the LMA, which are associated with an interface of the MN, or when the MN is connected to a PMIPv6 domain through several interfaces. Each interface is managed independently of the mobility session, since the MN gets assigned distinct set of prefix(es) per interface, but the interfaces do not have the same IP address, and consequently, when a packet arrives to a different interface, it will be discarded. The MN is able to communicate using all interfaces, but such interfaces are not assumed as bellowing to the same user, and therefore, the traffic flow cannot be forwarded between interfaces. However, the multihoming operation in PMIPv6 needs to improve the efficiency and to extend the applicability to other deployment scenarios to create dynamic mobility sessions via interfaces and between them.

The current DMIPA protocol ensures distributed and dynamic mobility management support. However, it does not provide multihoming features for MN with multiple interfaces. Condeixa and Sargento [28] describe the protocol operation of DMIPA for a single interface MN. Assuming a MN with several interfaces, the operational mode of DMIPA may be different from the traditional one. Multihoming scenarios, such as the use-case scenario depicted on Figure 2.12, create new challenges to optimize network resources and enhance the user experience, raising a set of benefits such as reliability, session continuity in multihoming scenarios, load balancing and preference settings.

Having in mind the concept of Multihoming, its features and challenges, this document presents a study and evaluation of DMIPA with multihoming support for a multiple interface mobile node. Chapter 4 explores this concept, by describing the possible scenarios and by deploying the required mechanisms to test the dynamic mobility management with multihoming support in a real testbed.

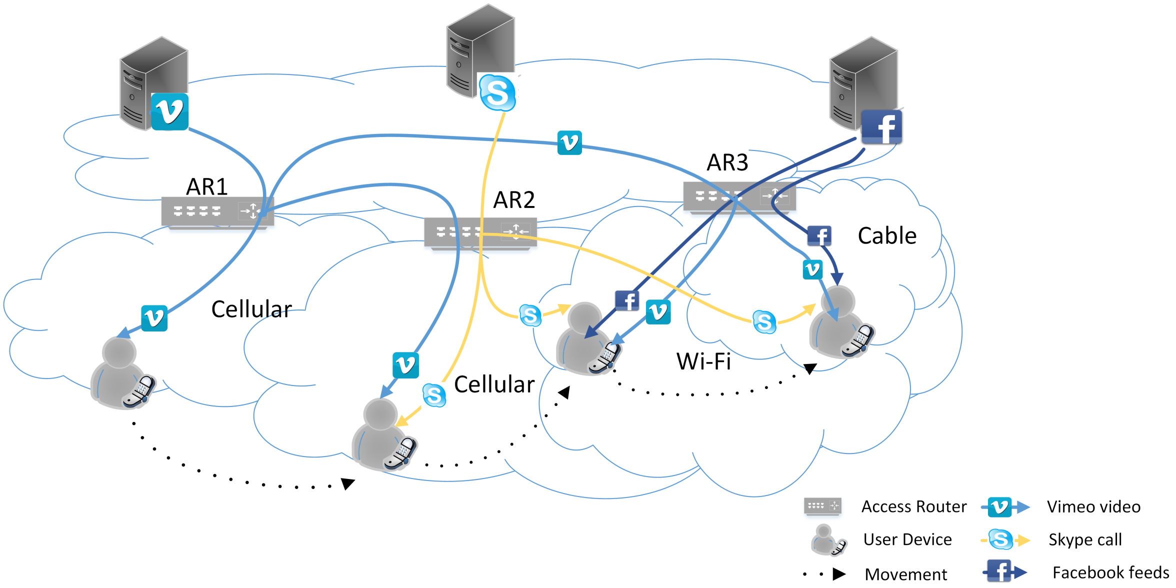

Figure 2.12: Use-case scenario.

2.6 Vehicular Ad-doc Networks (VANETs)

Vehicular Ad-doc Networks (VANETs) [1] are a modern class of wireless networks in which mobile nodes are vehicles. Such wireless networks have emerged due to the great advances in wireless technologies and the innovation in automotive industry. Since it provides communications between single vehicles and between them and the nearby fixed roadside equipments, the main goals of VANETs are to improve road safety by providing timely information to drivers as well as to concerned authorities. The vehicles can be either private, belonging to individuals or private companies, or public transportation means, and they are equipped with homogeneous or heterogeneous technologies in their wireless interfaces. The fixed roadside equipments can belong to other entities such as government, private network operators or/and service providers. Indeed, the high interest for these networks triggered the creation of specific research groups, commercial organizations and consortium, which aims to increase road traffic safety and improve efficiency by means of intervehicle communication.

2.6.1 Vehicular Network Architectures

Recent advances in wireless technologies and the current and advancing trends in ad-hoc network scenarios allow a number of deployment architectures for vehicular networks. Since architectures should allow communication among nearby vehicles and between vehicles and fixed roadside equipments, the Car-to-Car Communication Consortium (C2C-CC) [38] proposed an architecture that can be distinguished in three domains: in-vehicle, ad-hoc and infrastructure domain. The reference architecture is illustrated in Figure 2.13.

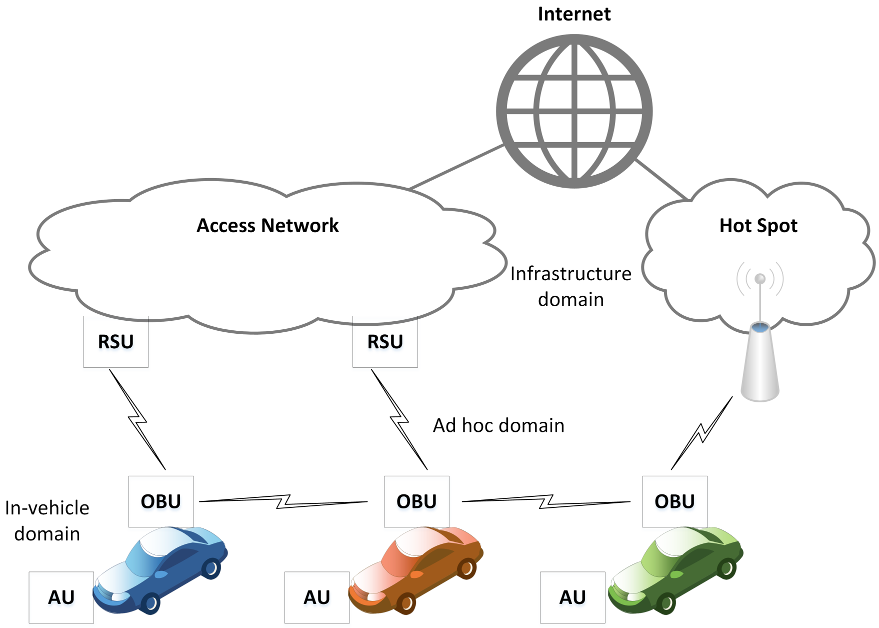

Figure 2.13: C2C-CC Reference Architecture [1].

The in-vehicle domain is a local network inside a single vehicle logically composed of two main units: On-Board Unit (OBU) and at least one Application Unit (AU). The OBU is a device that has communication capabilities either wireless or wired, while the AU is a device that executes applications making use of the OBU's communications functionalities. A set of vehicles equipped with OBUs and Road Side Units (RSUs) that are statically along the road form the ad hoc domain. The infrastructure domain can be composed in two sub-types:

a) RSUs that allow OBUs to attach to the infrastructure and, therefore, access to the Internet.

b) Hotspots are an alternative way to OBUs to communicate with Internet via public, commercial or private Wi-Fi hotspots.

Otherwise, OBUs can use cellular technologies such as WiMax, General Packet Radio Service (GPRS) and/or LTE to communicate with the network and consequently with Internet.

According to the explained reference architecture and taking into account the evolution of heterogeneous communication technologies, vehicular networks have two possible deployment communication scenarios: Car-to-Car (C2C) communication scenario and Car-to-Infrastructure (C2I) communication scenario. They can be integrated into wireless hotspots along the road which can operate individually by wireless Internet service providers or and integrated operator. The vehicles can communicate between them without a fixed infrastructure cooperating and forwarding critical information. The combination of these two deployment scenarios is also possible.

2.6.2 Characteristics of Vehicular Networks

The VANETs have distinct features and special behaviours, making them unique networks when compared to other types of mobile networks. These characteristics include:

- Unlimited transmission power, since the vehicle can provide continuous power,
- Higher computational, communication and sessing capabilities,
- Predictable mobility. Vehicles can change speed and direction constantly; however, the movements are limited to roadways.

Nevertheless, some characteristics have to be managed by specific mechanisms to provide useful services for drivers and passengers:

- Potentially large scale, in which vehicular networks can assume a big network size, and therefore, include many participants, unlike the traditional ad-hoc networks,
- High mobility. For example, in a highway the vehicles can achieve relative speeds up to 300 km/h with a density of 1 or 2 vehicles per 1 km, while in the city relative speeds of 60 km/h may occur and the vehicles' density will be very high. Furthermore, such characteristics rise new challenges for mobility management,
- Partitioned network and the frequent fragmentation due its dynamic behaviour,
- Network topology and connectivity frequently change, while vehicles are moving and changing their position and point-of-attachment.

2.6.3 Business and Technical Problems

The excitement surrounding vehicular networking is not only due to the applications or their potential benefits but also due to the challenges and scale of the solutions. Among technical challenges to be overcome, a number of these requirements are following discussed.

2.6.3.1 Routing and Dissemination

Unlike the conventional ad-hoc wireless networks, vehicular networks experience rapid changes in wireless link connections and different network densities. Then, routing and dissemination protocols should be efficient and should adapt to vehicular networks characteristics. Therefore, the algorithms should permit distinct transmission priorities according to application type: safety-related or nonsafety-related. The research community has focused on analysing routing algorithms to handle the broadcast storm problem in a network with very high density. As for message dissemination, the dissemination algorithms should depend on the network density and also on the application type. Therefore, safety-related application should disseminate the messages to all nodes on the network (broadcast-like) to ensure the message propagation to the required cluster of vehicles without causing broadcast storm. On the other hand, non-safety-related applications should transfer the messages through unicast or multicast transmission.

2.6.3.2 Security

Security in vehicular communication is an essential aspect that should be treated carefully due to potential impact on the future of deployment and application of vehicular networks. So, it is important to propose innovative solutions for secure communication between participants. Appropriate architectures should be in place providing communication between vehicles and allowing different service access. The security and privacy mechanisms should be focused on providing trust, authentication and access control authorization.

2.6.3.3 Mobility Management and IP Configuration

The vehicle-to-infrastructure architecture has tremendous potential if vehicles can have access to Internet as well as Internet-related services. However, two mobility challenges exist under this context: IP address configuration and mobility management. Triggered by the need of ubiquity and heterogeneity, the research community and international committees, such as IETF, started to develop several solutions that address the problem of terminal mobility and IP configuration. Some approaches deal with IP mobility management to enable the movement of terminals while preserving the communication context for running sessions. Indeed, the absence of mobility management mechanisms compromises service commercialization in vehicular networks and loses of benefits in vehicle-to-infrastructure architecture, since Internet-related services would not guarantee continuity and quality of services.

Moreover, the deployment of a hierarchical architecture which introduces a centralized element that manages the mobility of the vehicles will bring several performance limitation. As described previously, this centralized element, the HA in MIPv6 and the LMA in PMIPv6, is able to manage the mobility procedure of a few vehicles, without disruption of session continuity. However, in vehicular networks, there are several vehicles moving spontaneously and dynamically through the network. In order to manage the mobility of a huge amount of vehicles it is required a flat architecture, distributing the mobility management functionalities through the access routers. Chapter 3 evaluates the performance of a distributed mobility management scheme in contrast with the centralized mobility management architecture of MIPv6.

2.6.3.4 Distribution of Applications

Vehicular networks should have an unique platform in which drivers and passengers will be able to access services with an acceptable quality level while facilitating message exchange between vehicles. Consequently, to achieve this requirement it is important to develop new distributed algorithms to manage the group of participants and ensure data sharing among distributed programs.

2.6.3.5 Business Models

The manner how the people will make business in vehicular networks by distributing and commercializing services and applications represents an important challenge. The business model should be profitable for telecommunication operators and service providers aiming to promoting services with affordable and attractive prices for clients. Therefore, there must be special accounting mechanisms and tailored billing systems in order to provide easy and fast payments.

2.7 Conclusion

In this Chapter it was presented the mobility management solutions for different layers of the TCP/IP stack. According to the advantages and disadvantages of each paradigm, it is concluded that current mobility management solutions do not solve all the issues related to Internet mobility. However, the mobility management solutions based on the network layer can handle most of the requirements. Moreover, adding the multihoming concept to the mobility management mechanism will improve the reliability of networks applications and reachability to the mobile nodes in order to ensure session continuity, enhancing the communications' performance.

With the remarkable growth of mobile nodes and the rapid evolvement of mobile data traffic consumption, the need to support seamless, robustness and continuous multimedia services in vehicular scenarios is increasing. Then, it is important to understand the characteristics and challenges of vehicular networks, in order to enable terminals' movement while session continuity is maintained.

The next chapter (Chapter 3) will evaluate the performance of both IP mobility protocols: MIPv6 and DMIPA, in vehicular environments. The main objective is to understand the impact of each mobility management protocol and its related architecture, comparing signalling and data cost, data loss, average data delay and binding update time. For this purpose, it is created a network which connects the static correspondent nodes, gateways, core routers, and access points. Then, it is introduced traffic mobility patterns, where the vehicles represent the mobile nodes. Finally, the scenarios are tested and it is presented the results, analysis and comparisons.

The main focus of Chapter 4 is to show the multihoming concept by providing DMIPA with proper mechanisms in a real testbed. It gives a description of the testbed as well as an explanation of the use-case scenarios and the tests performed. The results and analysis are presented in the final of the chapter.

Chapter 3

Evaluation of MIPv6 and DMIPA performance in Vehicular scenarios

3.1 Introduction

With the increasing demand of traffic applications, it is required to support seamless multimedia services in the VANETs and Intelligent Transportation Systems (ITSs). Moreover, such traffic applications like traffic surveillance, traffic congestion, vehicle location and navigation, electronic toll collection and multimedia services require continuity while the vehicles move and change its point-of-attachment. Several mobility protocols have been developed to ensure seamless handover. The MIPv6 provides a set of features to solve the mobility issue, but its centralized architecture is quite prone to suboptimal routing raising scalability problems, network bottlenecks, long handover latency and consequently high packet loss. On the other hand, FMIPv6 solves these problems by predicting the handover, but a rapid change of direction and the high speed of vehicles make prediction mechanisms non-optimal and inaccurate.

However, distributed mobility management has been growing as a promising approach in the evolution of network architectures, where a modern society behaviour consumes a significant part of available network resources, in such manner that service providers are already implementing selective traffic offload strategies through the wireless local area networks. Hence, there is a paradigm shift in the network architectures with the deployment of flat models to deal with the growth of mobile traffic. Furthermore, session continuity should be guaranteed independently of the network architecture models, access technology or the type of multimedia service. DMIPA aims to provide session continuity in distributed and dynamic environments, moving the active sessions between networks through adequate mobility management mechanisms.

The performance of both IP mobility protocols, MIPv6 and DMIPA, are evaluated in a VANET simulation scenario. For this propose, it is given a brief introduction of the current simulation platforms. Based on the principal key features, it is chosen one network simulator and one vehicular mobility simulator providing a detailed description of the deployed scenarios and the modification performed in order to achieve the requirements of this work.

3.2 MIPv6 and DMIPA

This section provides an architecture overview of both mobility management protocols, as well as an in-depth analysis of the protocol operational mode.

MIPv6 is the standard host-based protocol that provides global mobility to mobile nodes, and its architecture is illustrated in Figure 3.1.

The protocol operation is explained according to Figure 3.2 and following the scenario presented in Figure 3.1. The BU message notifies the HA or the CN of the current binding of the MN. The BA is used to successfully inform the MN about the reception of a BU message. The RS and RA messages are defined in IPv6 Stateless Address Autoconfiguration [19].

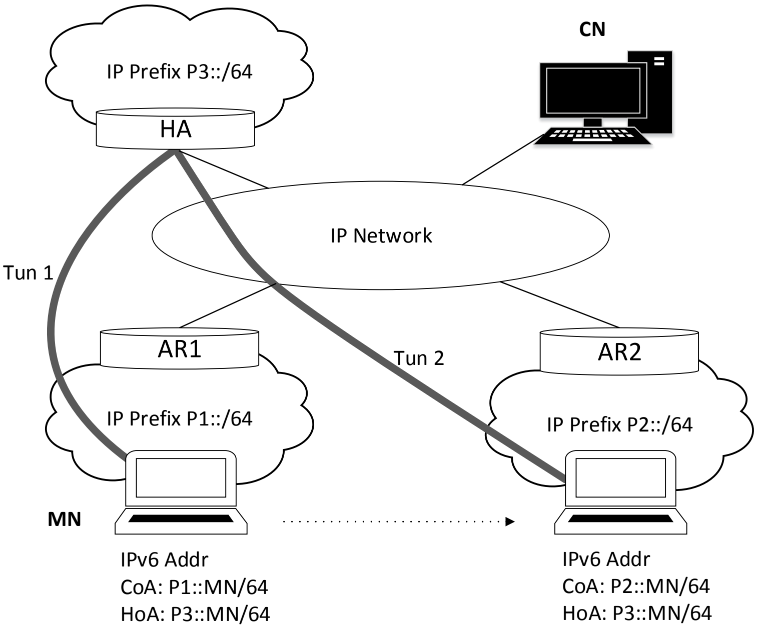

Figure 3.1: MIPv6 Architecture Overview.

MIPv6 works as follows:

1) **AR1**: The MN attaches to AR1.

2) **RS/RA**: MN sends RS message and receives RA with the network prefix P1::/64.

3) **Configure P1::MN/64**: The MN configures the CoA IPv6 address P1::MN/64.

4) **BU/BA to HA**: The MN performs the binding registration by exchanging BU and BA with HA. From now on, the packets are intersected on behalf of the path and are tunnelled to the MN.

5) **Data session 1**: MN initiates data session 1 using P1::MN/64 as IPv6 source address.

6) **AR2**: The MN moves from AR1 to AR2 and attaches to it.

7) **RS/RA**: the MN sends RS message to AR2 and receives RA from it with the network prefix P2::/64.

8) **Configure P2::MN/64**: MN acquires its CoA through a stateless or stateful auto-configuration.

9) **BU/BA to HA**: The MN performs the binding registration by exchanging BU and BA with HA. From this moment, the packets are intersected on behalf of the path and are tunnelled to the MN.

10) **Data session 1**: CN sends the data packets to the HoA, which are intersected by the HA and then tunnelled to the MN.

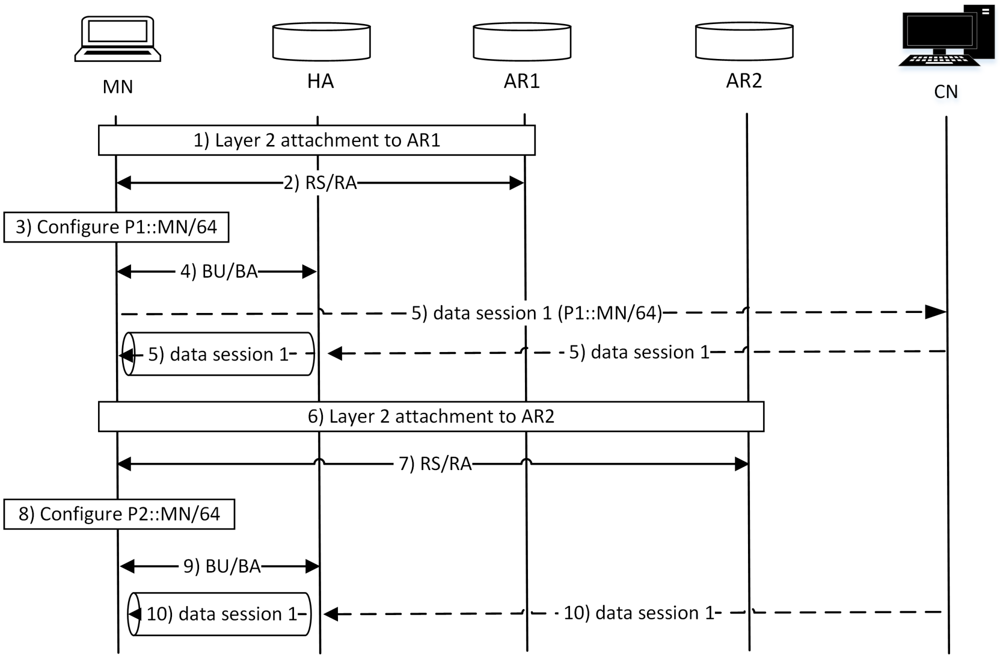

Figure 3.2: MIPv6 Operational Mode and Exchanged Messages (without RO).

DMIPA is a host-based distributed mobility management approach to provide global mobility. The MN can move through the heterogeneous network changing its point-of-attachment while still reachable. Since the CN can be any node of the network, this protocol does not provide mobility support to the CN. As depicted on Figure 3.3, the architecture of DMIPA is composed mainly by two special entities: the MN and the DMAR. The MN is in charge to collaborate in the maintenance of active sessions when it moves across different networks. For instance, if the MN is attached to an AR which does not support mobility functions, it has to use the set of current DMARs that are allocated on its database to establish tunnels with them. On the other hand, if the MN is linked to a DMAR in the current network domain, the DMAR is responsible for tunnelling the data packets and address translation to maintain global IPv6 mobility.

Regarding the scenario presented in Figure 3.3 and following the steps on Figure 3.4, it is explained the protocol operation.

The detailed explanation of the protocol operation is given considering the movement of the MN from DMAR1 to AR, and then to DMAR2 regarding Figure 3.3. Furthermore, it is matching with Figure 3.4 which illustrates the messages exchange along the MN's movement.

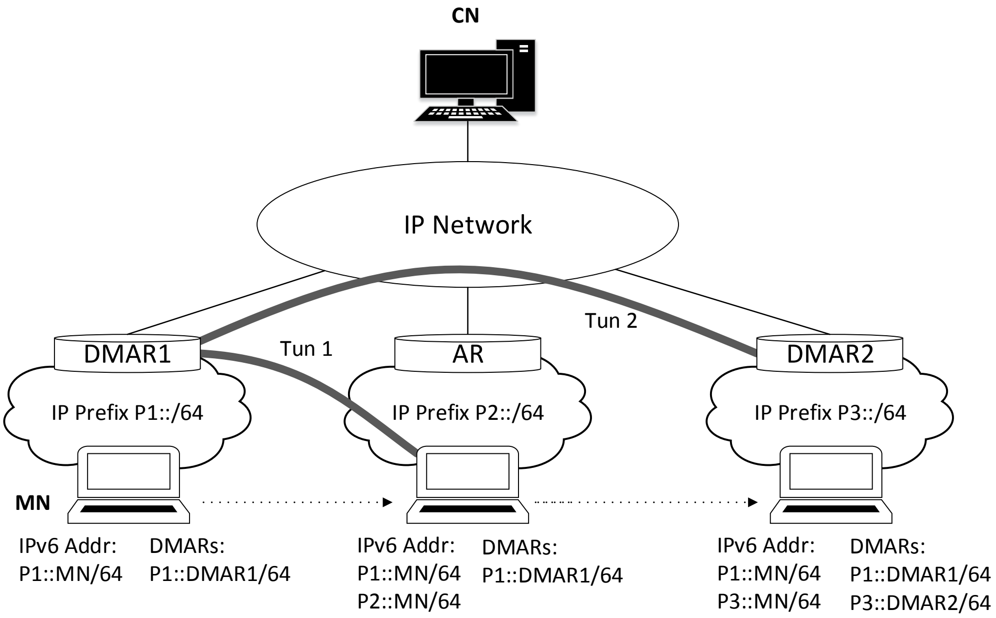

Figure 3.3: DMIPA Architecture Overview.

The BU and BA messages have the functions of updating the binding caches of DMARs and to create bi-directional tunnels between two DMARs or between a DMAR and a MN. The RS and RA messages have the same purpose as described earlier. However, DMIPA introduces a Mobility Support Flag (MSF) in the Reserved field of the RA message in order to provide useful information about if it is a DMAR or an AR. If the MSF flag is set to zero, then it is a legacy AR; otherwise MSF is equal to one indicating that it is a DMAR. Moreover, it is added two messages that are exchanged when MN and current DMAR communicate with each other: Anchor Set Update (ASU) and Anchor Set Acknowledgement (ASA). The MN sends the ASU message providing its attached DMAR with the IPv6 addresses of the current set of DMARs. The ASA is sent by the DMAR as a reply to the ASU message. This message indicates the success of the process.

DMIPA works as follows:

1) **DMAR1**: the MN attaches to DMAR1.

2) **RS/RA**: initially MN requests the network prefix by sending a RS message. Then, DMAR1 replies with a RA message which contains the network prefix P1::/64 and a true MSF value.

3) **Configure P1::MN/64**: after receiving the RA, the MN configures the IPv6 address P1::MN/64 as a preferred address.

4) **Add P1::DMAR1/64**: MN adds the IPv6 address of DMAR1 to the database that contains the available DMARs set.

5) **Session 1**: MN initiates data session 1 using P1::MN/64 as IPv6 source address.

6) **AR**: the MN attaches to a legacy AR.

7) **RS/RA**: the MN sends RS message and receives RA with the network prefix P2::/64 and a negative value of MSF.

8) **Configure P2::MN/64**: MN configures the P2::MN/64 address; however, the P1::MN/64 IPv6 address is kept as the preferred address.

9) **BU/BA to DMAR1**: DMAR1 receives BU from MN to establish a tunnel (Tun1), and then DMAR1 sends BA to confirm the success.

10) **Data session 1**: it is maintained active and the traffic flow from/to P1:MN/64 is tunnelled from/to P2::MN/64.

11) **Data session 2**: it is started a new session using the P1::MN/64 IPv6 address in order to provide session continuity if the MN changes its point-of-attachment. Therefore, data session 2 is tunnelled from the beginning.

12) **DMAR2**: the MN attaches to DMAR2.

13) **RS/RA**: to obtain the network prefix, the MN sends a RS to DMAR2 which replies with a RA message with the IPv6 prefix P3::/64 and a true MSF value.

14) **Configure P3::MN/64**: MN performs the configuration of the IPv6 address P3::MN/64 as the preferred IPv6 address.

15) **Add P3::DMAR2/64**: The MN adds the IPv6 Address of DMAR2 to the set of available DMARs IPv6 address list.

16) **ASU/ASA**: MN sends an ASU message to DMAR2 with DMAR1 IPv6 address information (P1:DMAR1/64) and with the respective MN IPv6 address (P1::MN/64). DMAR2 sends an ASA message to the MN to confirm the success.

17) **BU/BA**: DMAR2 sends BU message to DMAR1 to establish a tunnel. DMAR1 replies with BA message and it is created a tunnel (Tun2) between those DMARs.

18) **Data session 1 / Data session 2**: Both sessions are maintained through a tunnel between DMAR1 and DMAR2

If, for instance, the MN starts a new session (Session 3), when it is attached to DMAR2, the Session 3 follows a direct path without any mobility support.

Next, it will be compare the existent network simulators and the current vehicular mobility simulators. It will be chosen the best simulator for each category mentioned before.

3.3 Available Network Simulators

Before introducing the use-case scenarios to be used in the simulators to measure the performance of each IP mobility protocol in distributed and dynamic vehicular environments, it is given a comparison between the existent network simulators. The study of VANETs and the above mobility support protocols require efficient and accurate simulation tools. As the mobility of vehicles and driver behaviour can be affected by network messages, these tools must integrate a high quality network simulator. In this way, it is chosen the most suitable network simulator to achieve the objectives of the work.

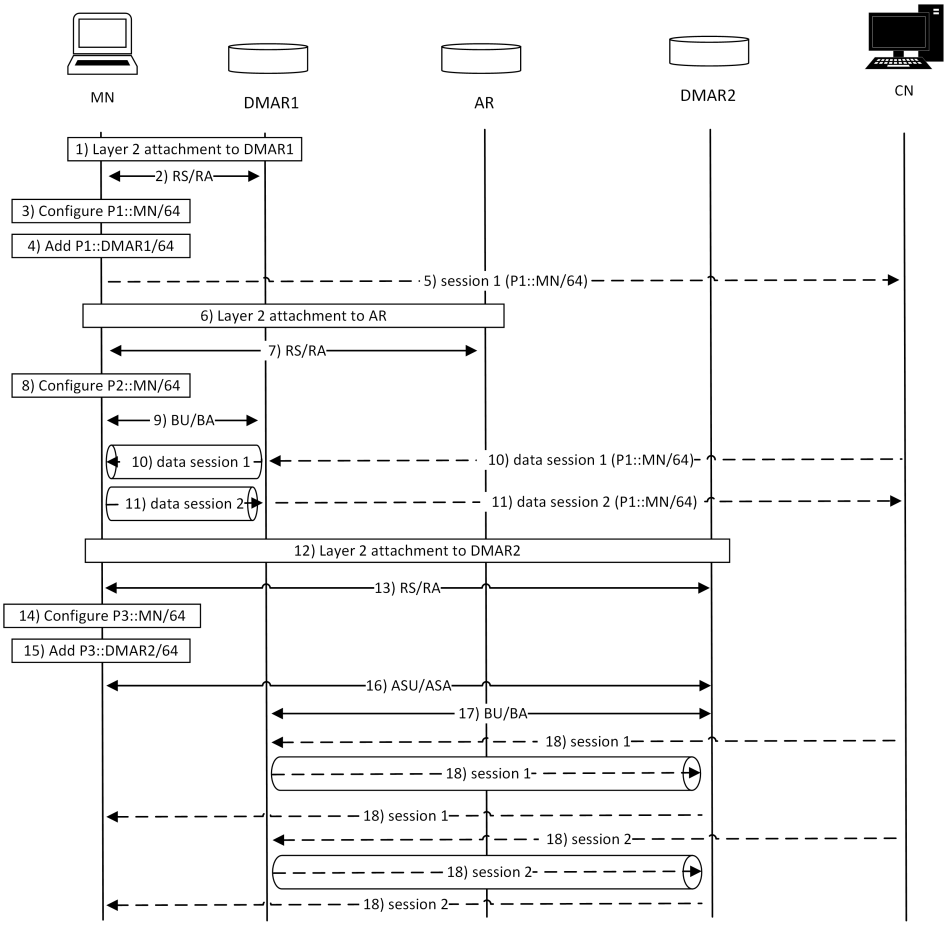

Figure 3.4: DMIPA Operational Mode and Exchanged Messages.

- **Global Mobile Information System Simulator (GloMoSim)** [39] is a scalable network simulator for wireless and wired network systems. It was built using a similar Open Systems Interconnection (OSI) seven layer network architecture under the discrete-event simulatior of Parsec.

- **Network Simulator 2 (NS-2)** [40] is an open-source discrete-event simulator designed particularly for research in computer communication networks. It has been under constant investigation and enhancement of several networks components such as routing, transport layer protocol, application, it has triggered the interest from industry, academia and government.

- **QualNet Communications Simulation Platform (QuelNet)** [41] is a communication simulation platform in which the user can evaluate the basic behaviour of a network and test combinations of network features to work in a real communication network environment. It is composed by five complementary components: QualNet Architect, QualNet Analyser, QualNet Packet Tracer, QualNet File Editor and QualNet Command Live Interface. This network simulator enables users to design new protocol models, optimize new and existing models, analyse the performance of networks and design large wired or/and wireless networks using pre-configured models. Some of the key features of QualNet are the speed of creating virtual network environment, scalability, portability and extensibility.

- **OPNET Modeler Suite Network Simulator (OPNET)** [42] is a software that provides performance analysis for computer networks and applications. It enables the users to analyse realistic simulated networks to compare the impact of different technology designs on end-to-end behaviour.

- **Network Simulator 3 (NS-3)** [43] is a network simulator that codifies the behaviour of a complex system as an ordered sequence of well-defined events. Therefore, it is suitable for research and educational use. The NS-3 simulation core supports research on both IP and non-IP based networks, and provides a variety of static or dynamic routing protocols such as Optimized Link State Routing (OLSR) and Ad Hoc On Demand Distance Vector (AODV) for IP-based applications. NS-3 is a solid simulator that is well documented, easy to use and debug.

Based on the most advantageous characteristics of each network simulators and regarding the main goals of this framework, it was decided to use NS-3 as the main network simulator tool. Some of its key features are: scalable and modular simulator, fast execution time and, since the modern hardware has strong capabilities, the compilation time is reduced. Documentation support is available, it is easy to integrate frameworks from other simulators and because NS-3 is implemented in C++, the memory management functions are available, improving data allocation.

3.4 Available Vehicular Mobility Simulators

The vehicular simulators are used to generate realistic mobility traces of vehicular traffic. The output trace files would then be fed into well-known network simulators such as NS-3, which was described on the above section to measure network performance.

There is a set of traffic simulators, each one with its own features and advantages:

- **CORSIM** [44] is a microscopic traffic simulator for signal systems, highway systems, and freeway systems. It models the movements of individual vehicles, including the influence of geometric conditions, control conditions and driver behaviour.

- **VanetMobiSim** [45] is an agent-based microscopic and macroscopic vehicular traffic simulator. It generates realistic vehicular movement traces for telecommunication networks simulators.

- **SUMO** [46] is an open source platform and highly portable for microscopic and continuous road traffic simulation. It was designed to handle large road networks.

- **VISSIM** [47] is a software solution for microscopic simulation tool and for modelling multimodal traffic flows. It provides ideal conditions for testing distinct traffic scenarios in a realistic manner.

SUMO was chosen to generate realistic mobility trace files, since it includes all the tools required to perform traffic simulation. It provides a realistic simulation regarding speed, priorities and car following model, easy to configure and to integrate in NS-3.

3.5 Network Topology implemented in NS-3

The remainder of this section is focused on documenting some models and supporting capabilities of NS-3 used on this work.

NS-3 is a powerful network simulator tool in which the models and the simulation core are implemented in C++. C++ is a high-level programming language similar to C, allowing the programmer to create objects within the code.

Particularly, the NS-3 was built as a library, therefore it can be statically or dynamically linked to a C++ main program that defines the simulation topology and initiates the simulator. In this main program it is coded the network topology illustrated in Figure 3.10. Therefore, it is necessary to create the required nodes by making use of the **NodeContainer** class which keeps track of a set of node pointers. Since the nodes have to be connected through a physical link, the **PointToPointHelper** class builds a set of **PointToPointNetDevice** objects which enables to create a basic point-to-point data link between two nodes or endpoints. The characteristics of each point-to-point data link, such as data rate and channel delay, are configured by the use of **SetChannelAttribute** function. The wireless communications have to be also configured. The **YansWifiPhyHelper** class provides a set of functions to set up the parameters in the wireless medium. According to the limits of the technologies used in vehicular networks and having in mind the real conditions of the surrounding environment, it is assigned the proper values for both starting and ending transmission power, transmission and reception gain, energy detection threshold and reception noise. For the propagation loss and propagation delay it is used the Two Ray Ground Propagation Loss Model and Constant Speed Propagation Delay Model, respectively. The **WifiHelper** helps to create **WifiNetDevice** objects and to configure the MAC address of Access Points (APs), MNs Wi-Fi interfaces and other attributes during the creation.

For a total coverage area in the larger highway traffic scenario or in a large city traffic scenario, in which flow, density and velocity are different, may require a group of access points with overlapping coverage. Thus, the APs are strategically placed in specific points; to archive this requirement the **MobilityHelper** class is used as helper class to assign positions to APs. In case of MNs (vehicles), the mobility scheme is defined by a SUMO trace file which can be inserted on the main program by making use of **Ns2MobilityHelper** class. As mentioned previously, the intention is to evaluate and compare two IP mobility protocols, which means that nodes need to communicate through the IP protocol. By default, IPv6 is disabled; therefore it is important to install the IPv6 stack into all nodes, as well as to configure the network prefixes and routing tables where it is stored the routing information to particular network destination. To accomplish these tasks efficiently, **InternetStackHelper**, **Ipv6AddressHelper** and **Ipv6StaticRoutingHelper** were used. At this moment the nodes are IPv6-capable and they are able to communicate taking advantages of IPv6 protocol and static routing information.

The *Router Advertisement Daemon (radvd)* application that implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbour Discovery Protocol (NDP) is installed in every AR. To compare MIPv6 and DMIPA, some of APs should have IP mobility management functions, so the **DMARHelper** application provides to APs a set of functions which enables them to exchange ASU/ASA and BU/BA, to tunnel data packets and to announce the MSF flag. The MNs are also responsible to collaborate in maintaining the active sessions, consequently the **MobileNodeHelper** application is responsible to provide the proper functions which includes the tunnel method, exchange ASU/ASA and

BU/BA, store the IPv6 addresses of its set of DMARs, and its own IPv6 addresses to keep sessions active.

In order to provide communication among the MNs and CNs, it is installed UDP Applications and Stream Video Application. For that purpose, it is used **UdpEchoServerHelper** class in specific CNs and **UdpEchoClientHelper** class in MNs for UDP Echo Application, while it is used **UdpServerDeviceHelper** class in particular CNs and **UdpClientDeviceHelper** in MNs for the Stream Video Application. It can be configured some attributes such as Maximum Packets Count, Packet Interval and Packet Size.

Finally, the NS-3 simulations use a fixed seed by default. It is required some randomness in the simulations to obtain different results and consequently to compute the mean of those results to achieve more accurate values. Then, to obtain randomness across multiple simulations runs, it is set the seed differently in each simulation by using the **SetSeed** function of the **SeedManager** class. This step must take place in the beginning of the main program, and also the **SetRun** function to set a run number with the same seed.

3.6 SUMO

This section shows three mobility scenarios created on SUMO, that are converted into SUMO trace files by making use of **traceExporter** tool to be inserted on the main program developed in NS-3.

The first scenario, called Short Highway, consists of a simple road containing two lanes, in which the vehicles move only in one direction. The objective is to create a short highway to simulate simple cases before using a more complex scenario. Figure 3.5 shows this scenario.

Figure 3.5: Short Highway.

The second scenario, called Long Highway, consists of several nodes connected by edges containing two lanes. The objective is to create a long highway road which is similar to the reality. The road network is illustrated in Figure 3.6.

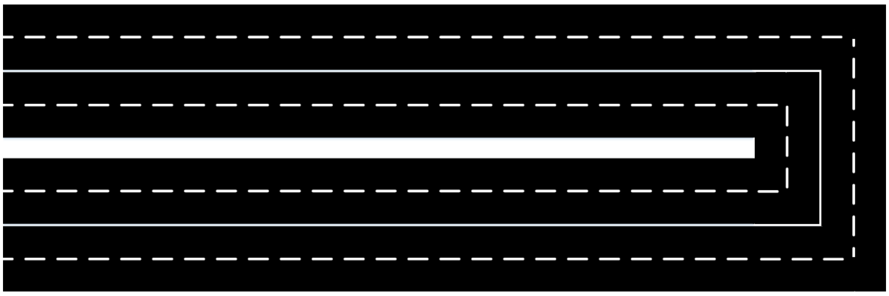

Figure 3.6: Long Highway.

For the purpose of providing a vehicular mobility model based on real traffic environment, it is used a **randomTrips** Python program that generates a set of random trips for the given network. The resulting trips are stored in an output file which is suitable for **DUAROUTER** command. As the last step, it is used the **sumo** command and **java** program to create the trace file.

The third scenario, called City, was developed in the same way as described before. The City scenario is illustrated in Figure 3.7 and consists in developing an area similar to a city by placing the nodes in such a way that, when connected, create city blocks. In addition, bus stops were inserted in specific places and it was used an additional step to create vehicles that behave like buses moving through a pre-determined route stopping in those locations. Figure 3.8 and Figure 3.9 illustrate in detail the City and represent a crossroad and a bus stop, respectively.

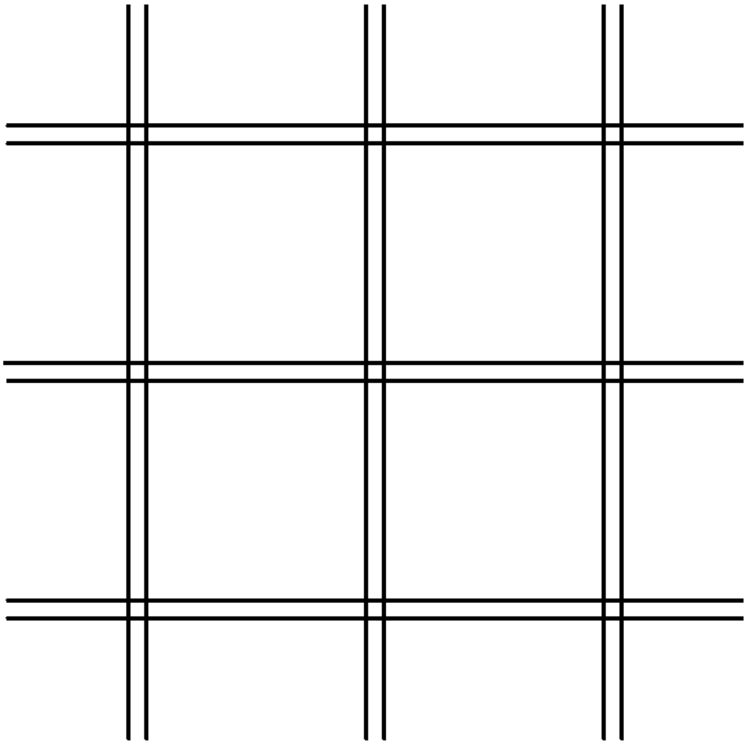

Figure 3.7: City.

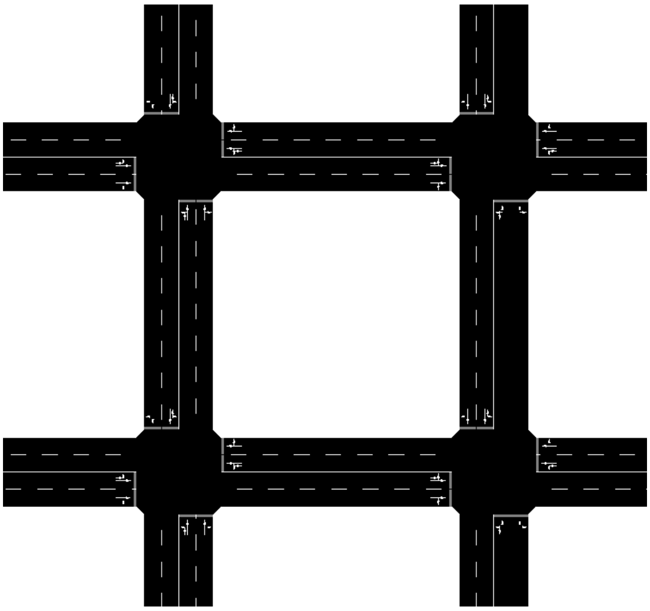

Figure 3.8: Crossroads Example.

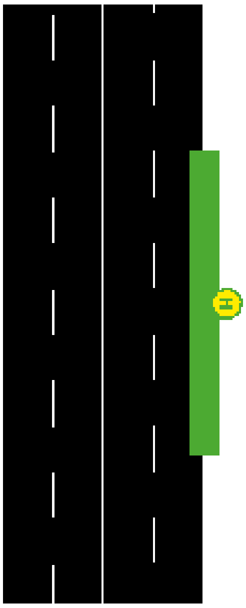

Figure 3.9: Bus Stop Example.

3.7 Network Topology and Deployed Scenarios

Figure 3.10 illustrates the network topology. The CN1, CN2, CN3 and CN4 are static correspondent nodes, which are able to communicate with the MNs through an UDP Echo or Stream Video Application. While CN1 and CN2 are linked to GW1 through a point-to-point data link with channel delay of 10 milliseconds, CN3 and CN4 are linked to GW2 through a 40 milliseconds delay poin-to-point data link which represents distant nodes. The HA is connected to GW1 through a point-to-point data link that has a delay of 2 milliseconds. The core router is a router that forwards data and control packets to other core nodes or edge nodes within the same network. All core routers are linked to its respective AR, and two of them are also linked to the gateways. The point-to-point data link that connects the gateways with the core routers, core router with ARs and the core router with other core routers, has a channel delay of 1 millisecond. All wired connections have a channel data rate of 100 Mbps capacity.

The wireless connections rely on the values of Transmission Power, Reception Power, Transmission Gain, Reception Gain and Energy Detection Threshold, but more important, they depend on both propagation loss and propagation delay models. Thus, the wireless communication channel was configured with the Two-Ray Ground Propagation Loss Model which combines the Friis model with ground reflections, and with the Constant Speed Propagation Delay Model, respectively. In addition, it is used the IEEE 802.11p as a physical standard for wireless communication. The communication range is approximately 450 meters in line of site.

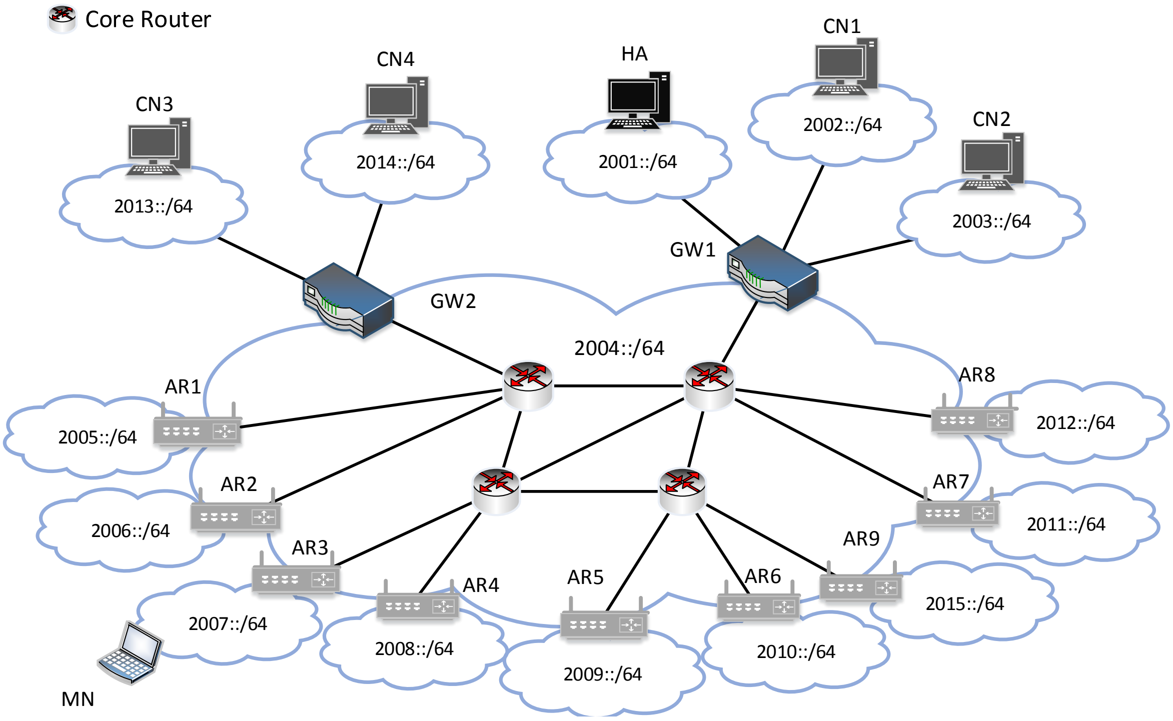

Figure 3.10: Example of the network deployed in NS-3.

Finally, the network is combined with three different scenarios created on SUMO (Short Highway, Long Highway and City) in such a way that ARs are strategically placed to provide a total coverage area. Therefore, the following figures illustrate the deployment scenarios where it can be seen that all the roads are inside the coverage area. Figure 3.11 illustrates the Short Highway scenarios, Figure 3.12 illustrates the Long Highway scenario and Figure 3.13 depicts the City scenario.

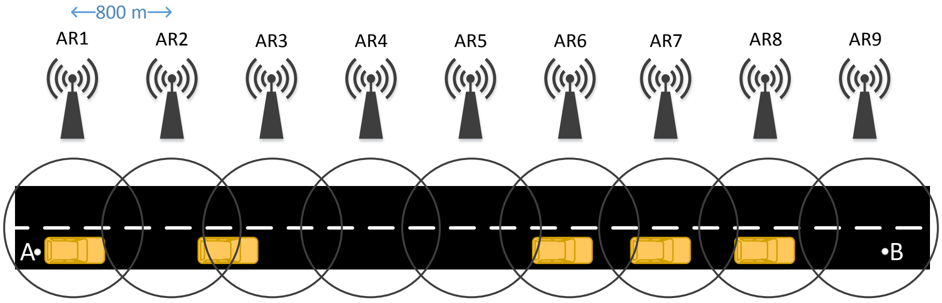

Figure 3.11: Deployment scenario - Short Highway.

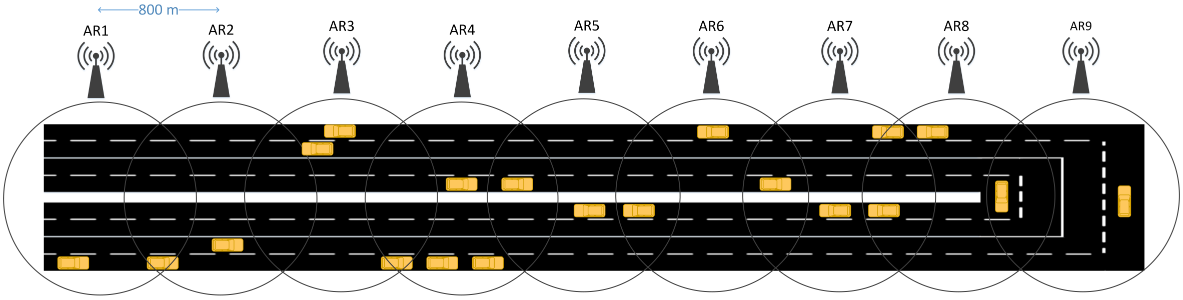

Figure 3.12: Deployment scenario - Long Highway.

The base DMIPA and MIPv6 protocols have been implemented in the framework of a PhD Thesis. This Dissertation addresses all steps required for its evaluation in vehicular scenarios. Next, it will be presented the results regarding these three scenarios and the two mobility management protocols in study.

3.8 Evaluation, Results and Analysis

The objective of this section is to analyse and compare the following results and take conclusions about the performance of MIPv6 and DMIPA in dynamic vehicular environment.

The purpose is to evaluate the signalling cost, data cost, data loss, average data delay, average session per MN instant, average number of IPs per MN and the binding update time. They are described as follows:

- **Signalling Cost**: the total cost required for mobility management signalling messages, defined as the size of the message ($S_{message}$), multiplied by the time spend by message in the network ($T_{network}$).

$$SignallingCost = S_{message} * T_{network}$$

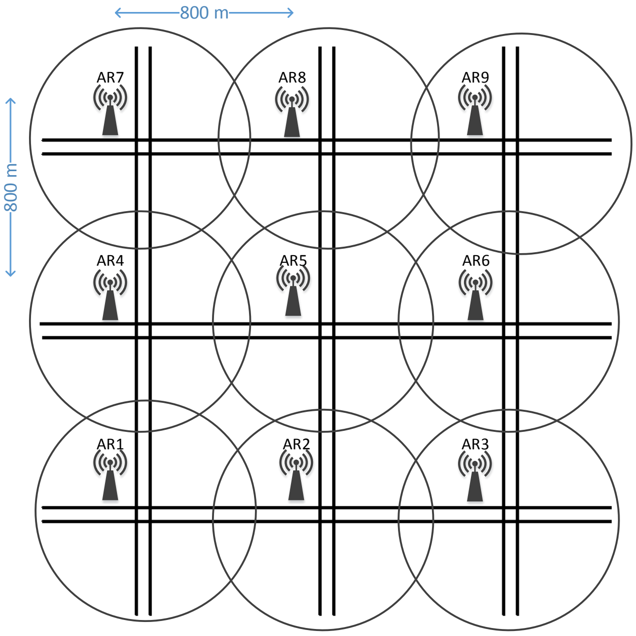

Figure 3.13: Deployment scenario - City.

- **Data Cost**: the end-to-end cost that is needed to deliver data messages from the CN to the MN, defined as the number of data messages received ($DataMessagesRcv$) multiplied by the message size and multiplied by the delay ($D_{message}$).

$$DataCost = DataMessagesRcv * S_{message} * D_{message}$$

- **Data Loss**: the percentage of data messages that are lost, defined as the total number of data messages sent ($DataMessagesSent$) subtracted to the total number of data messages received ($DataMessagesRcv$), divided by the total number of data messages sent and multiplied by 100.

$$DataLoss = \frac{DataMessagesSent - DataMessagesRcv}{DataMessagesSent} * 100$$

- **Average Data Delay**: the average end-to-end data messages delay time is computed as the one way delay (D_{OneWay}) divided by the session duration time ($T_{sessionDuration}$).

$$AvgDataDelay = \frac{D_{OneWay}}{T_{sessionDuration}}$$

- **Average Session per MN Instant**: the average number of sessions per mobile node in each instant, defined as the session duration time divided by the simulation time ($T_{simulation}$) divided by the total number of MNs (MN).

$$AvgSession = \frac{\frac{T_{sessionDuration}}{T_{simulation}}}{MN}$$

- **Average Number of IPs per MN**: the average number of IPs per mobile node is computed as the subtraction of the simulation time with the time that an IP address is available in the MN ($T_{IPavailableMN}$), multiplied by the number of IP addresses (IP) divided by the simulation time and divided by the total number of MN.

$$AvgNumIPs = \frac{(T_{simulation} - T_{IPavailableMN}) * IP}{\frac{T_{simulation}}{MN}}$$

- **Binding Update Time**: the average time to update the binding on the anchor point, computed as follows:

$$BUTime = \frac{(\frac{D_{BUDMAR}}{Rcv_{BUDMAR}} + \frac{D_{ASU}}{Rcv_{ASU}}) * A_{DMAR} + \frac{D_{BUMN}}{Rcv_{BUMN}} * A_{AR}}{A_{DMAR} + A_{AR}}$$

  Where the D_{BUDMAR} is the delay of the BU messages, the D_{ASU} is the delay of the ASU messages, the Rcv_{BUDMAR} and Rcv_{ASU} are the respective number of the BU and ASU received messages, the A_{DMAR} is the number of attached DMARs, the D_{BUMN} is the BU delay when MN is attached to an AR, the Rcv_{BUMN} is the number of its received messages and the A_{AR} is the number of attached ARs.

3.8.1 Evaluation of MIPv6 and DMIPA performance: Short Highway Scenario

The next results are related to the Short Highway scenario (Figure 3.11) in which five MNs start the movement in point A and end in point B. The speed changes in each simulations from 5 m/s up to 35 m/s. Moreover, The CN1 and CN3 initiate UDP Echo sessions, CN2 and CN4 initiate Stream Video sessions with the MNs. The sessions are randomly generated and they are characterized as follows:

- The inter-arrival time follows an exponential distribution with an average of 60 seconds.
- The sessions duration follow an exponential distribution with an average of 120 seconds.
- The packet interval for UDP Echo sessions follows an uniform distribution between 16 milliseconds and 128 milliseconds.
- The packet size for UDP Echo sessions follows an uniform distribution between 512 bytes and 1024 bytes.
- The packet rate for the Stream Video sessions is 256 Kbps.
- The packet size for the Stream Video sessions is 1024 bytes.

The AP2, AP4, AP6 and AP8 are access routers with mobility management functionalities, therefore they are considered DMARs.

The Figure 3.14 illustrates the signalling cost during this simulation.

The signalling cost of DMIPA is lower because the signalling messages spent less time in the network. In fact, the mobility management functionalities are distributed, therefore the management of the control plane is more closer to the end user which reduces the signalling cost.

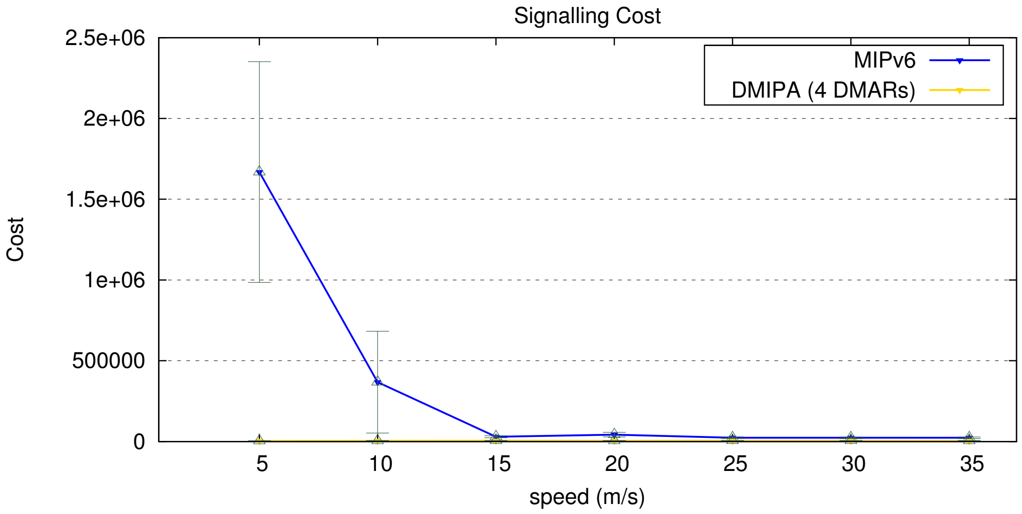

Figure 3.14: Signalling Cost in the Short Highway scenario.

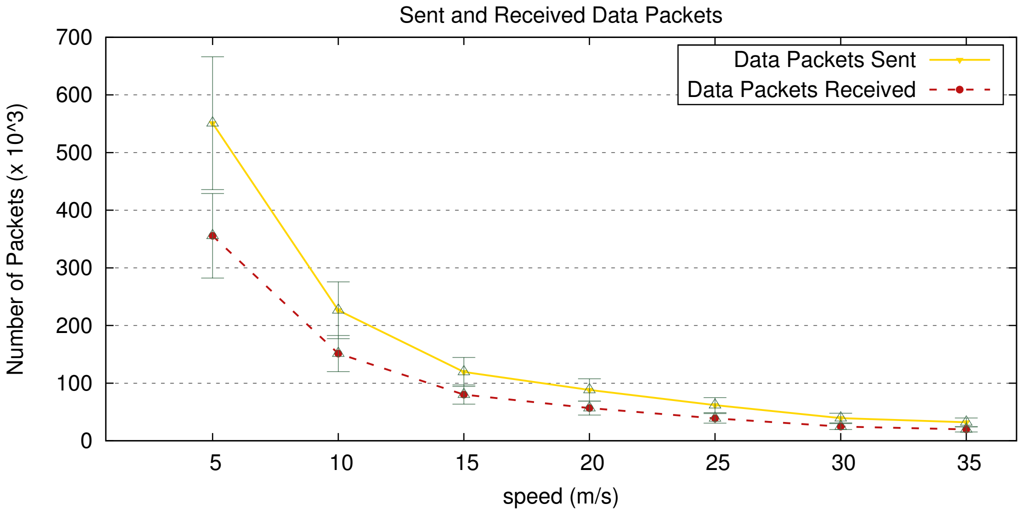

Figure 3.15: MIPv6 Data Packets in the Short Highway scenario.

The exchange of data messages are illustrated on Figure 3.15 and Figure 3.16. As the speed increases, the simulation time decreases and consequently the session time of each session decreases. Therefore, the MNs receive and send less data messages when the speed is high compared to the cases in which the speed is low. A comparison between the results illustrated in Figure 3.15 and Figure 3.16 demonstrates that it was sent/received less data messages when DMIPA was used, which is explained through a certain randomness of the data messages exchanged, even if the average number of sessions are similar between both simulations.

DMIPA protocol has lower values of data cost than MIPv6 (Figure 3.17). This can be justified by the fact that, messages received by the MNs and the values of data delay are lower for DMIPA than the values obtained for MIPv6. Furthermore, the result of data cost

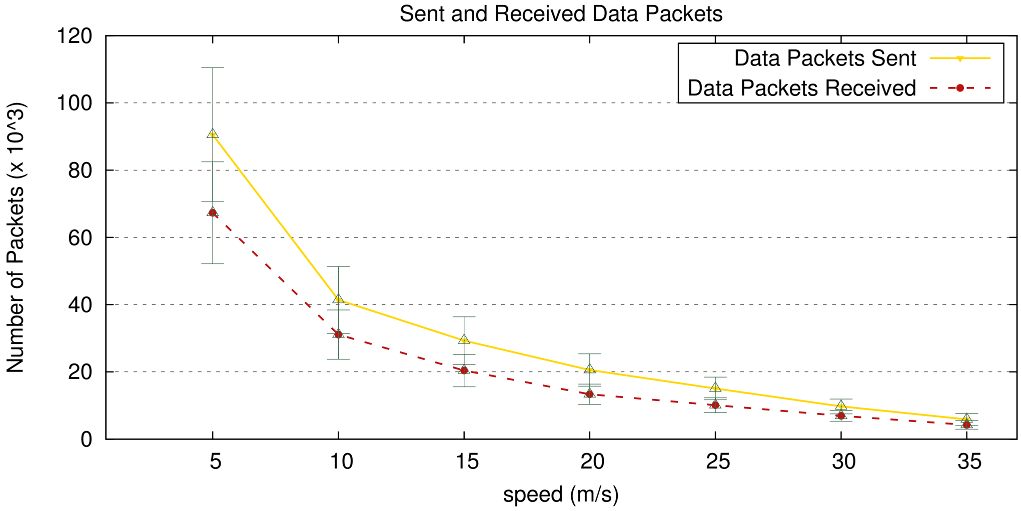

Figure 3.16: DMIPA (4 DMARs) Data Packets in the Short Highway scenario.

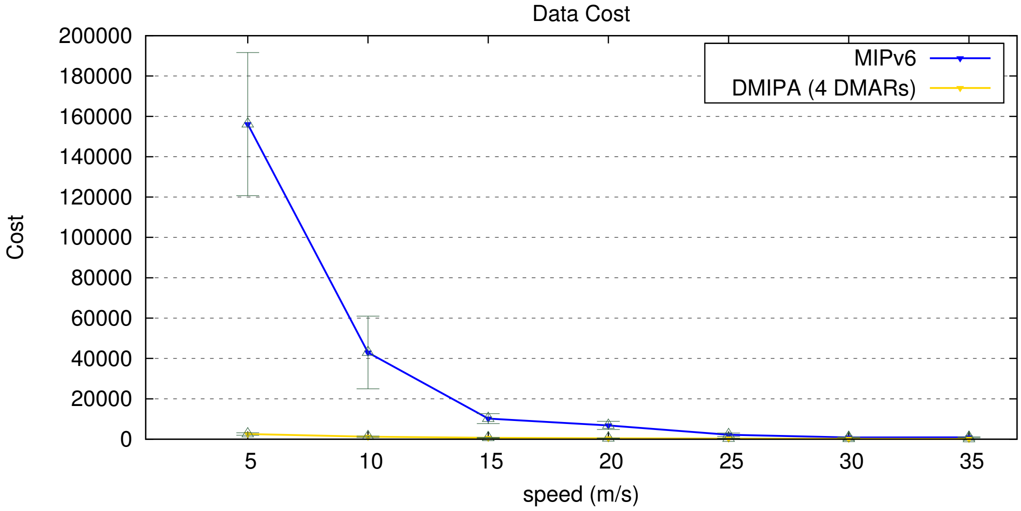

Figure 3.17: Data Cost in the Short Highway scenario.

for MIPv6 has a “c” sharp behaviour which are related with the average data delay in Figure 3.19. In the case of DMIPA, although the number of messages has been reduced while the speed increased, the data cost remained constant.

The data loss is depicted in Figure 3.18. In the same simulation conditions and evaluating data packet sent and received, it can be verified that MIPv6 has higher percentage values of data loss comparing with DMIPA. This is one of the consequences of distributing the mobility management functionalities. By allowing the access routers to manage the data plane, it is eliminated the centralized element, which is a single point of failure, congestion and bottlenecks; therefore, the values of data loss are improved.

It is interesting to observe that, for the speed value of 20 m/s, the data loss is similar to both cases. However, the two protocols have high values of data loss compared with the

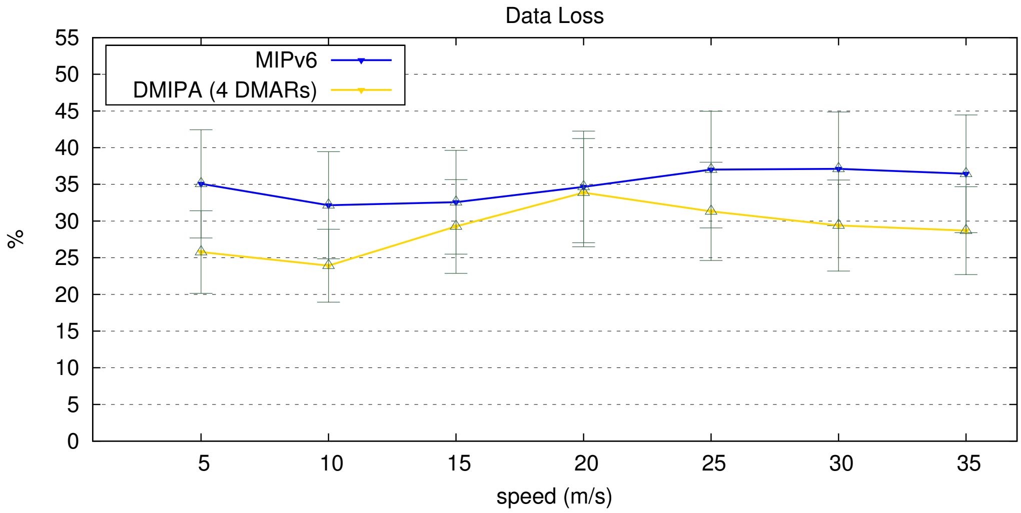

Figure 3.18: Data Loss in the Short Highway scenario.

expected ones. Therefore, next section will evaluate the causes of the high data packet loss.

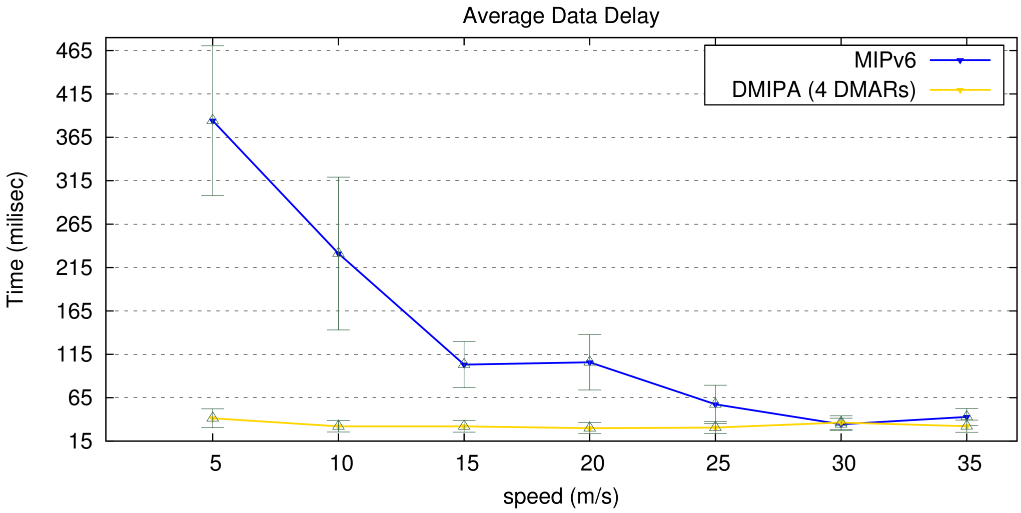

Figure 3.19: Average Data Delay in the Short Highway scenario.

According to the average data delay, Figure 3.19, DMIPA shows lower values than MIPv6. However, for 30 m/s and 35 m/s the results are similar. The reason why the results are similar is related to the high speed of the mobile nodes, which raises challenges to the mobility management. In this scenario, we concluded that, for high speeds, DMIPA does not improve the mobility management regarding average data delay.

As the speed value increases, the simulation time decreases and the average session per MN instant decreases along the graphic of Figure 3.20. The results of both mobility management protocols cannot be compared because the sessions are randomly initiated according to the arriving session time and session duration time, but give an idea of the behaviour during the simulation.

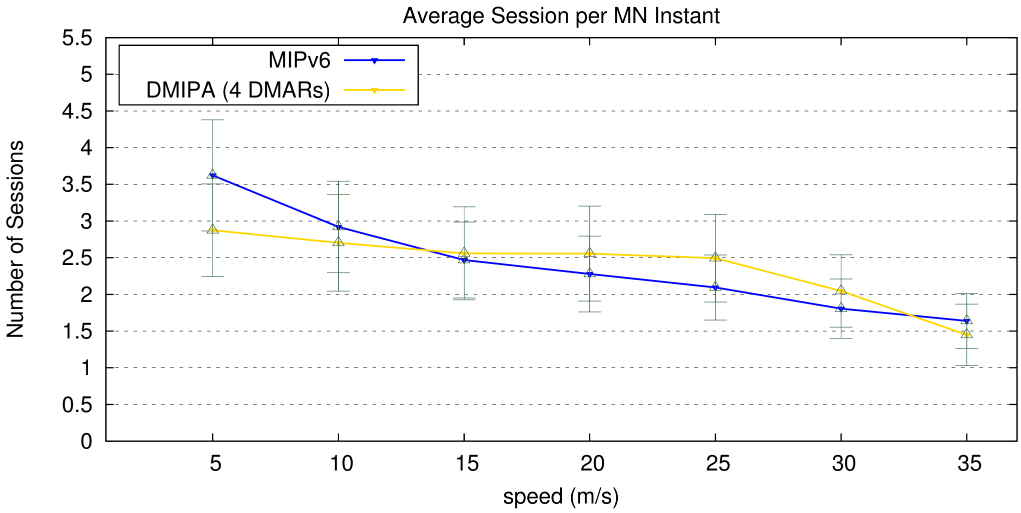

Figure 3.20: Average Sessions per MN in the Short Highway scenario.

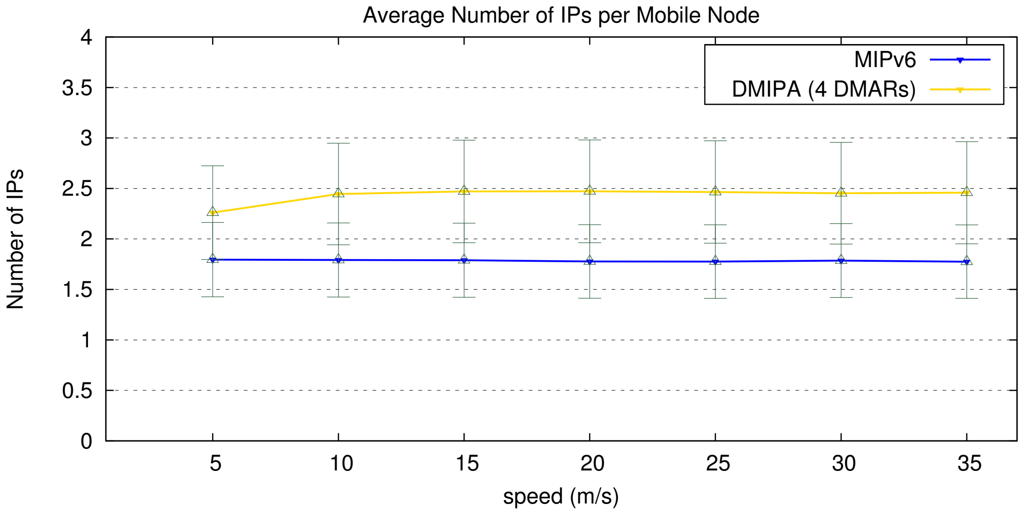

Figure 3.21: Average Number of IP per MN in the Short Highway scenario.

Figure 3.21 shows the average number of IPs per MN. The results demonstrate that DMIPA has to manage more IP addresses than MIPv6. According to the results of binding update time (Figure 3.22), MIPv6 has higher values for 5 m/s and 10 m/s when compared with DMIPA. For the speed of 5 m/s, MIPv6 shows more sessions in average than DMIPA; therefore, there are more messages exchanged in the wireless medium which introduces a delay in the signalling packets. Moreover, due to the existence of a centralized element, HA, that manages the signalling and data messages, it delays the process of updating the binding caches. Thus, the average mobility handover is higher for MIPv6 camparing to DMIPA. When the speed of MNs is 10 m/s, it is observed that the values of binding update time still high, but if we look at the range of variation, the lower values is closer to the value of the binding update time of DMIPA.

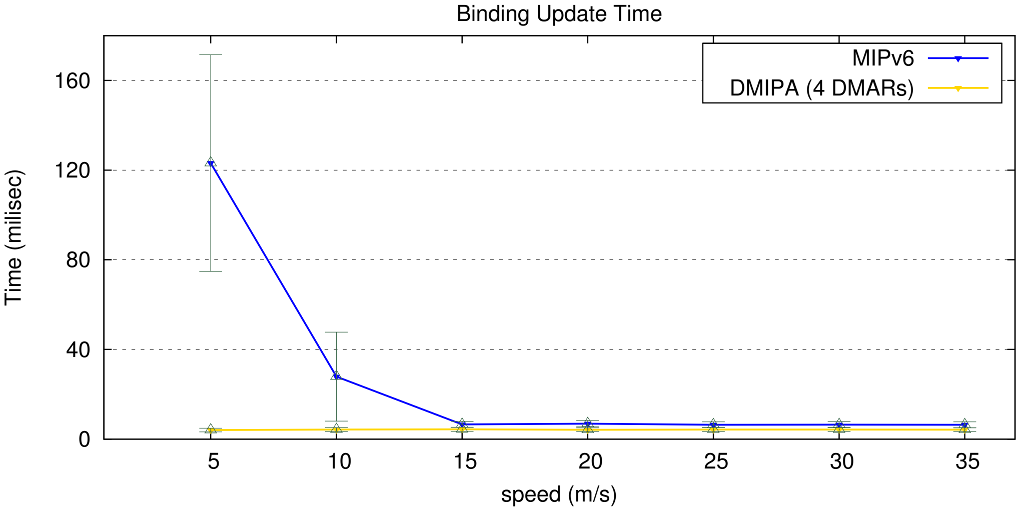

Figure 3.22: Binding Update Time in the Short Highway scenario.

Comparing both MIPv6 and DMIPA, and regarding the available results, it can be concluded that DMIPA has lower percentage of data loss than MIPv6. However, the value of data loss is higher than expected, but there is a considerable improvement in the average data delay. DMIPA has lower values of signalling cost, data cost and binding update time for slow speed.

3.8.2 Evaluation of the Data Packet Loss Cause

In order to understand if the data packet loss is due to the handover procedure or an overloading issue in the network, the same scenario was simulated using the same UDP Echo and Stream Video applications, but this time the packet rate was set to a lower value. The sessions parameters are defined as follows:

- The inter-arrival time follows an exponential distribution with an average of 60 seconds.
- The sessions duration follow an exponential distribution with an average of 120 seconds.
- The packet interval for UDP Echo sessions follows an uniform distribution between 128 milliseconds and 264 milliseconds.
- The packet size for UDP Echo sessions follows an uniform distribution between 512 bytes and 1024 bytes.
- The packet rate for the Stream Video sessions is 16 Kbps.
- The packet size for the Stream Video sessions is 1024 bytes.

The results are presented below.

Figure 3.23 shows the signalling cost. As a result of the high time spent by the signalling messages in the network, DMIPA has high values of signalling cost when compared with

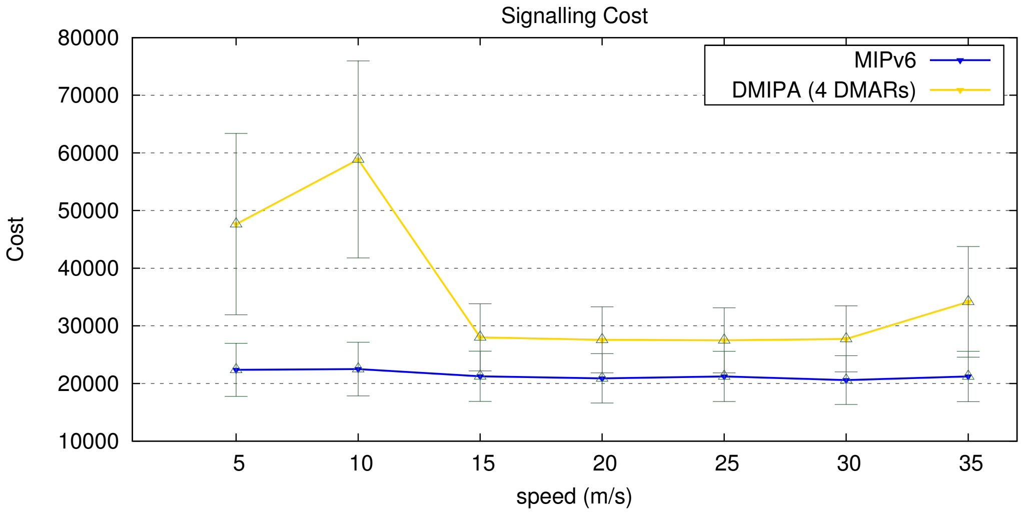

Figure 3.23: Signalling Cost in the Short Highway scenario (Applications with lower Packet Rate).

MIPv6. For speeds between 15 m/s and 30 m/s, the value of signalling cost for DMIPA is constant and lower than 30000. For the case of MIPv6, the signalling cost is constant around the 20000 cost value.

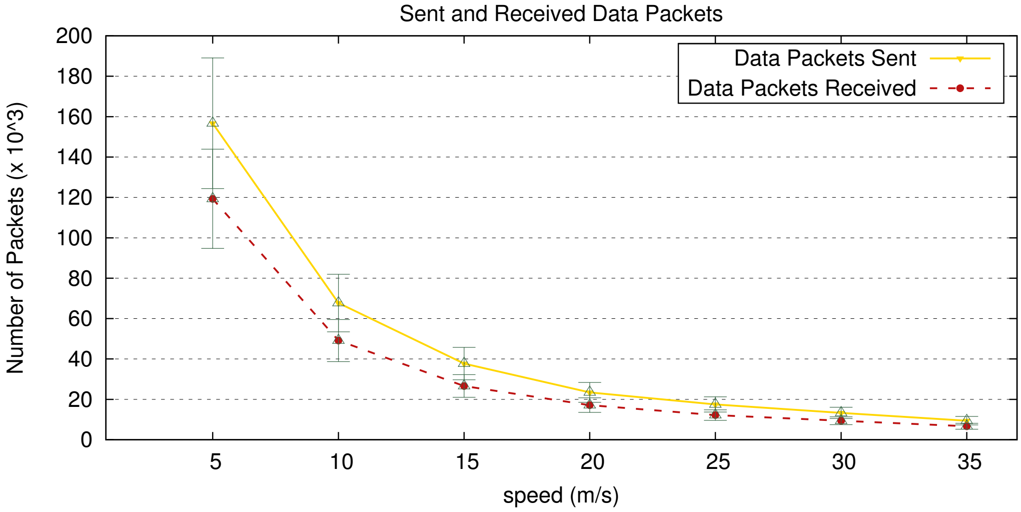

Figure 3.24: MIPv6 Data Messages in the Short Highway scenario (Applications with lower Packet Rate).

The Figures 3.24 and 3.25 show the exchange of data messages for MIPv6 and DMIPA, respectively. It is concluded that both results have identical values and the graphics have similar shape.

When we evaluate the data cost of Figure 3.26, it is concluded that the values of MIPv6 are slightly higher. Therefore, the number of data messages received, the size of the messages and the delay are similar for both cases.

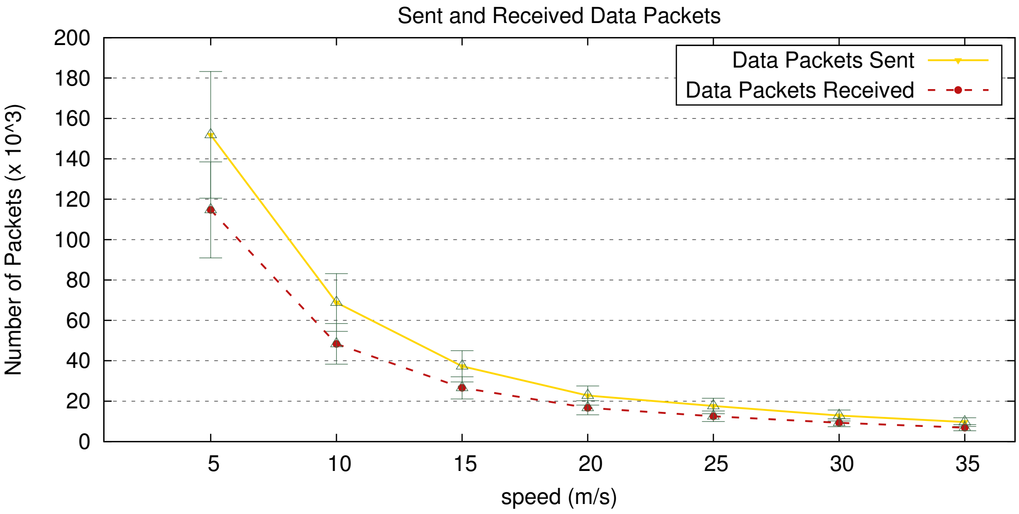

Figure 3.25: DMIPA (4 DMARs) Data Messages in the Short Highway scenario (Applications with lower Packet Rate).

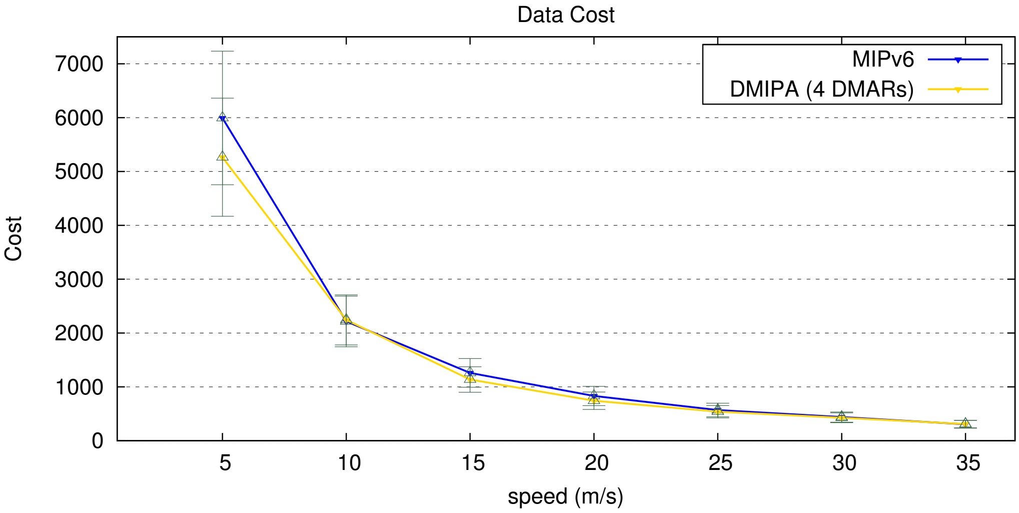

Figure 3.26: Data Cost in the Short Highway scenario (Applications with lower Packet Rate).

The data loss is illustrated in Figure 3.27. Analysing the data loss of both mobility management protocols, it is notorious the high values for the two cases even when the packet rate is lower compared with the case before.

The average data delay in Figure 3.28 is lower when DMIPA is used, and despite the fact of having high percentage of data loss, it is observed an improvement of the average delay.

As mentioned earlier, as the speed of MNs increase, the simulation time decreases as well as the average number of session per MN instant. The result is shown in Figure 3.29.

The average number of IPs per MN is according with the expectation. It is higher for DMIPA, using 4 DMARs, when compared with MIPv6 (Figure 3.30). When analysed the 5 m/s case, the average number of IPs for DMIPA is lower because MNs spend more time

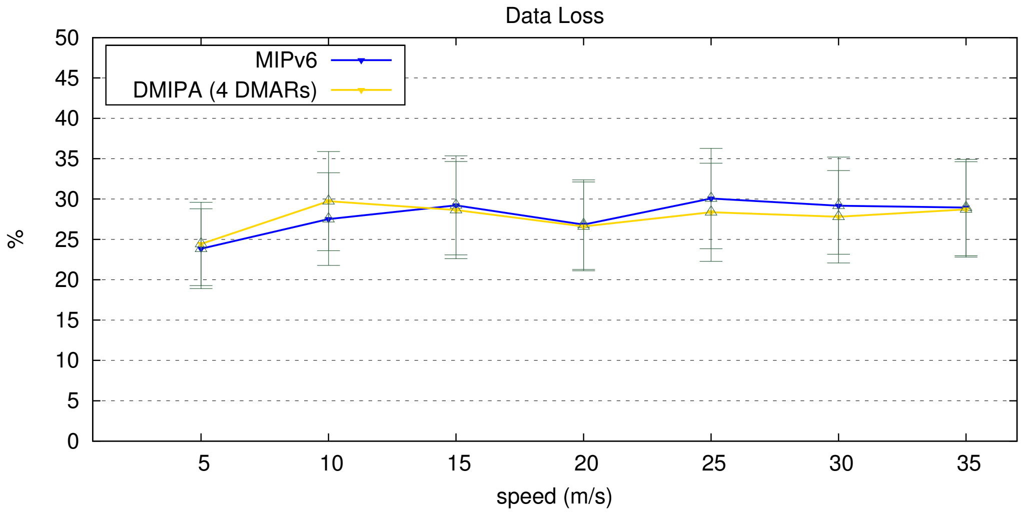

Figure 3.27: Data Loss in the Short Highway scenario (Applications with lower Packet Rate).

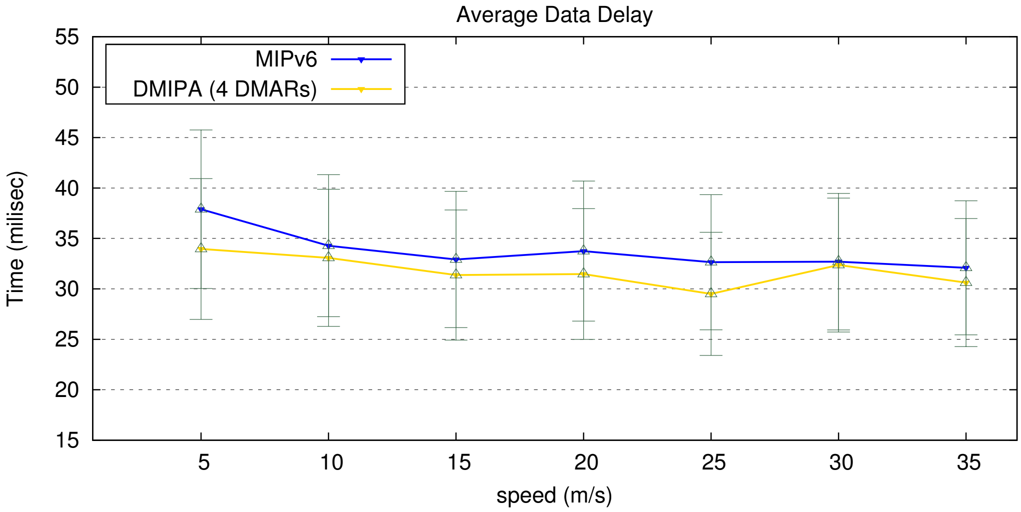

Figure 3.28: Data Delay in the Short Highway scenario (Applications with lower Packet Rate).

attached to the same DMARs.

Regarding Figure 3.31, it is visible an improvement of the binding update time value when comparing MIPv6 with DMIPA.

So, the results presented in this section, in which the packet rate is lower, show that DMIPA has significant improvements when compared with MIPv6. Although the values of data loss are still higher, it is notorious the decrease of the average data delay, binding update time and data cost values. Concluding, these results may suggest that a high percentage of data loss may be caused by the loss of packets during the handover procedure. When comparing Figure 3.18 with Figure 3.27, it can be observed that there is no significant decrease in the data loss values, even when the packet rate of each application was reduced.

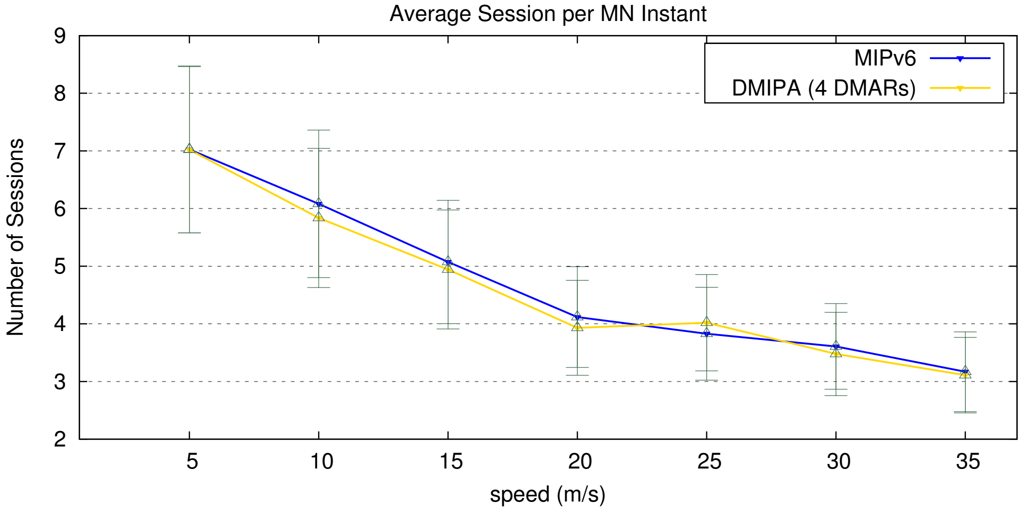

Figure 3.29: Average Sessions per MN in the Short Highway scenario (Applications with lower Packet Rate).

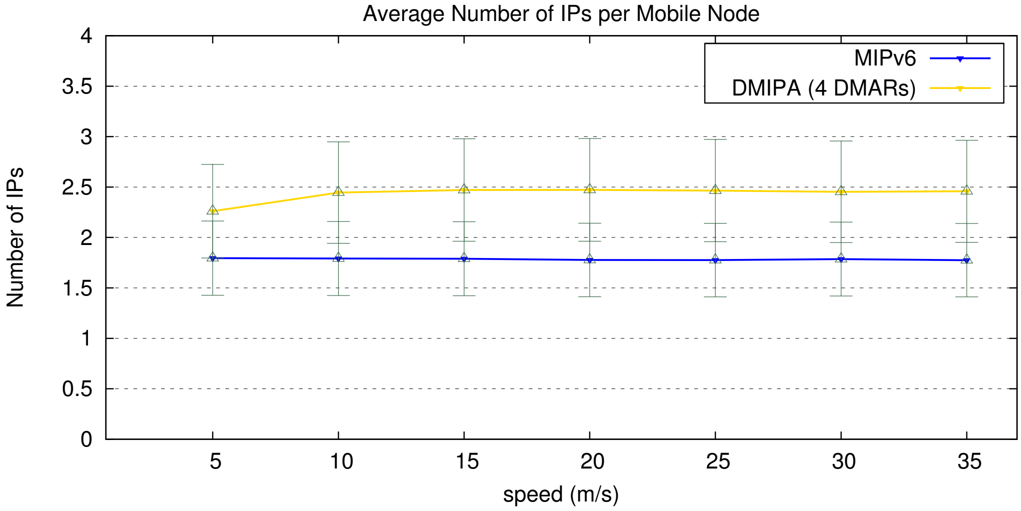

Figure 3.30: Average Number of IP per MN in the Short Highway scenario (Applications with lower Packet Rate).

3.8.3 Evaluation of Long Highway Scenario

The Long Highway scenario was used to perform other simulations. In this case, it was evaluated the influence of different numbers of DMARs according with the different number of MNs. The MN movements are modelled by a vehicular mobility scheme based on real traffic environment. Then, the simulation time was set to 200 seconds and the sessions were randomly generated from the following characteristics:

- The inter-arrival time follows an exponential distribution with an average of 40 seconds.
- The sessions duration follow an exponential distribution with an average of 60 seconds.

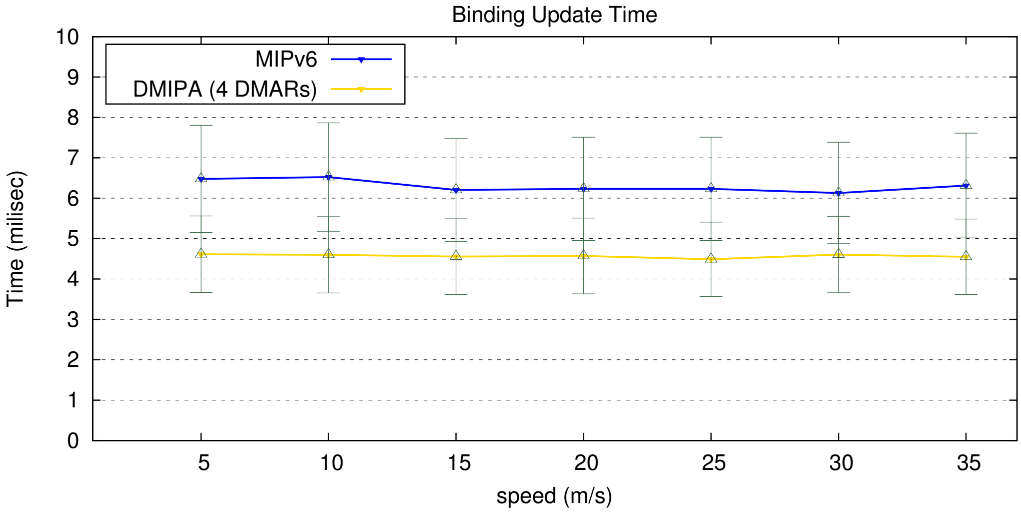

Figure 3.31: Binding Update Time in the Short Highway scenario (Applications with lower Packet Rate).

- The packet interval for UDP Echo sessions follows an uniform distribution between 16 milliseconds and 128 milliseconds.
- The packet size for UDP Echo sessions follows an uniform distribution between 512 bytes and 1024 bytes.
- The packet rate for the Stream Video sessions is 128 Kbps.
- The packet size for the Stream Video sessions is 1024 bytes.

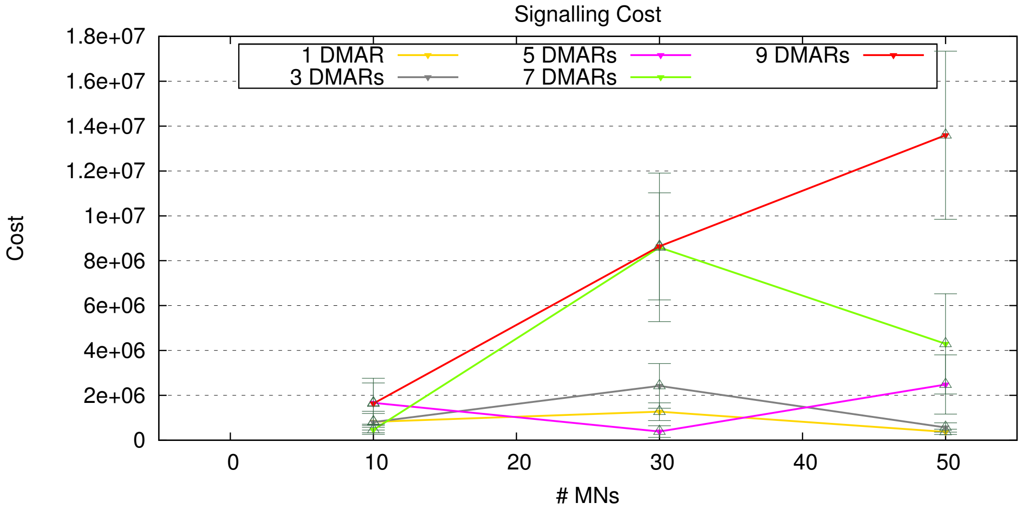

Figure 3.32: Signalling Cost in the Long Highway scenario.

The Figure 3.32 illustrates the results of signalling cost regarding the number of DMARs. It can be seen that,the value of signalling cost is higher for 9 DMARs. In general, as the number of MN increases, the signalling cost increases. This behaviour is related with the average number of sessions per MN which, for 9 DMARs, are constant and equal to 1.8, even when the number of MNs are higher. Therefore, the 9 DMARs case have to manage the old and new sessions of all MNs, exchanging more signalling messages than the other cases, because all the access routers have mobility management functions. The results are better for a lower number of DMARs.

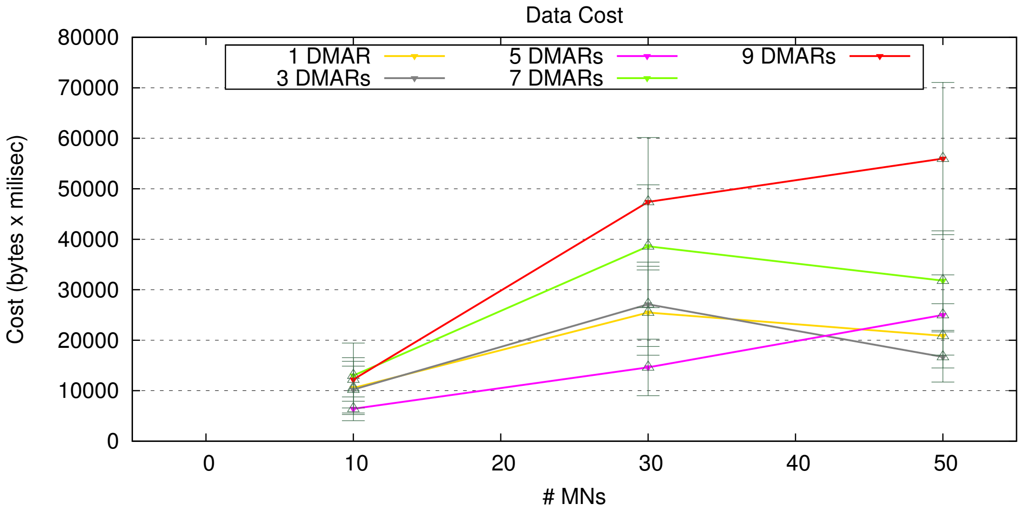

Figure 3.33: Data Cost in the Long Highway scenario.

Figure 3.33 illustrates the data cost for the simulations performed in the scenario of Figure 3.12. It can be concluded that the worst result corresponds to the case of have 9 DMARs. The main reason is the high delay value and the long session duration time. The protocol DMIPA has to manage the old and new sessions, therefore if a session has a long duration time, it has to be managed through different IP tunnels between DMARs that are far away from each other causing longer data delay. On the other hand, having 5 DMARs significantly reduces the data cost.

The case of have 5 DMARs in Figure 3.34 demonstrates that the value of data loss is lower comparing with the other cases. The second best result belongs to the 3 DMARs case, and the worst result corresponds to the case of use 9 DMARs. Indeed, having more access routers with mobility management functionalities implies more signalling in the network in order to maintain the active session through IP tunnels. Then, the time needed for the MN to receive a packet after changing its point-of-attachment is longer because the protocol has to deal with more IP tunnels and signalling messages.

When comparing the different cases and regarding the average data delay illustrated in Figure 3.35, it is observed that the values are very similar, but for the 5 DMARs case the values are still lower when the number of MNs are lower.

The average number os sessions per MN, in Figure 3.36, is constant for the 9 DMARs case. For other cases it is notorious a decrease of the average number of sessions per MN instant.

The Figure 3.37 shows the results according to the average number of IPs per MN. For lower number of MNs, the 5 DMARs case has the best result, contrasting with the case of 9 DMARs that has the worst values.

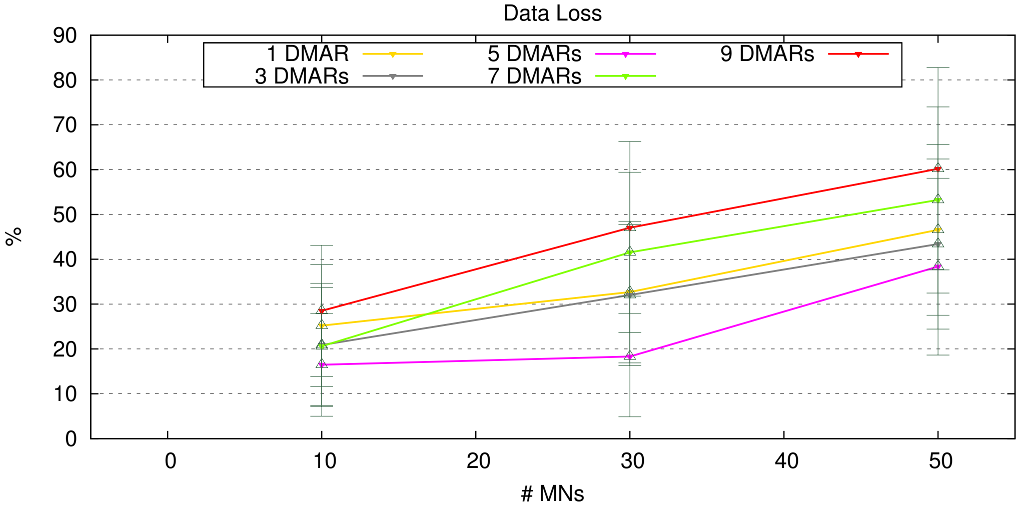

Figure 3.34: Data Loss in the Long Highway scenario.

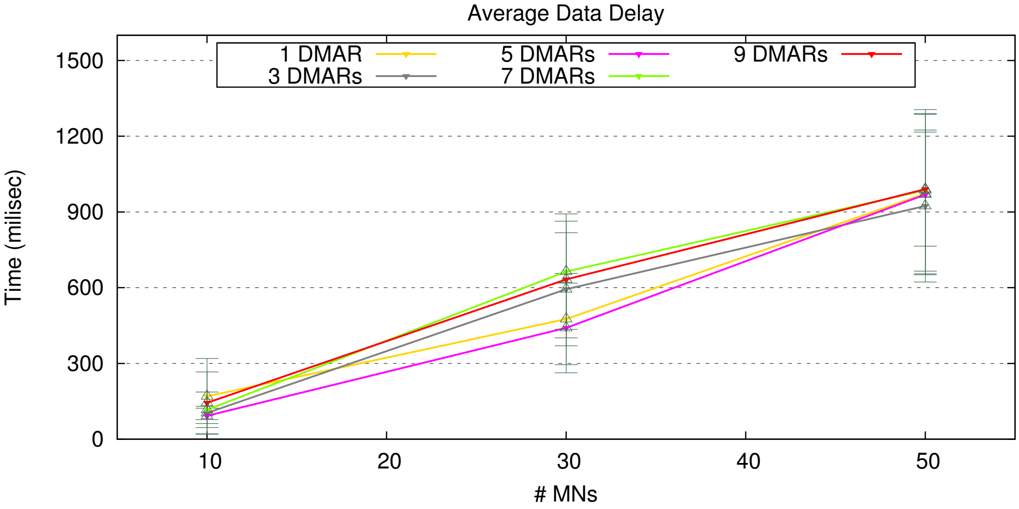

Figure 3.35: Average Data Delay in the Long Highway scenario.

According with Figure 3.38, the binding update time results, it can be verified that the lower values correspond to the case of use 3 and 5 DMARs.

So, regarding data cost, data loss, average data delay and average number of IPs per MN, it is concluded that the best result is achieved when 5 DMARs are used. In this case it may be considered that the use of one DMAR is similar to use the HA, and therefore, it may be assumed that the results for 1 DMAR are the same results for MIPv6. So, it can be compared, as example, the results of 1 DMAR with results of 5 DMARs. Concluding, if 5 DMARs are used, DMIPA has better performance than MIPv6.

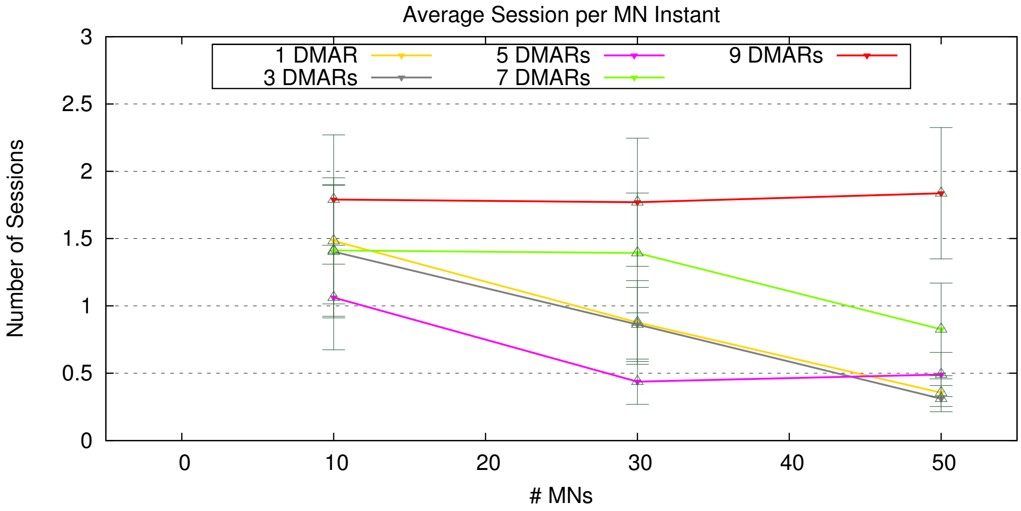

Figure 3.36: Average Session per MN in the Long Highway scenario.

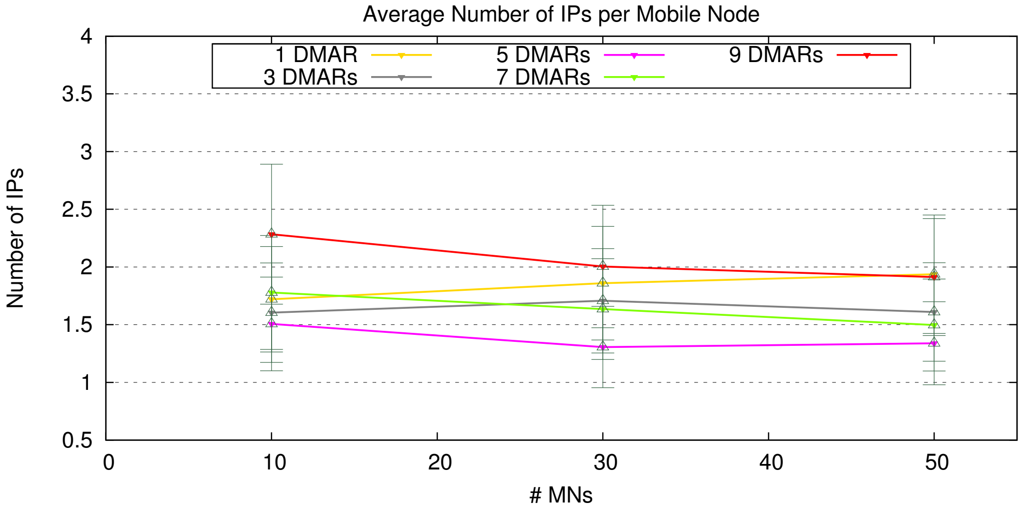

Figure 3.37: Average Number of IPs per MN in the Long Highway scenario.

3.8.4 Evaluation of DMIPA performance: City Scenario

The City scenario was used to perform simulations and evaluate the protocols in an environment which is similar to the today's cities. In this case, it was evaluate the influence of different number of DMARs according with different number of MNs. The MNs movements are modelled by a vehicular mobility scheme based on real traffic environment. Then, the simulation time was set to 500 seconds and the sessions are characterized as follows:

- The inter-arrival time follows an exponential distribution with an average of 60 seconds.
- The sessions duration follow an exponential distribution with an average of 120 seconds.
- The packet interval for UDP Echo sessions follows an uniform distribution between 16

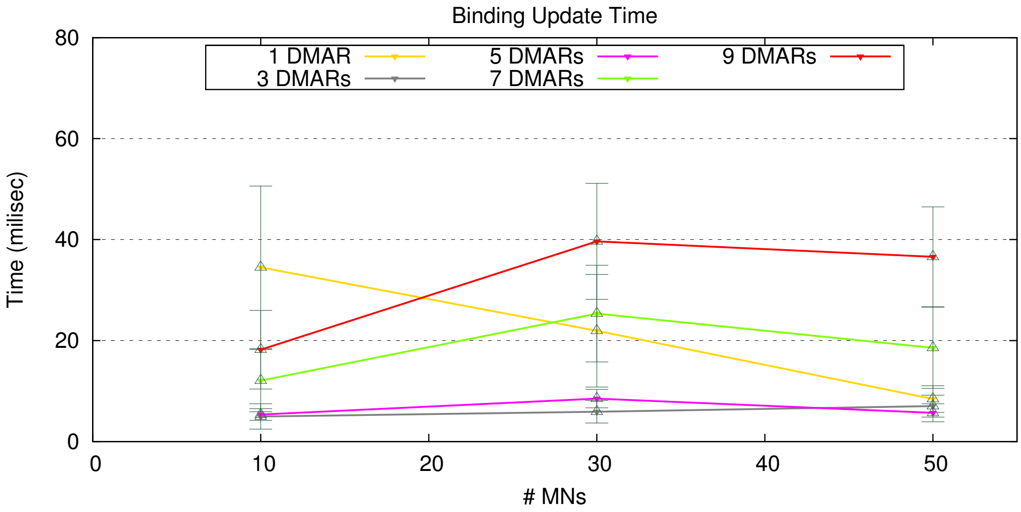

Figure 3.38: Binding Update Time in the Long Highway scenario.

milliseconds and 128 milliseconds.

- The packet size for UDP Echo sessions follows an uniform distribution between 512 bytes and 1024 bytes.
- The packet rate for the Stream Video sessions is 256 Kbps.
- The packet size for the Stream Video sessions is 1024 bytes.

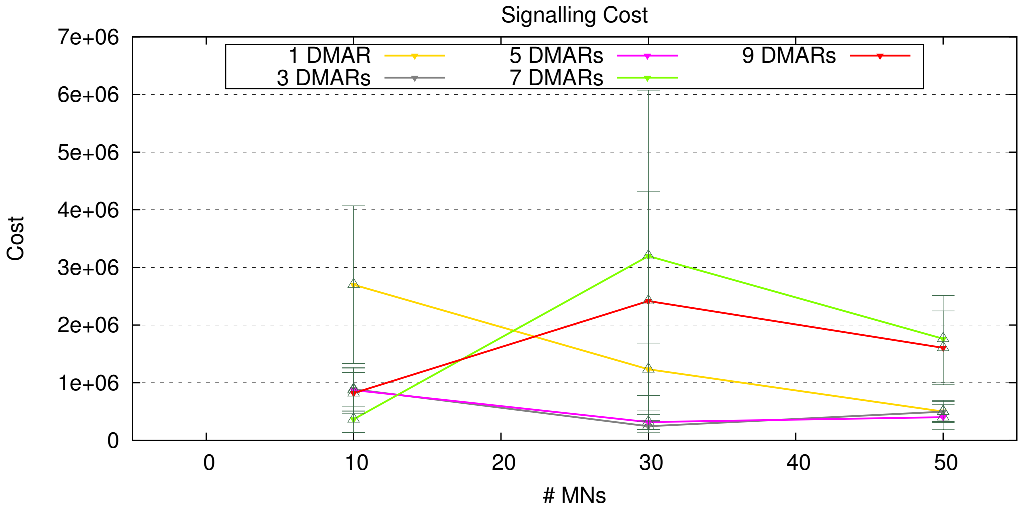

Figure 3.39: Signalling Cost in the City scenario.

The Figure 3.39 and Figure 3.40 show the signalling cost and data cost, respectively. In general, for 3 and 5 DMARs the values are lower, which means that in this scenario, in the same conditions, the best results are achieved when 3 and/or 5 DMARs are used.

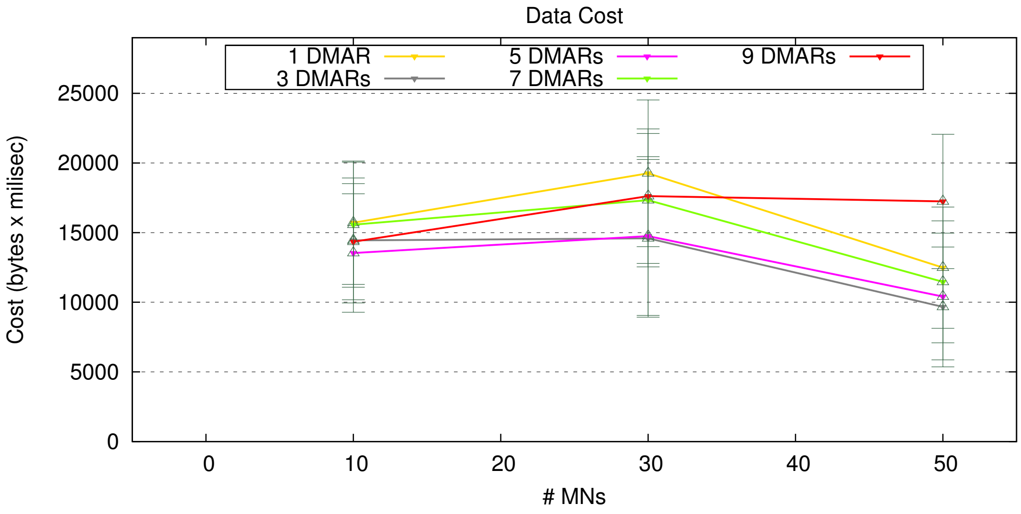

Figure 3.40: Data Cost in the City scenario.

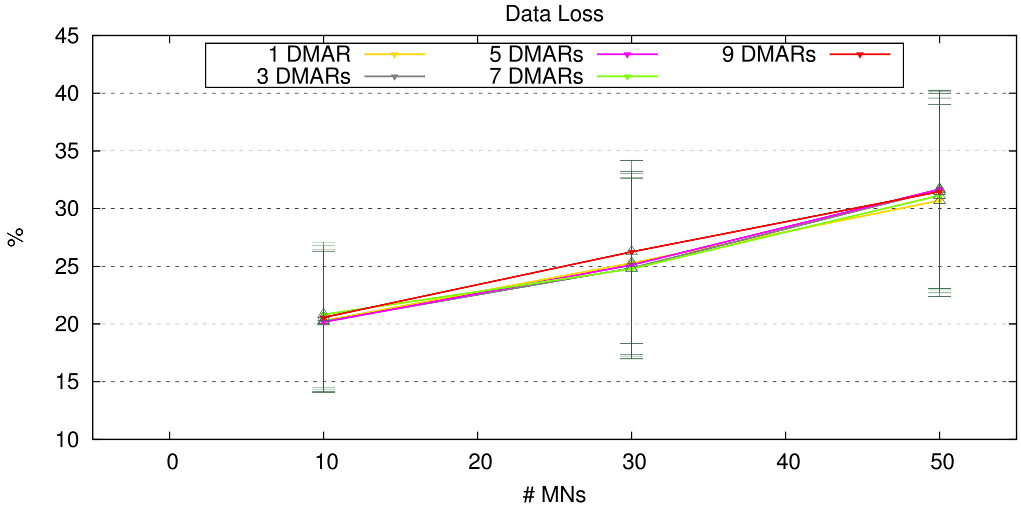

Figure 3.41: Data Loss in the City scenario.

The results of data loss are similar for all the cases, but it is visible slightly high values for the 9 DMARs case.

The Figure 3.42 illustrates the results of the average data delay. As the number of MNs increases, the value of the average data delay decreases. However, these values are lower when 3 and 5 DMARs are used instead of 9 DMARs.

The average number of sessions per MN stays constant for the 9 DMARs case, and decreases for the 1, 5 and 7 DMARs cases.

It is also visible a decrease of the average number of IPs per MN as the number of MN increases. Since the average number of IPs per MN is defined as the inverse of the number of MN, if the number of MNs increases, the average number of IPs per MN decreases.

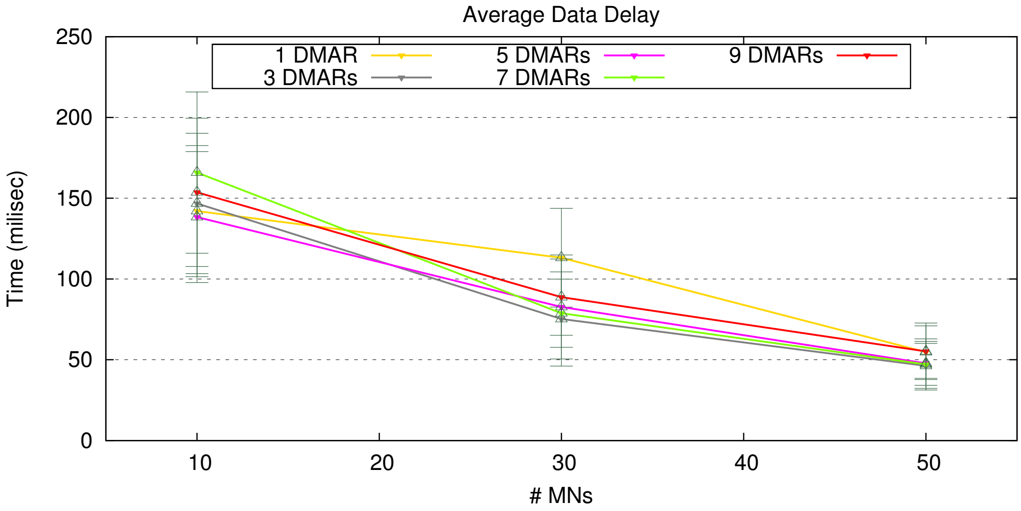

Figure 3.42: Average Data Delay in the City scenario.

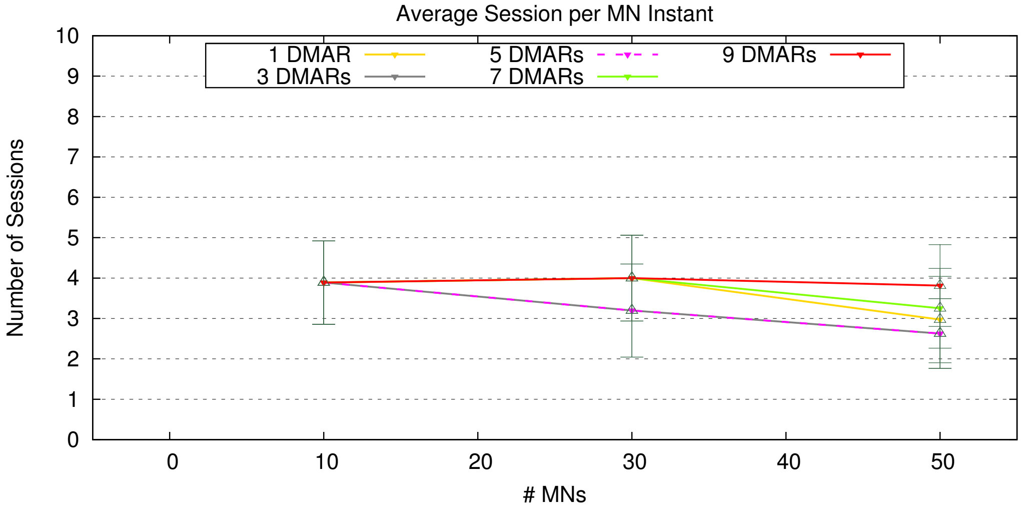

Figure 3.43: Average Session per MN in the City scenario.

Once again, for the cases of having 3 and/or 5 DMARs, the values of mobility handover are lower. Therefore, they are a good solution regarding this parameter and comparatively with other cases. The worst result belongs to the case of having 9 DMARs.

3.8.5 Evaluation of MIPv6 and DMIPA performance: City Scenario

Following, it is presented a comparison between MIPv6 protocol and DMIPA with 4 DMARs. The main goal is to evaluate these two cases, the MIPv6 which is a centralized mobility management protocol and, DMIPA, which is a distributed mobility management.

Figure 3.46 shows the signalling cost results for the two cases. It is concluded that the use of 4 DMARs reduces the signalling cost when compared with MIPv6. We can conclude

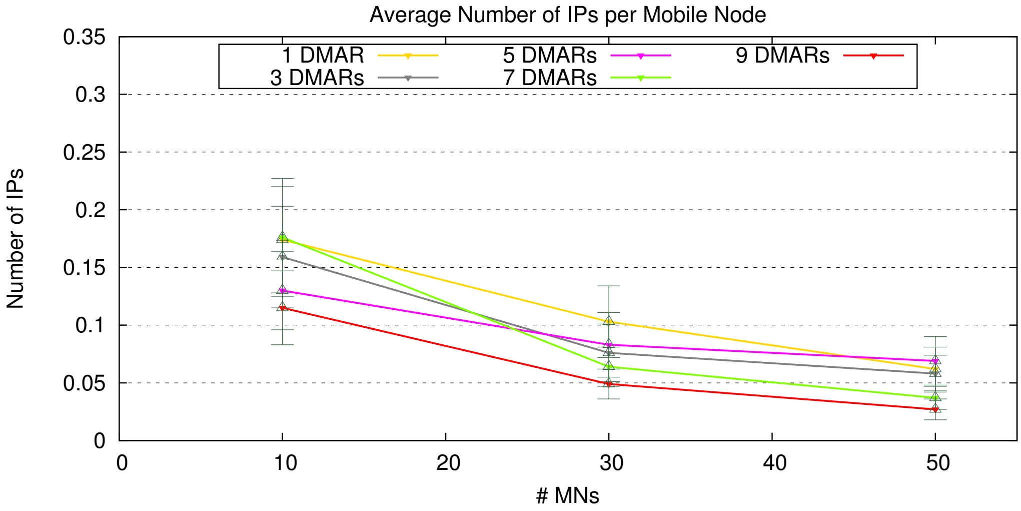

Figure 3.44: Average Number of IPs per MN in the City scenario.

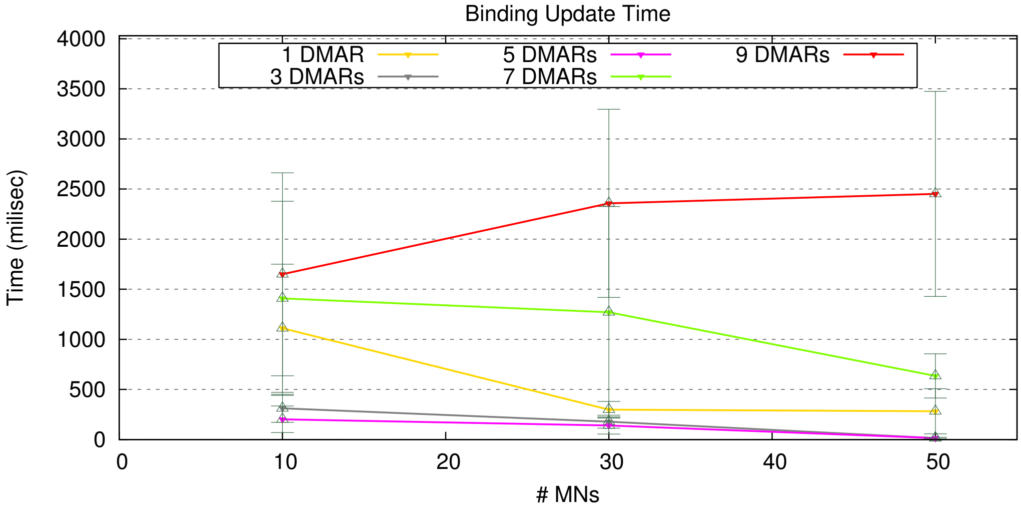

Figure 3.45: Binding Update Time in the City scenario.

that the signalling messages spend less time in the network for the 4 DMARs DMIPA case, when compared with MIPv6. Since the HA is far away from the MNs, the time to exchange signalling messages is longer.

Analysing the data cost of Figure 3.47, we conclude that DMIPA with 4 DMARs has better results in contrast with MIPv6.

The DMIPA reduces the data loss and the values of average data delay, Figure 3.48 and 3.49, respectively. As mentioned before, the high number of packet losses is a consequence of the handover mechanism. The use of 4 DMARs cleary reduces the values of the binding update time.

The binding update time is illustrated in Figure 3.52. When analysing the two protocols, the use of 4 DMARs clearly reduce the values of mobility handover. Due to the fact that

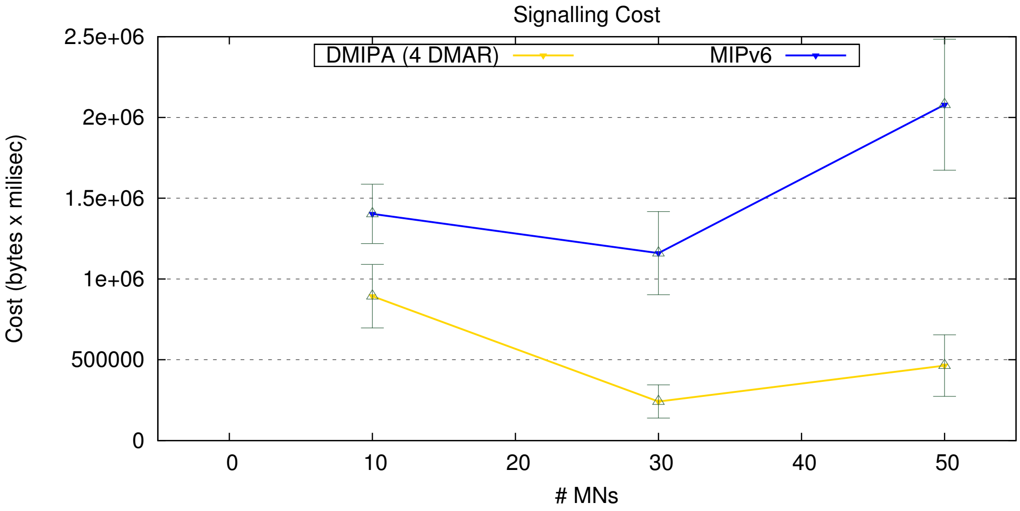

Figure 3.46: Comparing Signalling Cost of MIPv4 and DMIPA (4 DMARs) in the City scenario.

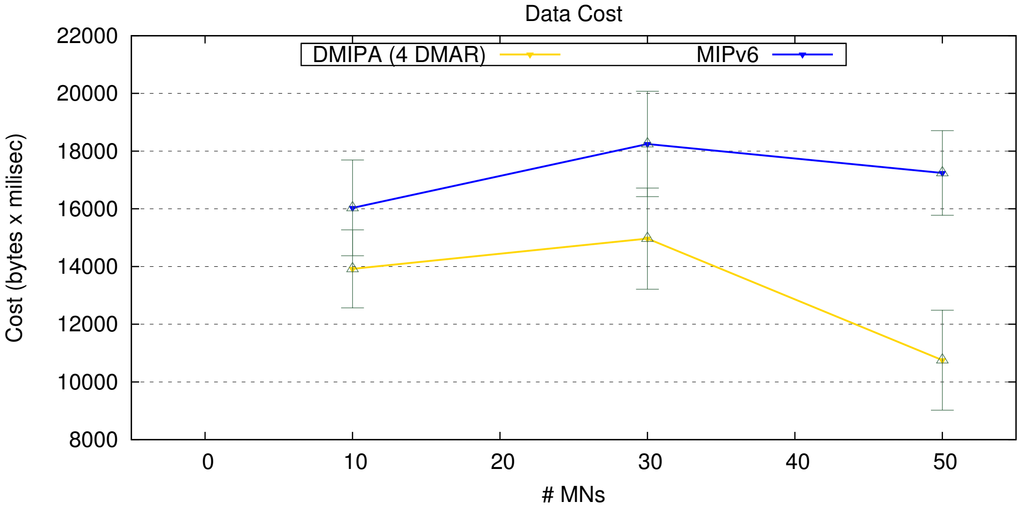

Figure 3.47: Comparing Data Cost of MIPv6 and DMIPA (4 DMARs) in the City scenario.

DMARs are closer to the end user, the time to update the binding is lower, comparatively with the time that is needed to update the binding in the HA.

According to the results shown in this section, DMIPA with 4 DMARs has the ability to significantly reduce the values of signalling cost, data cost, data loss, average data delay and binding update time, when compared with the other two cases. In this scenario, DMIPA is better than MIPv6 because the nodes can exchange messages with less packet loss and less average data delay.

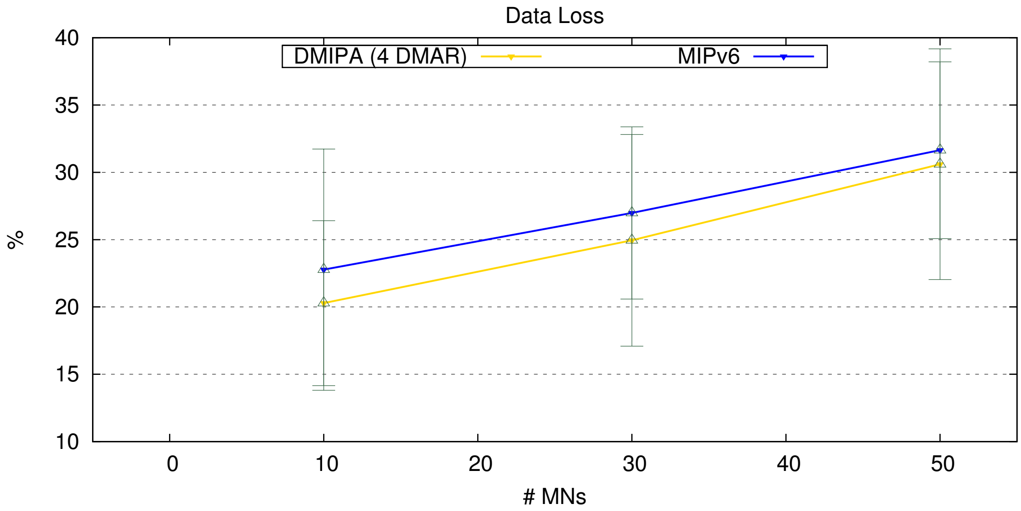

Figure 3.48: Comparing Data Loss of MIPv6 and DMIPA (4 DMARs) in the City scenario.

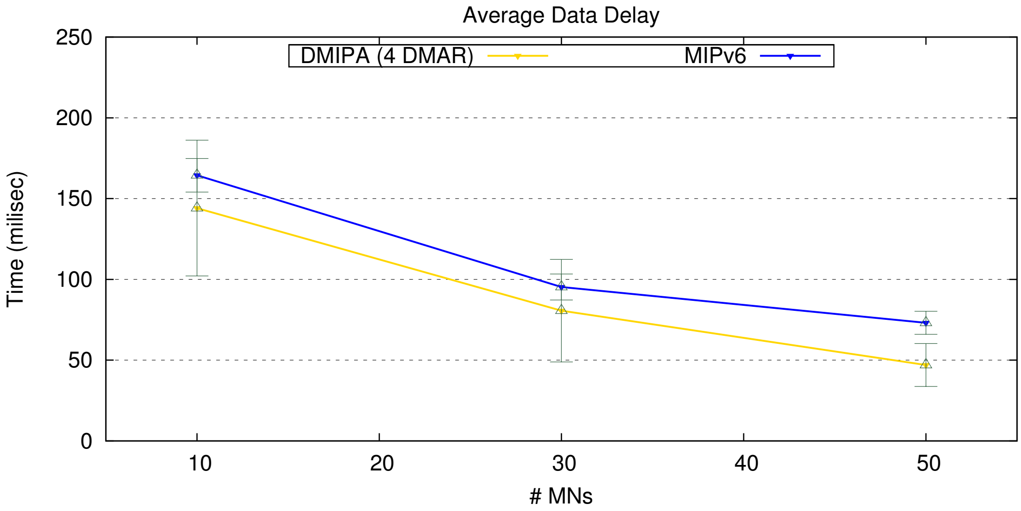

Figure 3.49: Comparing the Average Data Delay of MIPv6 and DMIPA (4 DMARs) in theu City scenario.

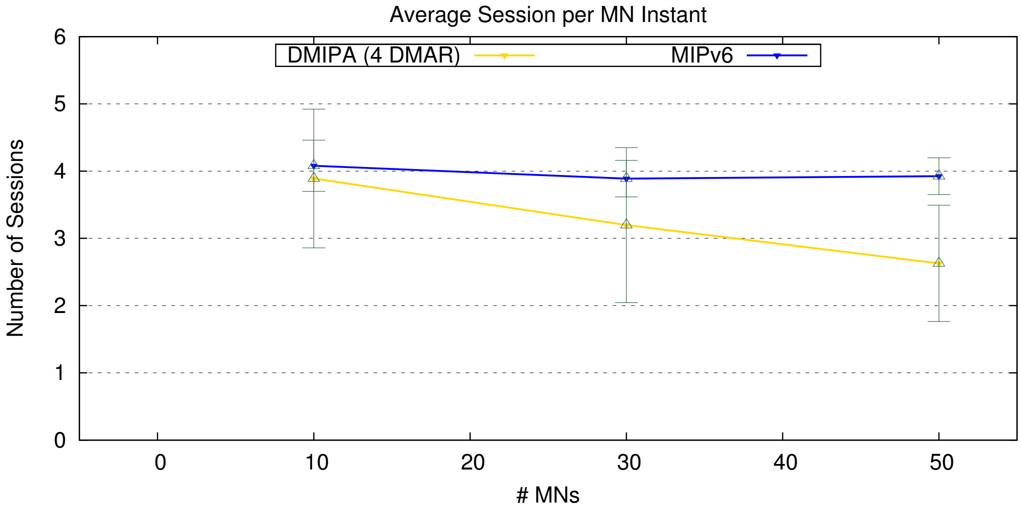

Figure 3.50: Comparing the Average Session per MN of MIPv6 and DMIPA (4 DMARs) in the City scenario.

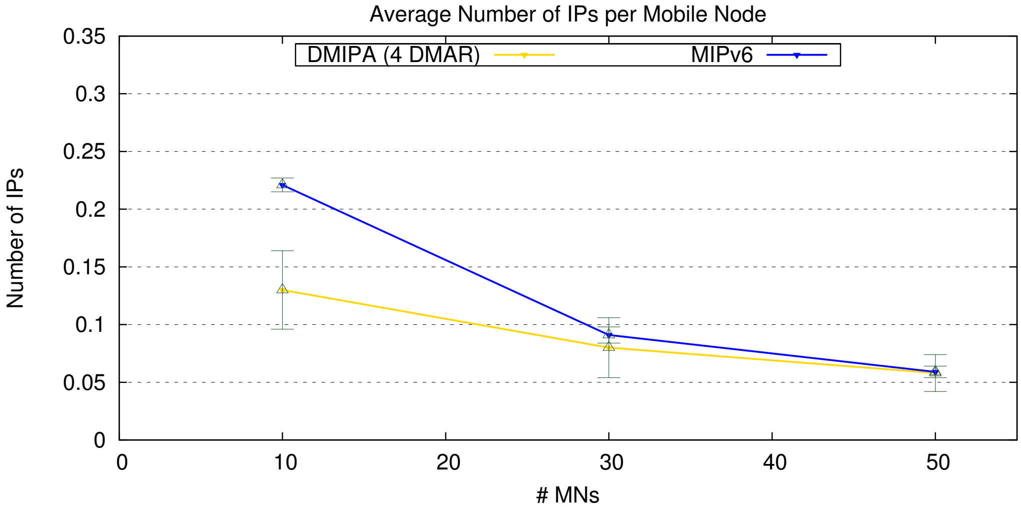

Figure 3.51: Comparing the Average Number of IPs per MN of MIPv6 and DMIPA (4 DMARs) in the City scenario.

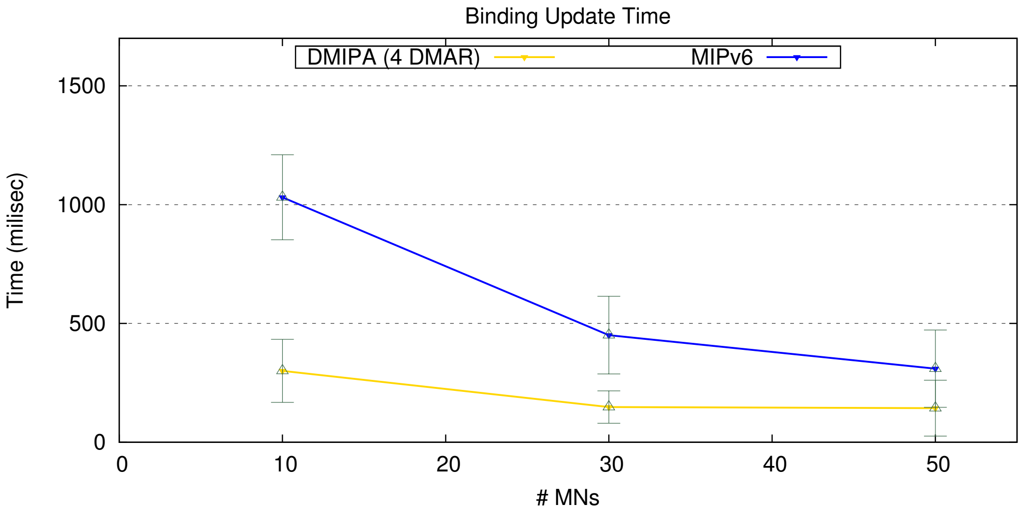

Figure 3.52: Comparing the Binding Update Time of MIPv6 and DMIPA (4 DMARs) in the City scenario.

3.9 Overall Discussion, Analysis and Conclusions

This Chapter evaluated two distinct protocols that aim to solve the mobility management problem in IP networks. MIPv6 provides global mobility management to mobile terminals by managing tunnels and binding updates. Unfortunately, the centralized architecture upon which the MIPv6 has been developed is not suitable for the demand in dynamic mobility patterns in vehicular networks. As an emerging solution, DMIPA provides global mobility by adding proper mobility management mechanism to the access routers and mobile nodes. Thus, its decentralized architecture avoids single point of failures, congestion and bottlenecks.

When we compared these two mobility management protocols in the Short Highway scenario where the speed is increased, we concluded that DMIPA is better than MIPv6. However, for high speeds, the results are similar, which leads to the conclusion that a centralized architecture has the same performance as a distributed architecture. Additionally, both protocols are tested in the City scenario. In this case, we analyse MIPv6 with DMIPA using 4 DMARs. Comparing both protocols, we notice an improvement in the evaluated parameters.

The results of the simulation scenarios show that, regarding the signalling cost, data cost, data loss, average data delay and binding update time, DMIPA provides lower values when compared with MIPv6 in vehicular environments. Moreover, it is interesting to observe that for a balanced solution, which means, that the number of DMARs and legacy ARs, are similar, the results are better. Therefore, there must be a careful planning when assigning the mobility management functions to the access routers in a real vehicular environment.

DMIPA improves the overall performance in vehicular environments when compared with the legacy mobility management protocol, called MIPv6. Therefore, DMIPA is a better solution than MIPv6, when mobility management is needed in vehicular environments. These protocols face large challenges, due to a dynamic and high mobility of MNs in vehicular environment. We will choose DMIPA as the solution to provide mobility management in vehicular networks.

Nevertheless, mobility management approaches for all-IP networks have to be improved to provide a better solution for VANETs. The future approaches have to take into account the vehicular's behaviour, as well as the widely dynamic environments in order to solve the mobility management in dynamic and spontaneous vehicular networks.

Chapter 4

Proof of Concept in Distributed and Dynamic Mobility Management

4.1 Introduction

The objective of Chapter 4 is to evaluate, in a real network, the performance of DMIPA with and without multihoming support. Section 4.2 explains and illustrates the use-case scenarios in which the MN communicates through a single interface. Furthermore, in Section 4.3 it is presented DMIPA with multihoming support with multi-interface mobile nodes.

Finally, both concepts are evaluated in the implemented scenario proving the ability of DMIPA to provide session continuity and the capability to improve user experience in multihomed scenarios, as well as in scenarios in which the mobile node has only one interface. This section is concluded by presenting the results, the respective analysis and the conclusions.

4.2 DMIPA Without Multihoming Support

This section will describe the use-case scenarios for the DMIPA protocol without multihoming support.

4.2.1 Use-case Scenarios Description

First of all, it is presented an use-case scenario that is very common in a DMIPA topology in which not every AR has mobility management capabilities. Therefore, in the access level the network has DMARs and ARs, as illustrated in Figure 4.1. This scenario provides the handover mechanism between DMARs and ARs, running the DMIPA protocol, in which the MN uses only one wireless interface to communicate with the CN. As a normal procedure of DMIPA protocol, the DMARs and the MN are responsible to ensure session continuity, thus when the MN is attached to an AR with IP prefix P2::/64, they have to establish a tunnel to guarantee the continuity of any session initiated when the MN was attached to DMAR1. The MN has to manage IP addresses in order to set the P1::Intf1/64 as a preferred IP address; on its turn, the DMAR1 has to manage routing rules to keep any ongoing sessions active. For instance, if the MN moves from the AR domain to DMAR2 domain, the DMAR1 and DMAR2 establish a tunnel and manage routing rules, while the MN is in charge to set the P3::Intf1/64 as a preferred IP address and the P1::Intf1/64 as deprecated state. Since the

P3::Intf1/64 IP address is configured as a preferred state, any new session that is initiated with the MN goes through DMAR2 without tunnelling due its capability to ensure session continuity. On the other hand, any session that is initiated when the MN is attached to an AR follows a data path in which the packets are tunnelled from MN to DMAR1, since the AR does not support mobility capabilities.

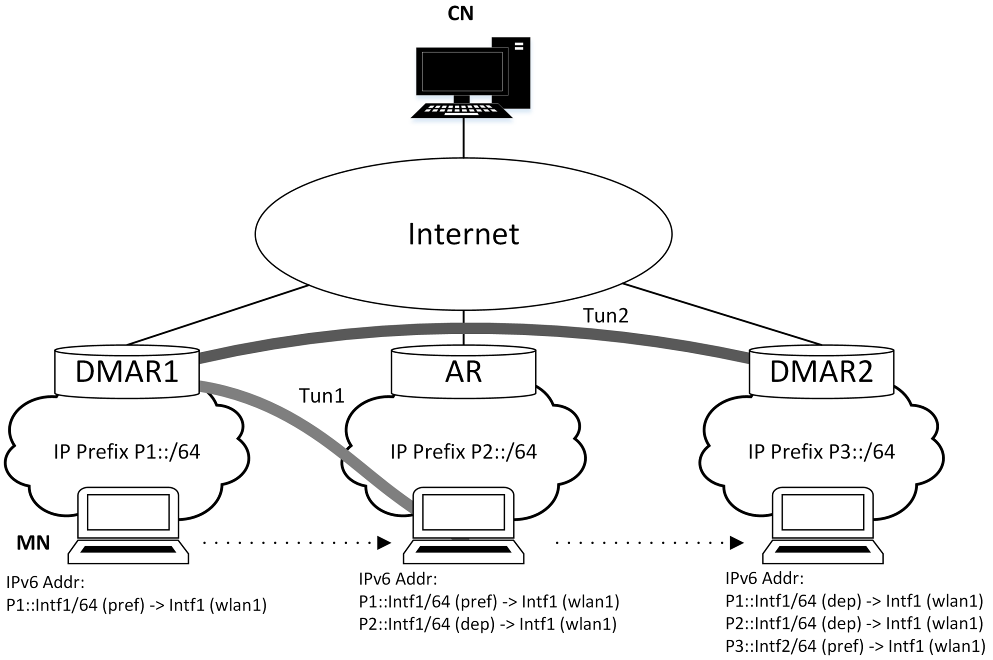
CN
Internet
Tun2
DMAR1
AR
DMAR2
Tun1
IP Prefix P1::/64
IP Prefix P2::/64
IP Prefix P3::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
P2::Intf1/64 (dep) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (dep) -> Intf1 (wlan1)
P3::Intf2/64 (pref) -> Intf1 (wlan1)

Figure 4.1: Common Scenario in DMIPA topology (without multihoming support).

The Scenario A (Figure 4.2) provides the handover mechanism between different DMARs using only one interface. This scenario is used as a reference model to Scenario D (Figure 4.8 - Section 4.3.2) which provides the handover mechanism to move sessions between interfaces connected to DMARs in the same or different IP domains. The CN initiates Session 1 when the MN is attached to DMAR1, Session 2 when MN is attached to DMAR2, and starts Session 3 when the MN is attached to DMAR3.

In Scenario B (Figure 4.3), the MN performs handovers from DMAR1 to DMAR2 and then from DMAR2 to AR. It is used only the Interface 1 (wlan1). When the MN is attached to DMAR1, the CN initiates Session 1 to the IP address P1::Intf1/64 . When the MN roams to DMAR2, Session 1 is anchored to DMAR1 and the data packets are forwarded to DMAR2 through a tunnel bewteen those DMARs. While the IP address P1::Intf1/64 is configured as deprecated to maintaing the ongoing Session 1, the IP address P2::Intf1/64 is set as preferred to start the new data session (Session 2). When the MN performs handover to the AR domain, the sessions are kept active because DMARs an MN establish tunnels to forward data packets to and from the CN. In this reference model, the DMARs and the MN have to manage the tunnels and routing rules to maintain session continuity. The correspondent multihoming scenario is illustrated in Figure 4.9 - Section 4.3.2.

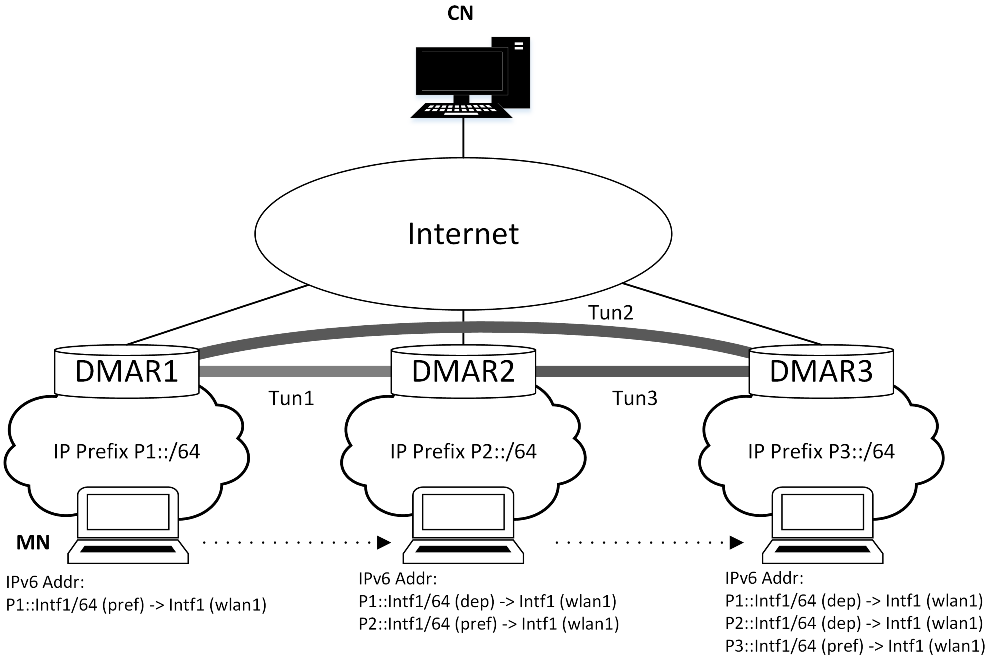
CN
Internet
Tun2
DMAR1
DMAR2
DMAR3
Tun1
Tun3
IP Prefix P1::/64
IP Prefix P2::/64
IP Prefix P3::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (dep) -> Intf1 (wlan1)
P3::Intf1/64 (pref) -> Intf1 (wlan1)

Figure 4.2: Scenario A.

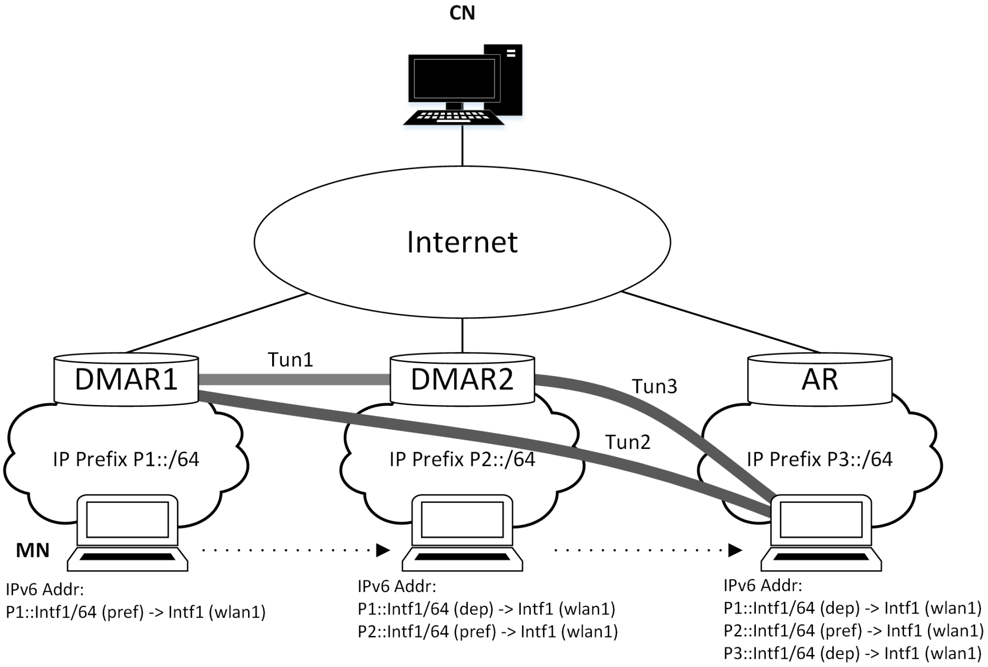
CN
Internet
Tun1
DMAR1
DMAR2
Tun3
AR
Tun2
IP Prefix P1::/64
IP Prefix P2::/64
IP Prefix P3::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
P3::Intf1/64 (dep) -> Intf1 (wlan1)

Figure 4.3: Scenario B.

4.3 DMIPA With Multihoming Support

The present section gives a brief overview of the multihoming concept and explains the specifications for a distributed mobility management with multihoming support.

4.3.1 Multihoming Overview and Specifications

In this framework, multihoming is the configuration of different network prefixes through multiple network interfaces, or the assigning of multiple IP addresses to a single interface. The combination of both methods are also possible. Thus, DMIPA with multihoming support is possible by configuring a specific set of mobility mechanisms on the mobility management. One of the main features to be considered by the mobility management is the session continuity and so, it has to detect and react to user interface state changes (e.g. link up/down).

Since cellular operators seek for offloading solutions, and the paradigm of mobile data traffic consumption is changing very fast, it is important to think carefully about the features that are essential to include in the mobility management decision. Therefore, the resources available and the information about users' daily routines such as locations, network applications and contents should be part of a whole set of decisions that mobility management can take. The mobility mechanisms must have the ability to initialize the mobility management decisions via the network mobility entities, and to provide the required interactions with IP address, mobility anchors, IP tunnels and routing rules. Two mechanisms are following explained, and each one introduces different complexities in order to solve distinct situations. The first mechanism was developed to improve session continuity for local mobility, when the MN moves inside a building, crosses the streets or roams to another neighbourhood. The second was proposed when the first mechanism does not ensure session continuity for global mobility.

Figure 4.4 illustrates a case that provides a handover mechanism to move sessions between interfaces connected to the same DMAR where distinct IP domains are available. Such mechanism allows MN to maintain session continuity while moving ongoing sessions to another interface(s) that are connected to the same DMAR. There are network topologies that can provide one or more IP domains, using several interfaces or different access technologies. Adopting a strategy based on the occurred events, like reacting to a link down or simply optimize the resources, the mobility management could enable the described mechanism in the following use-case scenarios:

a) MN connected to the same DMAR (one IP domain) through several interfaces to different access technologies (802.3, 802.11b/n or 802.11p) suffers a disruption in one of the interfaces, or one of the medium access is overloaded.

b) Network operator might use distinct IP domains from the same or different access technologies connected to the same DMAR and a link down might occur in one of the user's interfaces, or the network operator desire to maintain load balancing.

As illustrated in Figure 4.4, when the MN performs the handover of sessions from Interface 1 to Interface 2 it needs to update the connected DMAR and to perform the required changes. The DMAR is in charge to introduce routing rules to forward packets from the IPs of Interface 1 to the preferred IP of the Interface 2. In the current example, the sessions anchored in DMAR1 and DMAR2 with IP addresses P3::Inft2/64 and P2::Inft2/64, respectively, are forwarded to P1::Inft1/64 in DMAR1. In addition, the MN has to move these IP addresses assigned to Interface 2 to Interface 1 to guarantee that Interface 1 sends and receives packets with these IP addresses. The configuration of the IPv6 addresses as preferred state or deprecated state is determined by the mobility management strategy. Then, if one of the IPv6 addresses of Interface 1 is configured with preferred state, the others are setup to deprecated state. For instance, if the mobility management decides to anchor a new session to DMAR1 through Interface 1, then the IP addresses moved to Interface 1 are configured with the deprecated state only to maintain the ongoing sessions, while the IP address received in Interface 1 from Network 1 is configured with the preferred state.

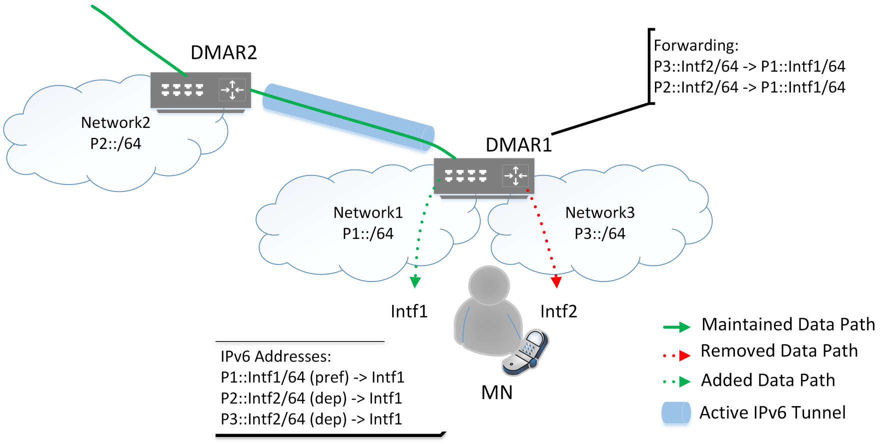

Figure 4.4: Example of handover between interfaces connected to the same DMAR.

The cases illustrated in Figure 4.5 and Figure 4.6 allow the MN to perform handover for sessions moved between interfaces connected to different ARs/DMARs, which are not able to be solved by the case of Figure 4.4. As previous explained, the case of Figure 4.4 deals only with routing rules to forward sessions, while the cases of Figure 4.5 and 4.6 introduce the IP tunnels management mechanism. In Figure 4.6 is assumed that MN interfaces are connected to different ARs; otherwise the handover mechanism might be solved as in the case of Figure 4.4.

The cases of Figure 4.5 and 4.6 differ in the mobility support of the connected AR. The first one is shown in Figure 4.5 and provides a scenario where sessions are moved to other interfaces connected to a DMAR.

The MN is connected to DMAR5 through Interface 1 and connected to DMAR4 in Interface 2. As such, the MN maintains sessions anchored to DMAR2 which are tunnelled to DMAR5, and also, sessions anchored to DMAR3 are tunnelled to DMAR5. If for some reason the mobility management decides to forward sessions anchored to DMAR3 and DMAR4 to DMAR5, it has to manage the existing tunnels in a way that Tun2 is modified and Tun3 is created. Then, the MN has to move the IP addresses P2::Intf2/64 and P3::Intf2/64 to Interface 1 in the deprecated state in order to keep the current sessions active. Figure 4.6 illustrates the scenario of the second case, where sessions are moved to other interfaces connected to an AR. The MN is connected to AR2 in Interface 1 (Intf1) and connected to AR1 in Interface 2 (Intf2). The way MN maintains sessions active is simple: a tunnel is established between DMAR1 and Interface 1 and DMAR2 and Interface 1, as well as sessions are anchored

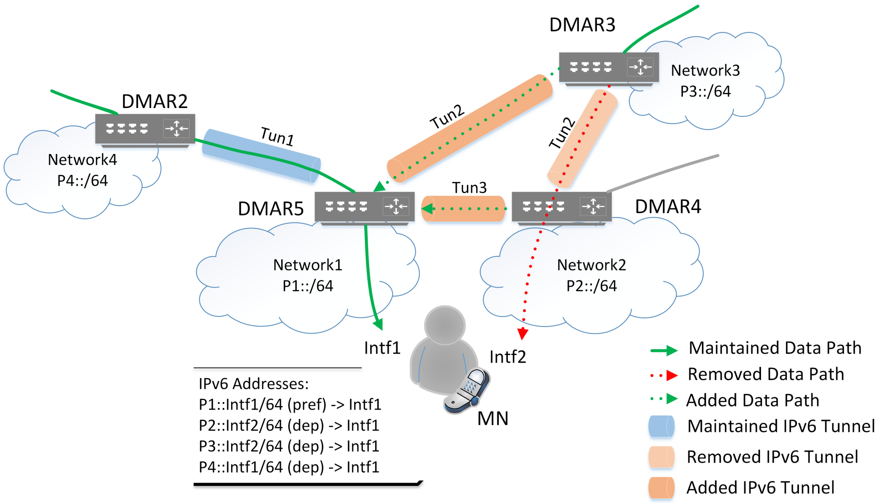

Figure 4.5: Example of handover between interfaces connected to different DMARs.

to DMAR3 which are tunnelled to Interface 2. At a given time, the mobility management decides to change sessions anchored to DMAR3 from Interface 2 to Interface 1, so Tun3 has to be modified to be attached to Intf1 and its preferred IPv6 address (P3::Inft2/64) in the MN. Since the connected AR does not support mobility management capabilities, the mobility management mechanism must select a preferred tunnel attached to Interface 1 in order to established new sessions that need session continuity support. Moreover, if the mobility management decides to use Inff2 to initiate sessions that require continuity, this mechanism has to establish a tunnel between Intf2 and the correspondent DMAR and configures the respective IPv6 address. Otherwise, the MN will not be able to keep sessions active when it roams to different networks.

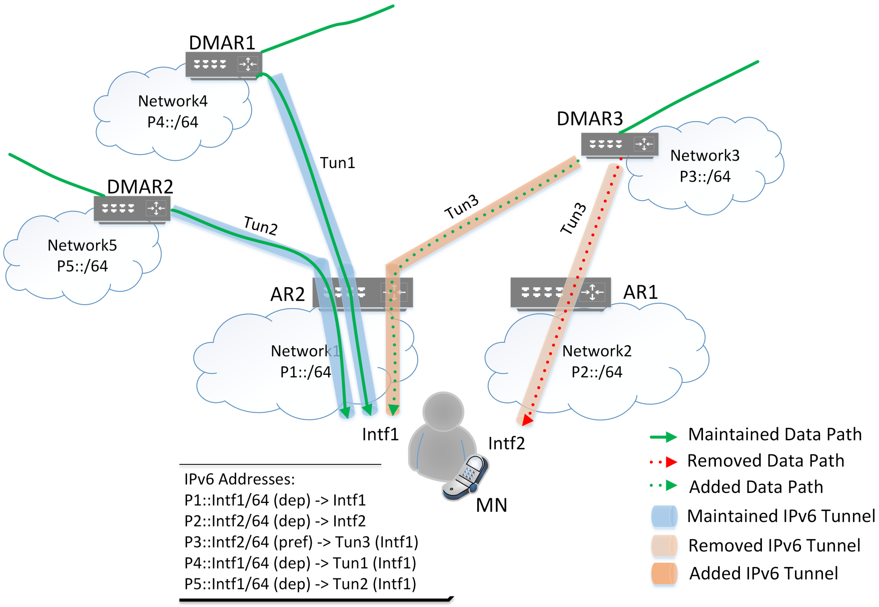

Figure 4.6: Example of handover between interfaces connected to different ARs.

As a conclusion, the mechanisms explained above are focused on the resources management and data delivery performance, therefore the handover execution time is not optimized. The mobility management makes possible handovers of sessions between DMAR/interfaces that might be caused by the resources optimization, improvement of QoS, QoE and due a reaction to a link down event, as well as, select part of the DMARs associated to an interface and consequently the attached sessions, to be forwarded to the other MNs interface through direct tunnel or through a tunnel with the connected DMAR.

4.3.2 Use-case Scenarios Description

The first example is shown in Figure 4.7 and represents a simple case of multihoming in which the MN initiates Session 1 when it is attached to DMAR1 through Interface 1 (wlan1). After it is moved to DMAR2, it initiates Session 2, while maintaining the ongoing Session 1 through Interface 1. The DMARs establish a tunnel between themselves to ensure session continuity. At a certain moment, the MN decides to change both sessions from Interface 1 to Interface 3 (eth0). The deployment of this scenario follows the specification described in Section 4.3.1 and illustrated in Figure 4.4. The main goal is the ability of change Session 1 and 2 from Interface 1, which is connected to DMAR2 through the network with IP prefix P2::/64, to Interface 2 which is also connected to DMAR2 but through a different network domain.

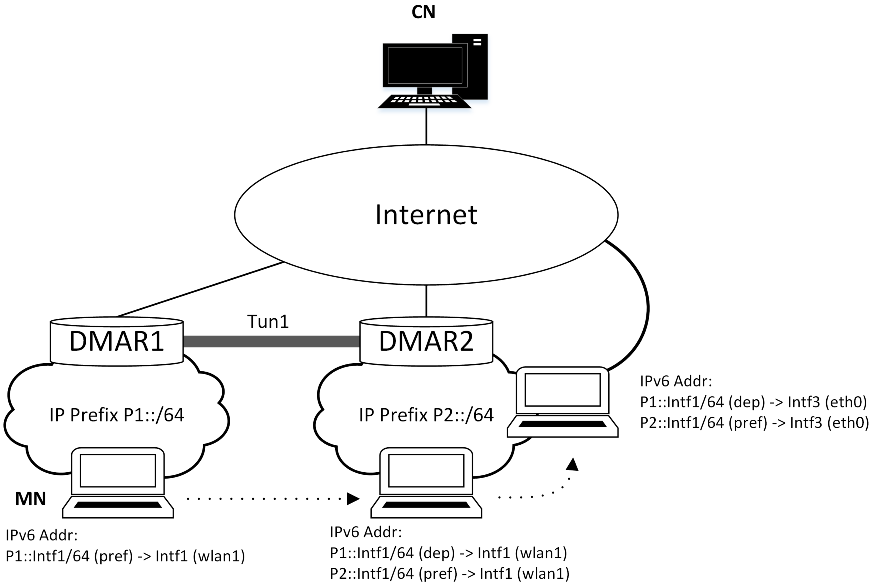
CN
Internet
Tun1
DMAR1
DMAR2
IP Prefix P1::/64
IP Prefix P2::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf3 (eth0)
P2::Intf1/64 (pref) -> Intf3 (eth0)

Figure 4.7: Scenario C.

The Figure 4.8 illustrates the case where the MN has to update the connected DMAR and to perform the required changes, when it moves the Session 1 from Interface 1 (wlan1) to Interface 2 (wlan0) and then to Interface 3 (eth0). The Session 2 is mantained through Interface 1 (wlan1) during the movement, as well as Session 3 that stays anchored to Interface 3 (eth0). The DMARs are responsible to ensure a data path between the CN and the MN, therefore they introduce routing rules to forward packets from the IPs of the previous interface to the preferred IP of the interface. In Scenario D, when the MN is connected to DMAR3 through Interface 2, the sessions anchored in DMAR1 with the IP address P1::Intf1/64 are forwarded to P3::Intf2/62 in DMAR1. Moreover, the MN has to move the IP address assigned to Interface 1 to the Interface 2, with the purpose of ensuring the data flows of Session 1. The Session 2 is maintained through Interface 1 (wlan1), and Session 3, that is anchored to DMAR3, is moved from Interface 2 (wlan0) to Interface 3 (eth0).

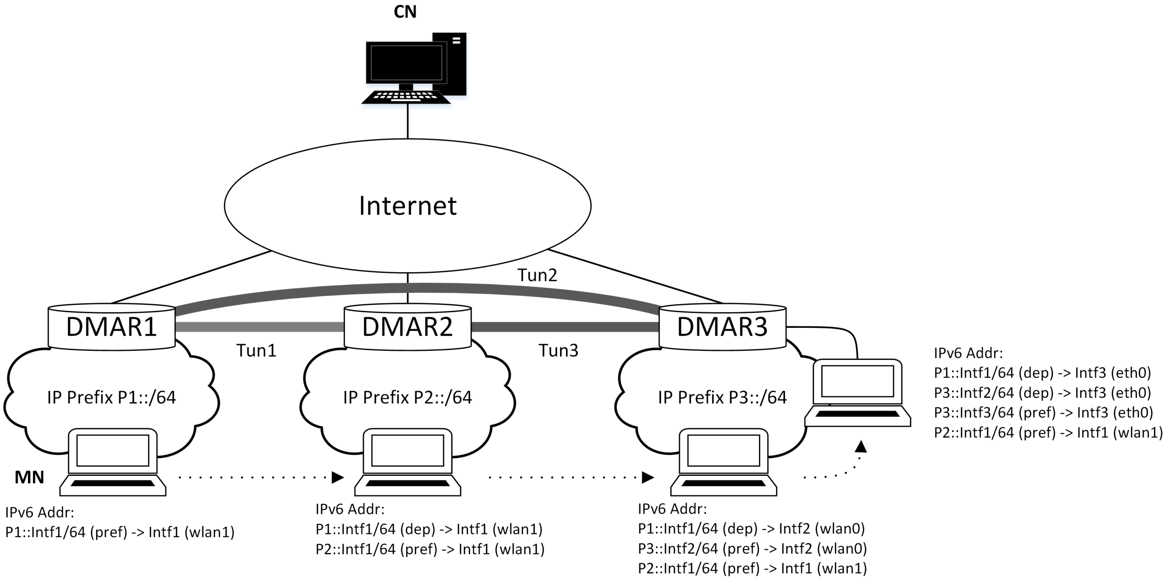
CN
Internet
Tun2
DMAR1
DMAR2
DMAR3
Tun1
Tun3
IP Prefix P1::/64
IP Prefix P2::/64
IP Prefix P3::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf2 (wlan0)
P3::Intf2/64 (pref) -> Intf2 (wlan0)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf3 (eth0)
P3::Intf2/64 (dep) -> Intf3 (eth0)
P3::Intf3/64 (pref) -> Intf3 (eth0)
P2::Intf1/64 (pref) -> Intf1 (wlan1)

Figure 4.8: Scenario D.

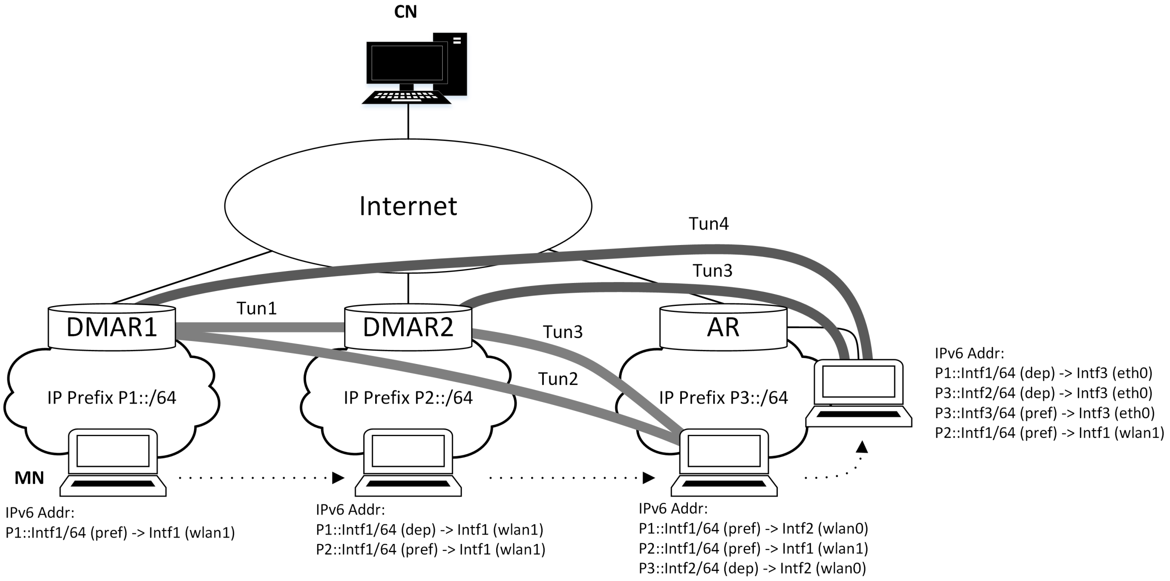
CN
Internet
Tun4
Tun3
Tun1
DMAR1
DMAR2
Tun3
AR
Tun2
IP Prefix P1::/64
IP Prefix P2::/64
IP Prefix P3::/64
MN
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf1 (wlan1)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
IPv6 Addr:
P1::Intf1/64 (pref) -> Intf2 (wlan0)
P2::Intf1/64 (pref) -> Intf1 (wlan1)
P3::Intf2/64 (dep) -> Intf2 (wlan0)
IPv6 Addr:
P1::Intf1/64 (dep) -> Intf3 (eth0)
P3::Intf2/64 (dep) -> Intf3 (eth0)
P3::Intf3/64 (pref) -> Intf3 (eth0)
P2::Intf1/64 (pref) -> Intf1 (wlan1)

Figure 4.9: Scenario E.

Figure 4.9 illustrates the case where the MN has to roam Session 1 from Interface 1 (wlan1) to Interface 2 (wlan0) and then to Interface 3 (eth0), while maintaining Session 2 through

Interface 2 during the movement. In order to guarantee a data path between the CN and the MN, the DMARs and the MN itself introduce routing rules to forward packets from the IPs of the previous interfaces to the preferred IP of the new interface.

At a certain point, the MN roams to the AR domain and uses the Interface 2 to establish a tunnel with DMAR1 to keep Session 1 active. Thus, MN changes the IP address P1::Intf1/64 from Interface 1 to Interface 2, while the IP address P2::Intf2/64 still configured on Interface 1. Finally, the MN moves the IP address P1::Intf1/64 from Interface 2 to Interface 3, as well as the P3::Intf2/64 IP address from Interface 2 to Interface 3.

4.4 Testbed Description

The available testbed is shown in Figure 4.10. Internet Protocol version 6 is provided through the Neighbour Discovery Protocol messages by the network of Institute of Telecommunications (IT) of Aveiro. Three Single Board Computers (SBCs) with OpenWrt [48] are connected through Ethernet cable to IT Aveiro network, and the Router Advertisement Daemon *radvd* of each SBC announces the respective IPv6 prefix. The SBCs can be configured as simple Access Router (AR) or as Data Mobility AR (DMAR). Therefore, if the SBC is configured as DMAR, the *radvd* is setup with the HA flag equal to 1, announcing the IPv6 address of the interface. In this case the MN is a mobile computer owning three interfaces: a Wi-Fi 802.11g (wlan0), an Universal Serial Bus (USB) Wi-Fi 802.11b/g (wlan1) and an Ethernet interface (eth0).

The architecture of the testbed is the matching between the use-case scenario illustrated in Figure 2.12 and the available testbed in Figure 4.10.

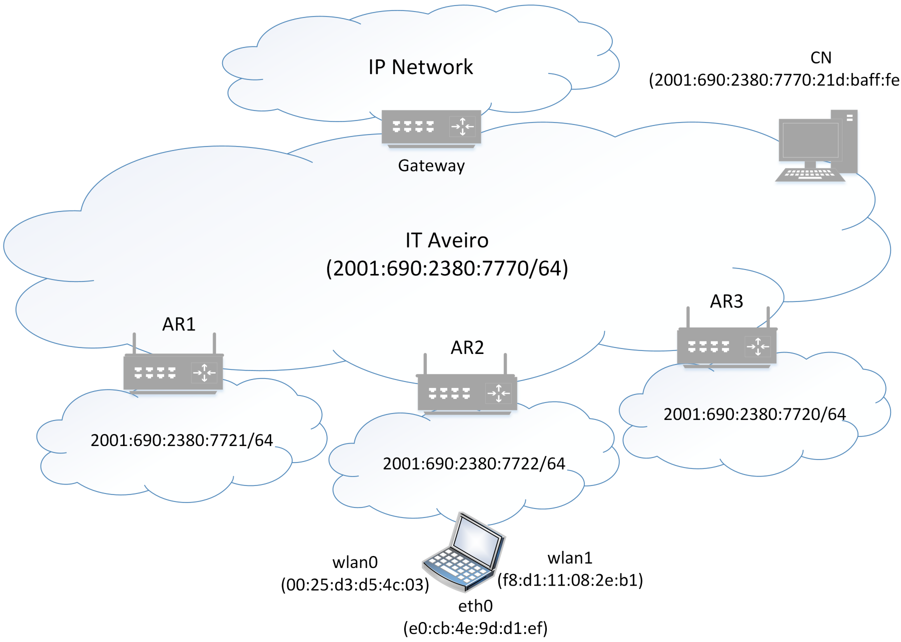

Figure 4.10: Testbed.

To generate UDP and TCP sessions it is used the Distributed Internet Traffic Generator (D-ITG) Application [49], which is a platform capable to produce traffic at packet level accurately replicating appropriate stochastic processes. In order to obtain the correct value of the end-to-end packet delay, it is used the Precision Time Protocol daemon (PTPd) application [50]. In this way, it is possible to synchronize the CN and MN clock. The Table 4.1 describes these similarities.

	Use-case Scenario	Testbed Scenario
Access Networks	AR1 (cellular)	AR1 (2001:690:2380:7721/64)
	AR2 (cellular)	AR2 (2001:690:2380:7722/64)
	AR3 (Wi-Fi+cable)	AR3 (2001:690:2380:7720/64)
MN's Interfaces	cellular	wlan1 (f8:d1:11:08:2e:b1)
	Wi-Fi	wlan0 (00:25:d3:d5:4c:03)
	cable	eth0 (e0:cb:4e:9d:d1:ef)
Services	Vimeo video	D-ITG Application from CN (2001:690:2380:7770:21d:baff:fe8b:2e53)
	Skype call	D-ITG Application from CN (2001:690:2380:7770:21d:baff:fe8b:2e53)
	Facebook feeds	D-ITG Application from CN (2001:690:2380:7770:21d:baff:fe8b:2e53)

Table 4.1: Matching between Use-case and Testbed scenarios.

- **Step 1**: The MN is connected through wlan1 to AR1, and the CN initiates an UDP or TCP session - Session 1.
- **Step 2**: The MN connects to AR2 through wlan1 and establishs a communication from CN to MN (UDP or TCP session) - Session 2, while the previous session is maintained via wlan1.
- **Step 3**: MN stays connected to AR2 through wlan1 and establishes a new connection with AR3 through wlan0. Both previous sessions, Session 1 and Session 2, are maintained through wlan0 and wlan1, respectively. The CN initiates a new session - Session 3 - using the D-ITG application through wlan0 interface.
- **Step 4**: Finally, the MN is connected through wlan1 to AR2 and through wlan0 and eth0 to AR3. The Session 2 between the CN and the MN is maintained through wlan1, while all other active sessions are maintained through eth0.

Note that, the steps above are according to a scenario in which the mobile node has multiple interfaces. For the case in which the mobile node communicates through a single interface, there is no exchange of sessions between interfaces, and therefore, the sessions are kept active through the single interface.

Regarding the possible scenarios, it was considered the two most important ones to evaluate the tested approach. The case-study assumes that AR3 may be a mobility capable router or a legacy access router. In the first case, AR2 is involved in the management of the mobility mechanism, while the MN is roaming to another network or while it moves the ongoing sessions to another interface, due to a link down event or because certain decision was taken by the mobility manager. When the AR3 is a legacy access router, which refers to the second case, the MN and the previous mobility capable router are in charge to manage the mobility mechanism themselves. Section 4.6 shows the results of the tested scenario where the experiment testbed runs IPv6 services from the IT Aveiro network as described before.

4.5 Implementation Description

This section describes the protocols and applications that were deployed to support the mobility management capabilities. We start to describe the implementation process from the CN, going through the ARs and ending in the MN, in order to provide a good explanation of the work done in the real testbed of Figure 4.10.

First of all, it was developed a scrip file with the proper code to initiate the sessions using the **ITGSend**. The **ITGSend** component is responsible for generating traffic flows and can work in three different modes: Single-Flow, Multi-Flow and Daemon. In this context, by making use of the Multi-Flow mode, we were able to read the traffic flows to generate from a script file. In this scrip file, we configured the parameters that characterize the sessions, and they are: the destination address, the session type, the session duration, the packet size, and the packet rate. The **ITGSend** component was locally triggered in the CN.

We developed script files in order to implement the DMIPA protocol, distributing the mobility management functionalities in the ARs. Therefore, in the ARs that represent the DMARs, we develop scrip files to provide the required interactions with IPv6 address, IPv6 tunnels and routing rules. These scrip files were able to create, modify and eliminate the IPv6 tunnels and routing rules between DMARs or betweem them and the MN. Moreover, such scripts were remotely triggered in the exact moment when they were needed.

Finally, in the MN, we developed a main scrip file that is initiated by hand and then it runs all the mobility process automatically. In this way, this scrip file is in charge to initiate the **ITGRecv** and to trigger the scrip files stored in the ARs. The **ITGRecv** component is responsible for receiving multiple parallel traffic flows generated by the **ITGSend** instance. We set the **ITGRecv** to produce the log files which are our output files, containing detailed information about every sent and received packet. In order to sync the clock of MN and CN, it was started the PTPd application.

This work was perdormed in cooperation with a PhD Thesis. The next section demonstrates the results obtained through the tests performed in the real testbed.

4.6 Testbed Evaluation, Results and Analysis

In this section it is present the result of the tests made using the testbed and it is compared the results between the reference and the multihoming matching model according with the different scenarios showed above.

4.6.1 Testing the Limitations of the Testbed: Part 1

First of all, to evaluate the limitation of the testbed it was tested the use-case scenario of Figure 4.1. The D-ITG Application was used to generate UDP packets with a constant payload size of 1024 bytes and a constant rate of 250 and 1000 packets per second (pps).

Figure 4.11 illustrates the bitrate for a constant rate of 250 packets per second. Theoretically, the bitrate is the multiplication of the packet rate with the payload size; therefore, the

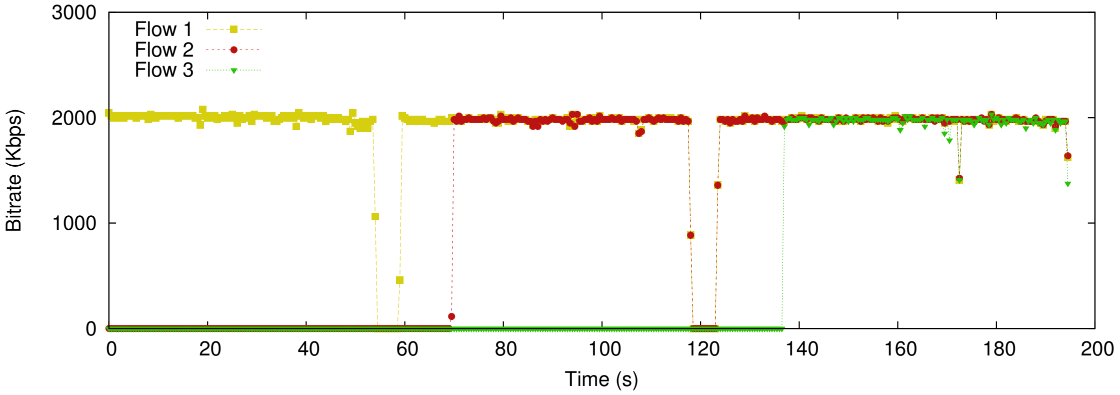

Figure 4.11: Bitrate at 250 packets per second.

value of bitrate is 2048 Kbps. Analysing the Figure 4.11, it is concluded that the results are according with the theoretical value.

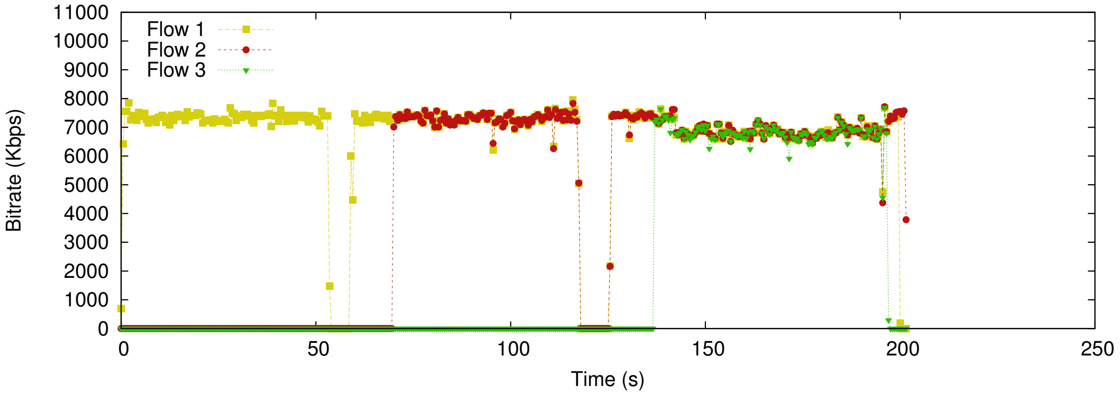

Figure 4.12: Bitrate at 1000 packets per second.

Figure 4.12 illustrates the bitrate values for the three sessions. Applying the same analysis as before, it is concluded that the network does not guarantee a bitrate of 8192 kbps, because the experimental values are lower.

When compared the graphics of bitrate at the different rate values, it can be concluded that the results of Figure 4.11 are according to expectations. However, when the rate is 1000 packets per second, it can be noticed the decrease of bitrate, especially when the MN is connected to DMAR2. Nevertheless, the bitrate value for a packet rate of 1000 pps is lower than expected during the test time. The testbed does not support a packet rate of 1000 pps if the payload size is 1024 bytes due the limitations of the wireless technology deployed on the SBCs.

The correspondent end-to-end packet delay results are illustrated in Figure 4.13 and Figure 4.14. As the packet rate increases, it can be verified the increase of the end-to-end packet delay. In fact, when comparing these results by making the matching with the respective bitrate, it can be concluded that for a high value of bitrate, the value of the delay is also high. It can be assumed that, for a 1000 packet rate, the network is overloaded and therefore it cannot guarantee the required bitrate value, and consequently, the value of end-to-end delay increases. Since the packets of Flow 3, which correspond to the packets of Session 3, are not tunnelled, the communication goes through a direct path between the MN and the CN. Consequently, a low value of delay is observed in Flow 3 (Session 3). This soft difference can be validated in the two graphics that shows the results of delay for 250 and 1000 packet per second.

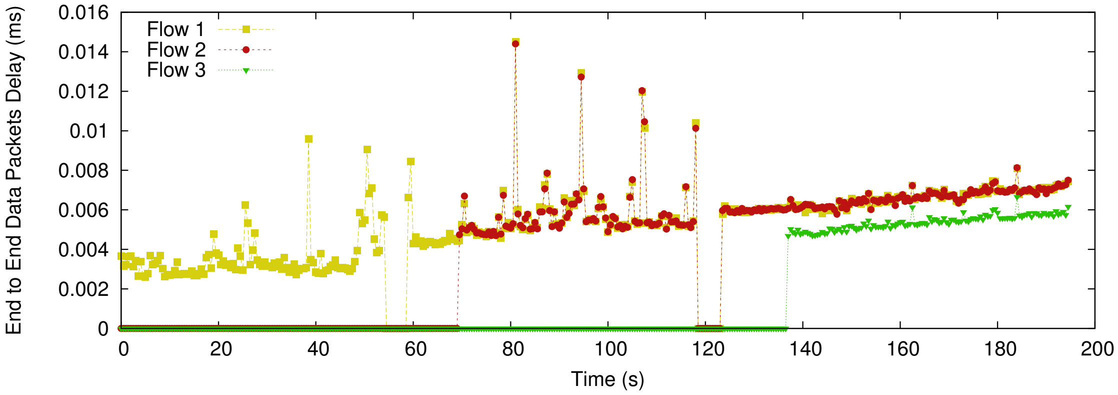

Figure 4.13: Delay at 250 packets per second.

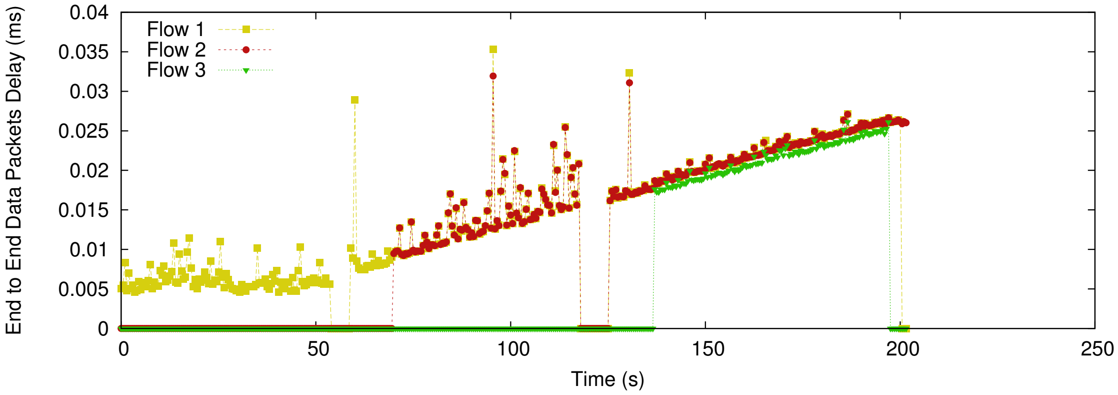

Figure 4.14: Delay at 1000 packets per second.

The results of packet loss are depicted in Figure 4.15 and 4.16. During the handover, the values of packet loss are high when the bitrate is high, which makes perfect sense. The MN sends more packets, and since there is no path to the CN, because the MN does not have network layer connectivity, the packets are lost.

Note that the handover mechanism, even being an automatic mechanism during the test, is not optimized, and for that reason, the handover time is approximately 6 seconds.

4.6.2 Testing the Limitations of the Testbed: Part 2

In addition, other tests are performed in the same scenario as before (Figure 4.1). In this specific case, it is evaluated the limitations of the testbed illustrated in Figure 4.10, by applying sessions with different parameters.

The tests are characterized into two types:

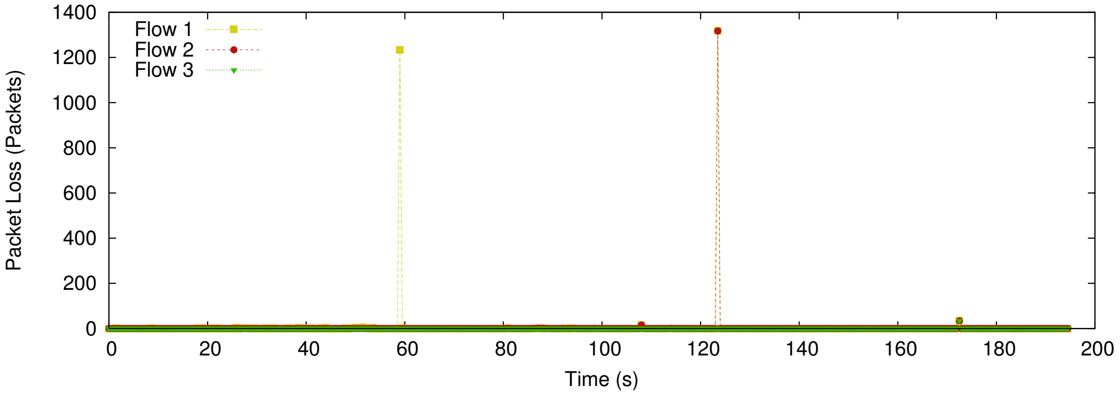

Figure 4.15: Packet Loss at 250 packets per second.

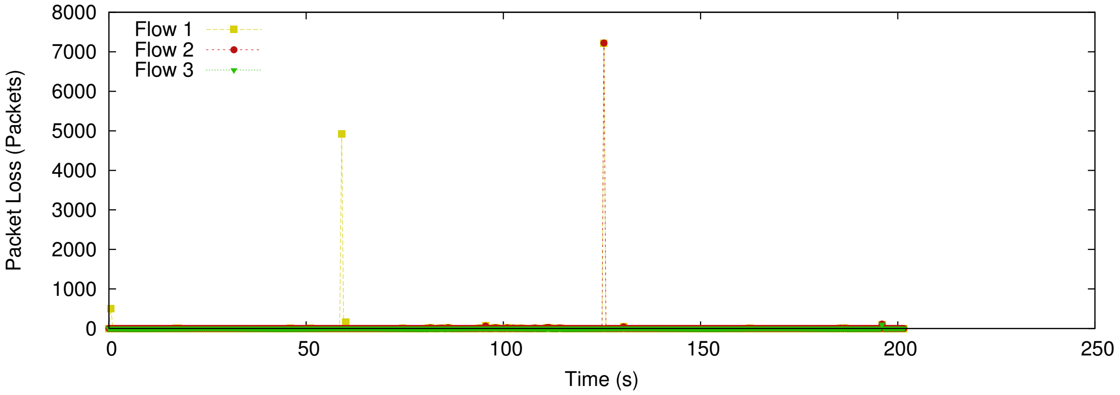

Figure 4.16: Packet Loss at 1000 packets per second.

- **Test A**: The CN initiates three sessions with the MN. Each of these sessions has a packet rate of 125 pps and the packets have a constant payload size of 1024 bytes. Session 1 starts when the MN is attached to DMAR1 (step 1), session 2 is initiated when the MN is attached to AR (step 2), and Session 3 starts when the MN is on the DMAR2 domain (step 3).

- **Test B**: The sessions can be categorized into three types: sessions that have a packet rate of 125 pps, 500 pps and 750 pps. The CN initiates one session of each type when the MN is attached to DMAR1. Then, CN initiates the three sessions when the MN is connected to the respective AR and when it is connected to DMAR2. The packets have a payload size of 1024 bytes as described before.

Note that the sessions can be UDP or TCP. In this framework, it was used these type of session separately, which means that if one session is UDP all others are UDP. This can be applied to the case of having a TCP session. The important aspect is to evaluate the impact of different sessions that have distinct characteristics, such as the type of session and packet rate.

4.6.2.1 Evaluating the UDP sessions in Test A and Test B

The following figures show the results when the sessions are UDP type. Figure 4.17 illustrates the bitrate for the Test A. Session 1 starts when the time is equal to zero. The first handover occurs at 55 seconds, then, Session 2 starts around 70 seconds. The second handover occurs at 119 seconds, and Session 3 initiates at 138 seconds.

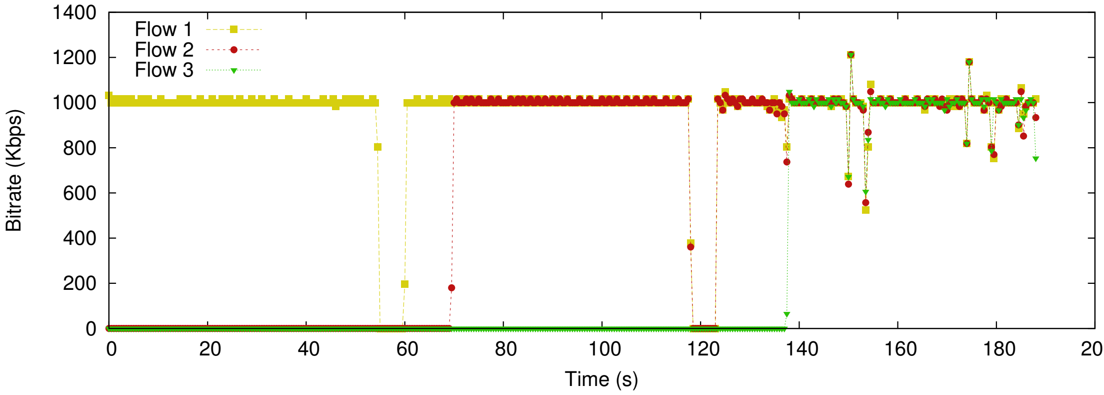

Figure 4.17: Bitrate for UDP sessions with a constant packet rate of 125 pps (Test A).

As illustrated in Figure 4.18, when the MN is attached to DMR2 (step 3), there is a bitrate crash, leading to the conclusion that the network is overloaded. To reinforce this conclusion, it is presented the graphics for the end-to-end packet delay and packet loss depicted in Figure 4.20 and Figure 4.22. In step 3, the delay is a little bit higher and, when compared with the other case, it can be concluded that it has the highest values. Thereby there is a large amount of packet loss.

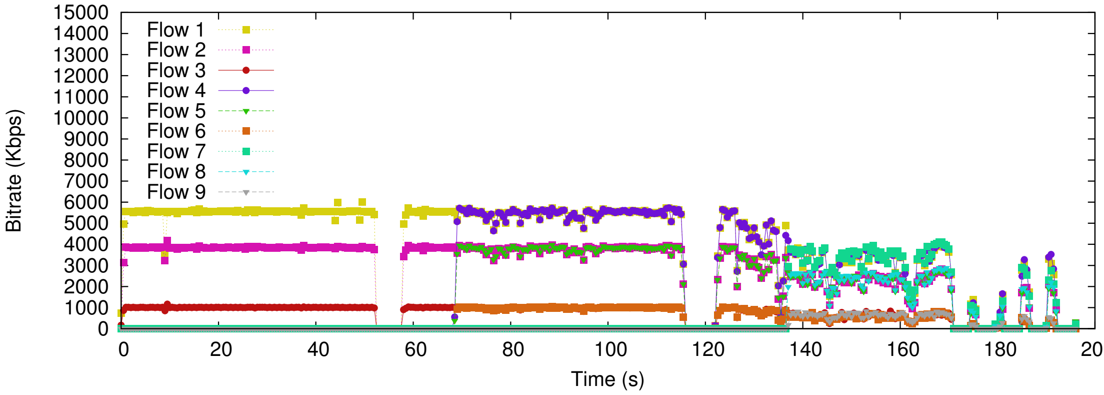

Figure 4.18: Bitrate for the UDP sessions with different packet rate (Test B).

Figure 4.19 shows the end-to-end packet delay for the Test A. In step 3, it is observed that Session 3, which corresponds to Flow 3, has a slightly lower value of delay comparing to Session 1 (Flow 1) and Session 2 (Flow 2). The reason is that data packets are not encapsulated (Session 3), therefore, the process of data packet forwarding in Session 3 is slow.

In Figure 4.20 it is observed that the value of end-to-end packet delay is higher than the values of Figure 4.19, because there is a large amount of packets in the network that cannot

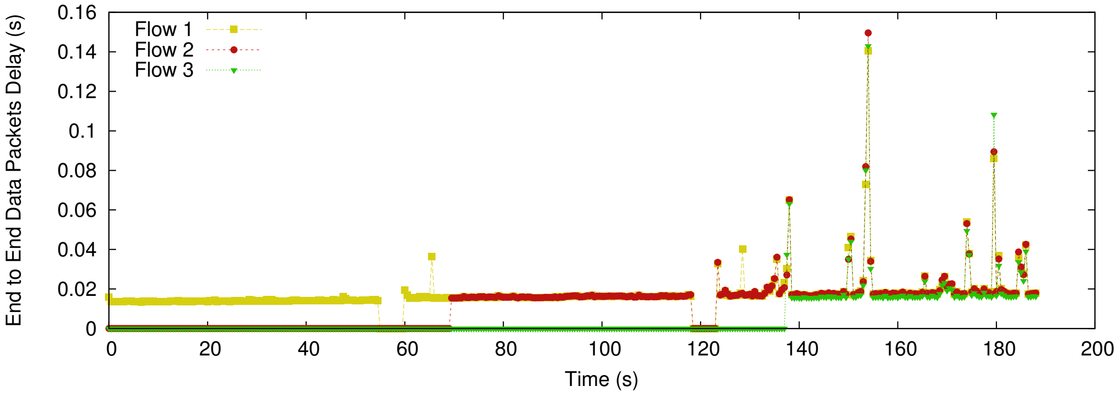

Figure 4.19: End-to-End Packet Delay for UDP sessions with a constant packet rate of 125 pps (Test A).

be supported by the testbed. As a consequence, the end-to-end packet delay is high and around 180 second the delay value is zero because the bitrate is also zero.

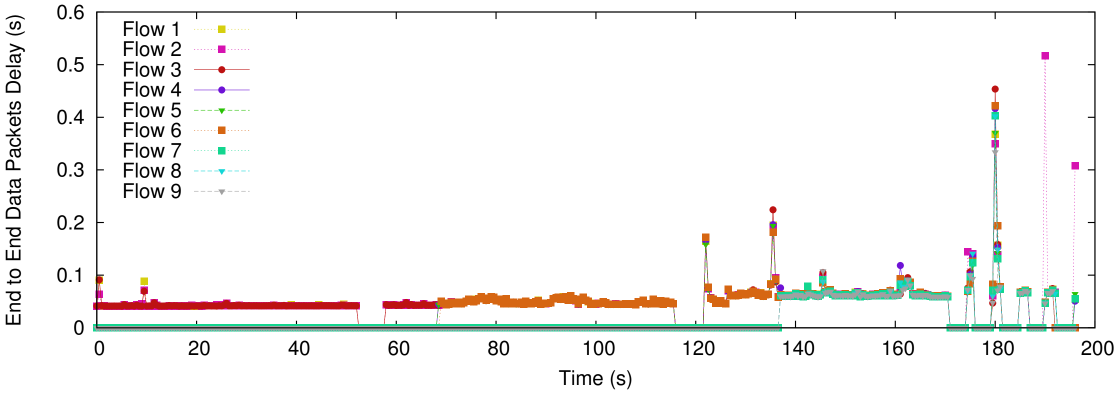

Figure 4.20: End-to-End Packet Delay for the UDP sessions with different packet rate (Test B).

Figure 4.21 and Figure 4.22 illustrate the packet loss for the Test A and Test B, respectively. As expected, there are more packets lost in the case of Test B than in the case of Test A. Indeed, the network is overloaded, and therefore, there is an increase of packet loss.

4.6.2.2 Evaluating the TCP sessions in Test A and Test B

The results of TCP sessions are similar to the results when sessions are UDP type. The bitrate experiences a decrease in step 3; however, it is not possible to conclude that there is an increase or decrease of delay because the graphics of Figure 4.25 and Figure 4.26 do not allow to see in detail. The TCP protocol uses a retransmission mechanism to ensure data delivery in the absence of any feedback from the remote data receiver. For that reason, no packets were lost during the test time.

Figure 4.23 illustrates the bitrate for the Test A using TCP session. The first handover occurs at 55 seconds, approximately; and the second handover occurs at 120 seconds. Both

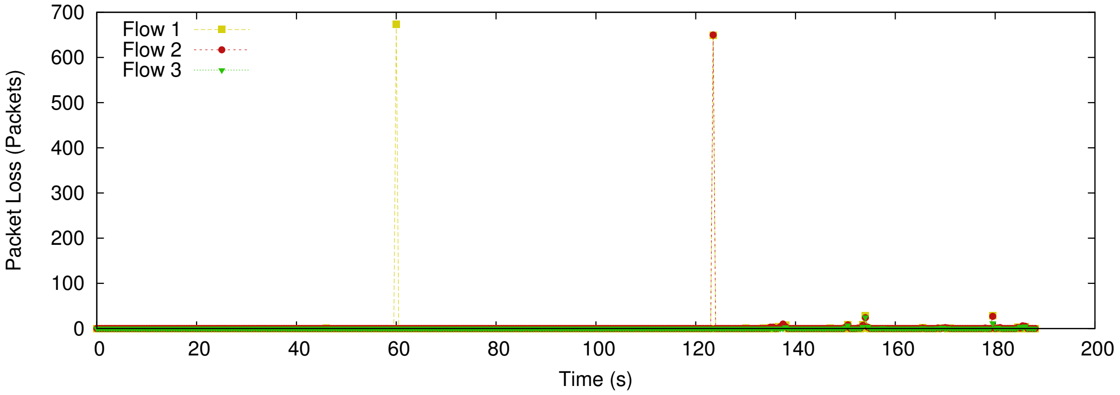

Figure 4.21: Packet Loss Results for UDP sessions with a constant packet rate of 125 pps (Test A).

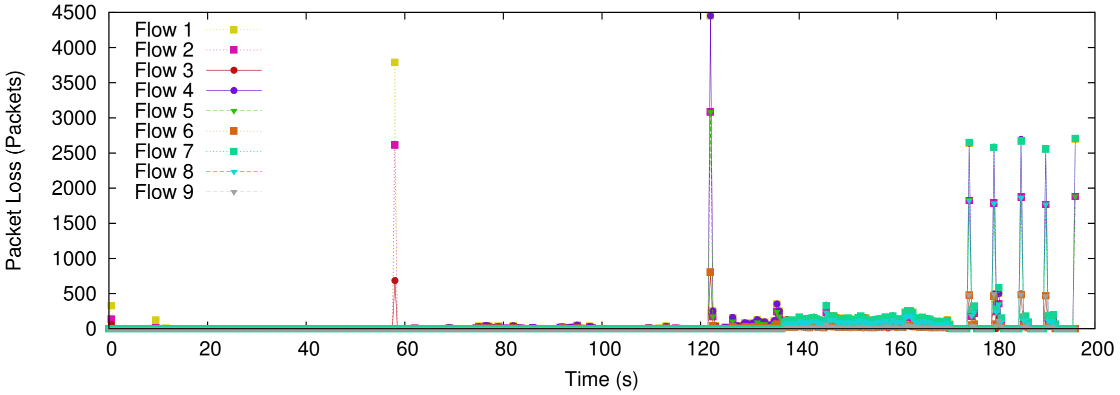

Figure 4.22: Packet Loss Results for the UDP sessions with different packet rate (Test B).

handover procedures take a long time, around 10 seconds. As it was mentioned before, the handover mechanism is not optimized and therefore, Figure 4.23 is the example of the consequence of the non-optimal handover.

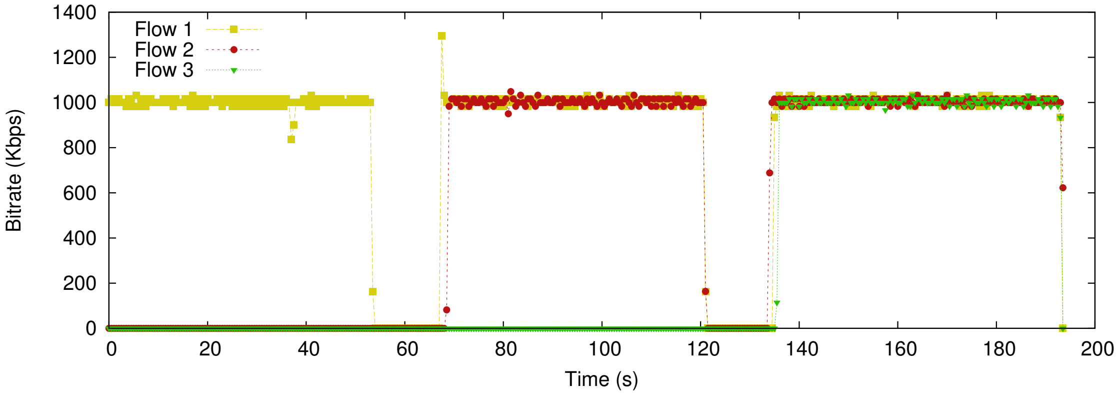

Figure 4.23: Bitrate for TCP sessions with a constant packet rate (Test A).

The bitrate for the Test B is depicted in Figure 4.24. It is observed a bitrate crash between 150 seconds and 200 seconds. It is concluded that the network is overloaded.

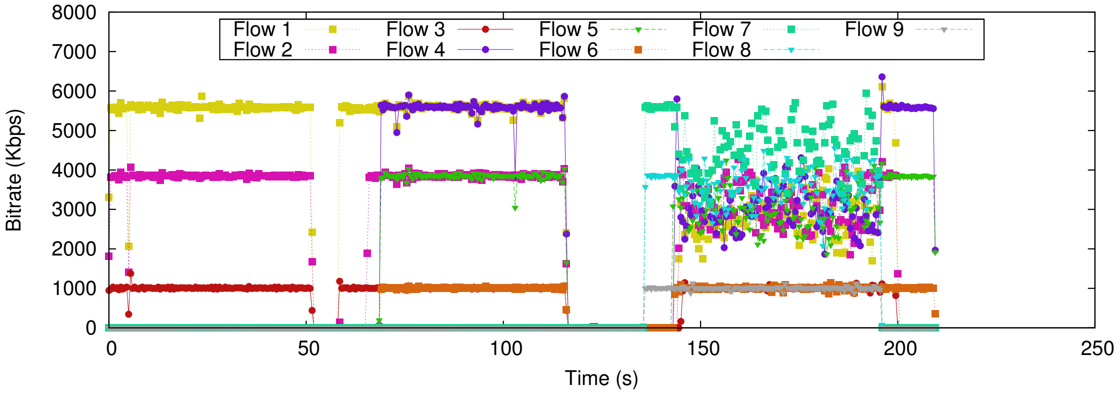

Figure 4.24: Bitrate for the TCP sessions with different packet rate (Test B).

Figure 4.25 shows the end-to-end packet delay in which it is observed a high value of delay. The reason can be related with the fact that all users inside the private IT Network share content and perform other tests. Thus, the data packets can be delayed.

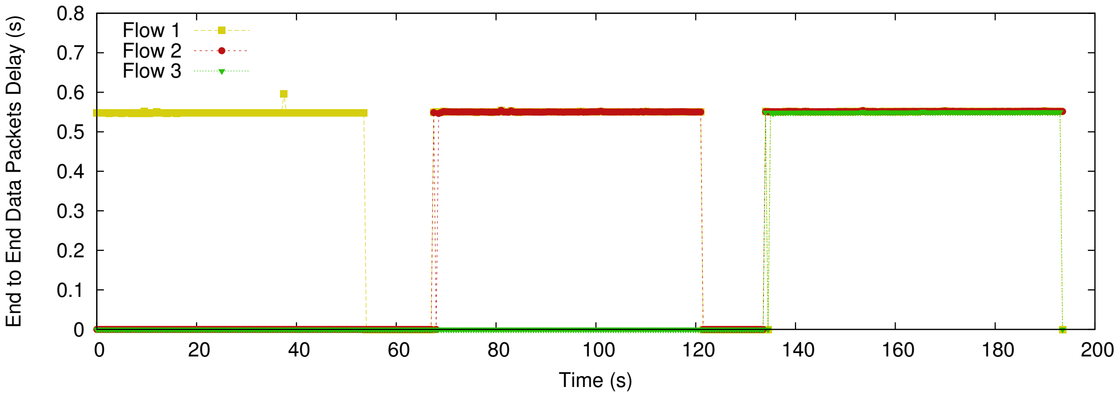

Figure 4.25: End-to-End Packet Delay for TCP sessions with a constant packet rate (Test A).

Finally, Figure 4.26 illustrates the end-to-end packet delay for the Test B, where it was initiated multiple sessions with different characteristics. The delay values are very unstable which lead to reinforce the conclusion that the network is overloaded.

In the next sections we will take into consideration the limitations of the testbed, in order to ensure the good working of the testbed and the good quality of the experiences.

4.6.3 Evaluating the performance of DMIPA with multihoming support in Scenario C

This subsection demonstrates the results obtained throughout the execution of tests in Scenario C (Figure 4.7). The first three figures illustrate the results when the sessions are of UPD type, while the last three are related to the test when TCP sessions were used. Session

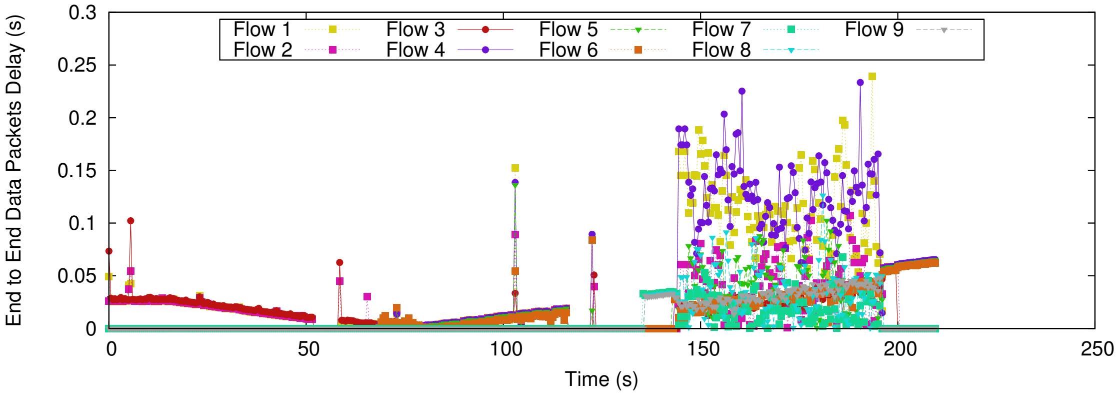

Figure 4.26: End-to-End Packet Delay for the TCP sessions with different packet rate (Test B).

1 (Flow 1) starts when the MN is connected to DMAR1, and Session 2 (Flow 2) is initiated when the MN is attached to DMAR2 via wireless interface. Then, the MN roams both sessions from the wireless interface (Intf1 - wlan1) to the wired interface (Intf 3 - eth0).

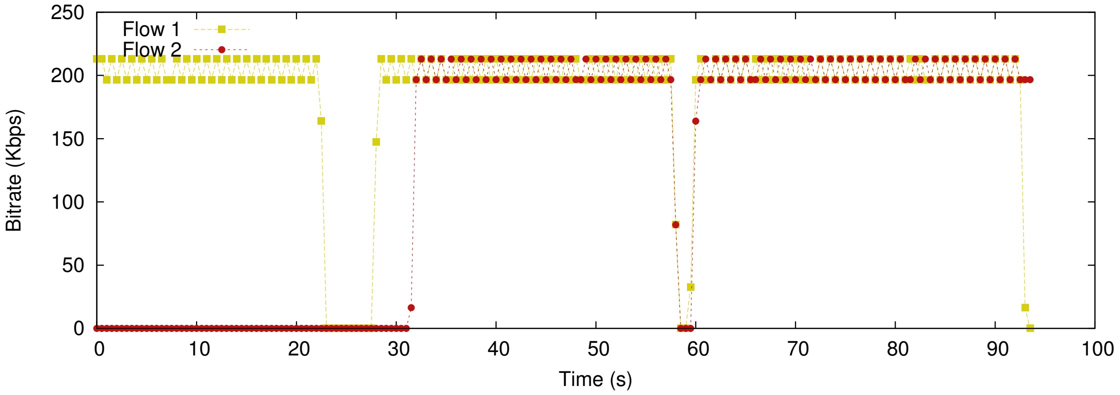

Figure 4.27: Bitrate of UDP Sessions in Scenario C.

The values of bitrate are according with expected ones. In Figure 4.27 it is observed the instant in which handovers occur.

The end-to-end packet delay decreases during the test, as shown in Figure 4.28. It is expected to see an improvement of the delay value after the MN changes the sessions from Interface 1 to the Interface 3 (wired interface). Then, it should be seen an abrupt decrease in the delay values of Session 1 and 2.

On the other hand, since the packets of Session 2 go through a direct path from the CN's wired interface to the wireless interface of MN, when Session 2 is moved from the MN's wireless interface to its wired interface, the value of delay is expected to be similar. Figure 4.28 shows that there is no significant change in the delay value of Session 2.

During the handover time, which occurs at the instants 27 and 60 seconds, it is observed a loss of data packets. When the MN changes network or interface, it does not have network connectivity and there is no way to successfully send or receive data packets. Figure 4.29 illustrates the results of packets loss.

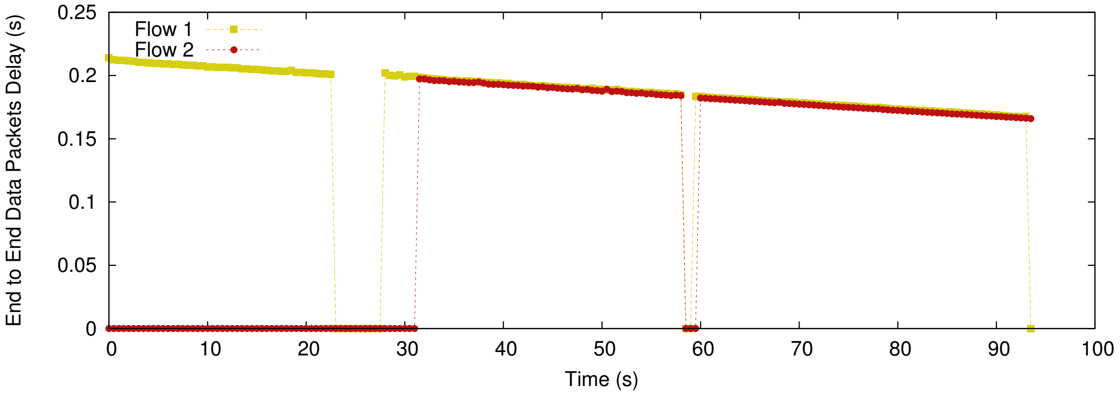

Figure 4.28: Delay of UDP Sessions in Scenario C.

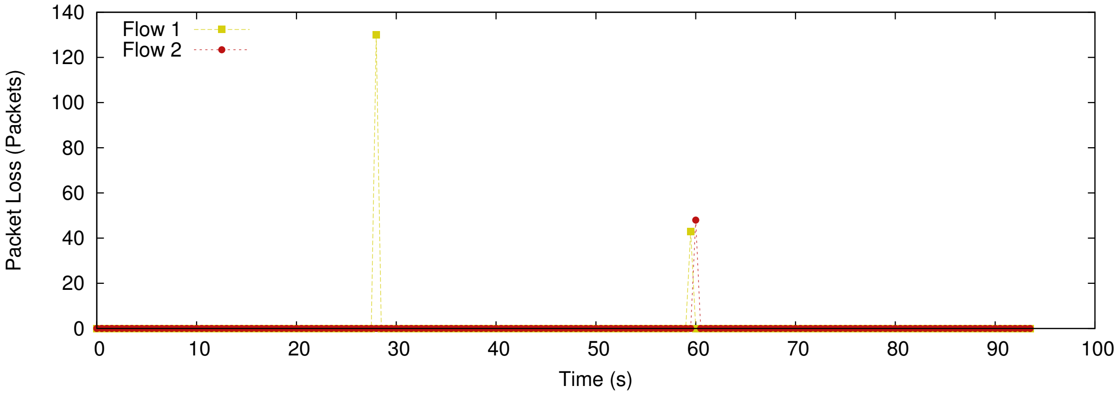

Figure 4.29: Packet Loss of UDP Sessions in Scenario C.

Figure 4.30 depicts the values of bitrate for TCP sessions, and the Figure 4.31 shows the delay during the test. There is a clearly improvement in the delay values, when the sessions are moved from the wireless interface (wlan1) to the wired interface (eth0) of the MN. Furthermore, focusing the attention on the period 60-100 seconds, the values of the end-to-end packet delay of Session 1 are higher than the values of Session 2, because the packets of Session 1 are tunnelled from DMAR1 to DMAR2, while the packets of Session 2 are sent directly.

4.6.4 Evaluating the performance of DMIPA with multihoming support in Scenario D

In this context, it is evaluated the performance of DMIPA in a multihoming scenario which is represented by Figure 4.8. Moreover, it makes a match between Scenario D and Scenario A (Figure 4.2).

Once again, it is measured the bitrate and end-to-end packet delay. Regarding the results presented earlier it was chosen a constant payload size of 1024 bytes and a packet rate of 25 packets per second. In this way, there is the guarantee that phenomenons like the bitrate crash mentioned before do not happen, which would negatively affecting the results. The next figures show the results when it is used UDP sessions.

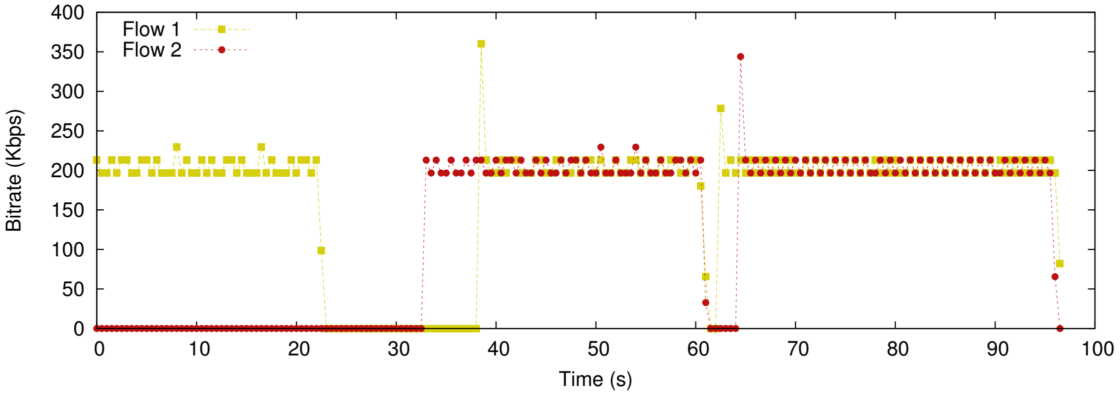

Figure 4.30: Bitrate of TCP Sessions in Scenario C.

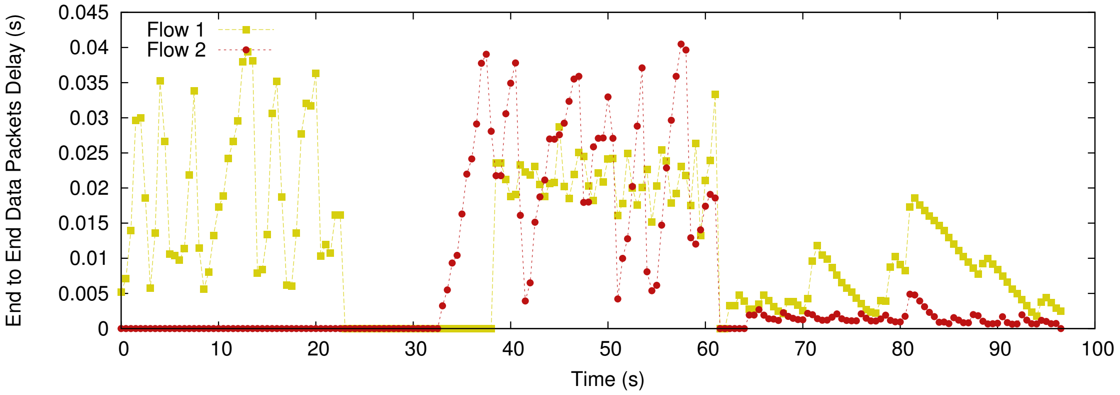

Figure 4.31: Delay of TCP Sessions in Scenario C.

Figure 4.32 and 4.33 illustrate the bitrate for the two scenarios. In both cases, the values of bitrate are according to the expected ones. Taking a close look to Figure 4.33, at the instant 82 seconds it can be notice the handover of sessions between the wireless interface (wlan0) and the wired interface (eth0).

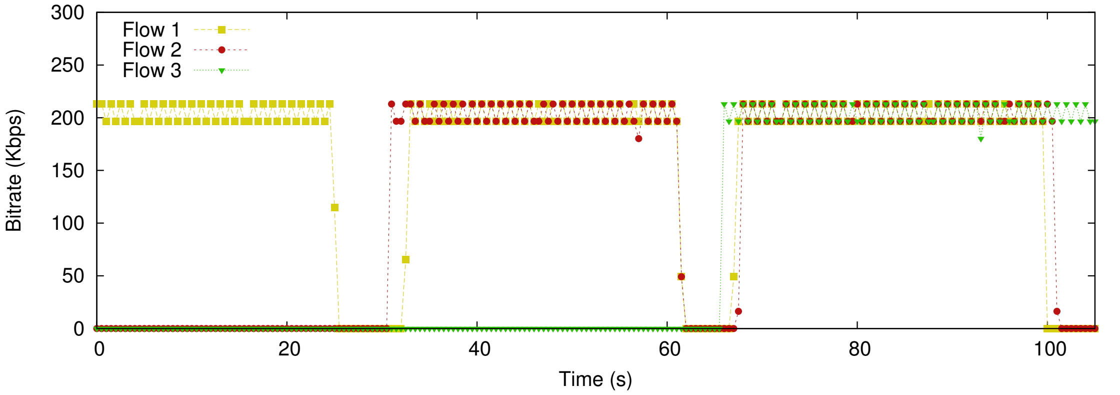

Figure 4.32: Bitrate of UDP Sessions (Reference Model - Scenario A).

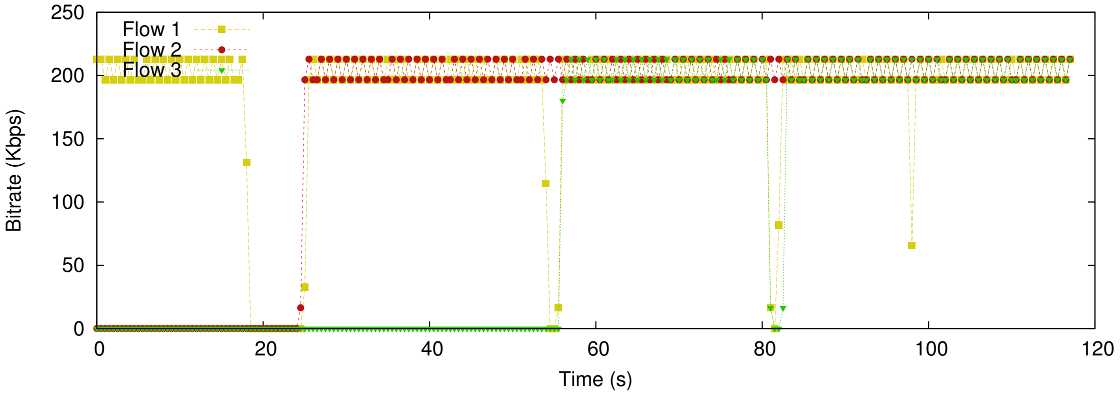

Figure 4.33: Bitrate of UDP Sessions (Matching Model - Scenario D).

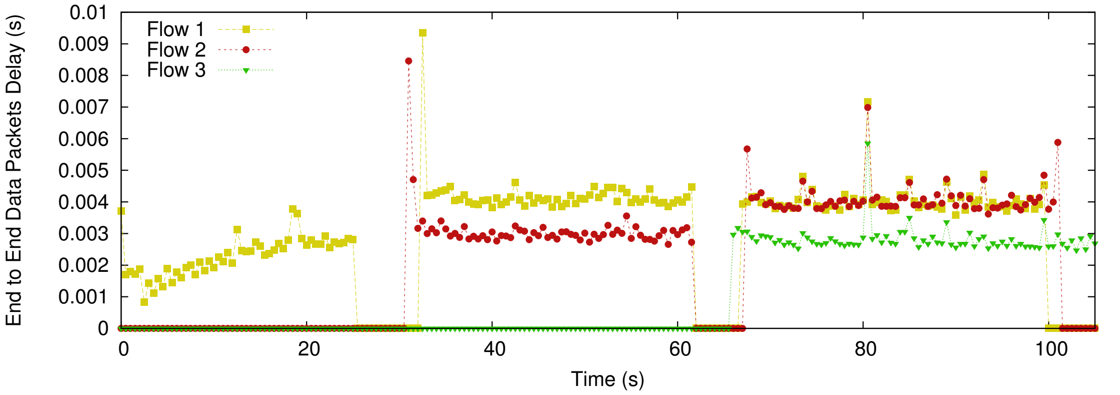

Figure 4.34: Delay of UDP Sessions (Reference Model - Scenario A).

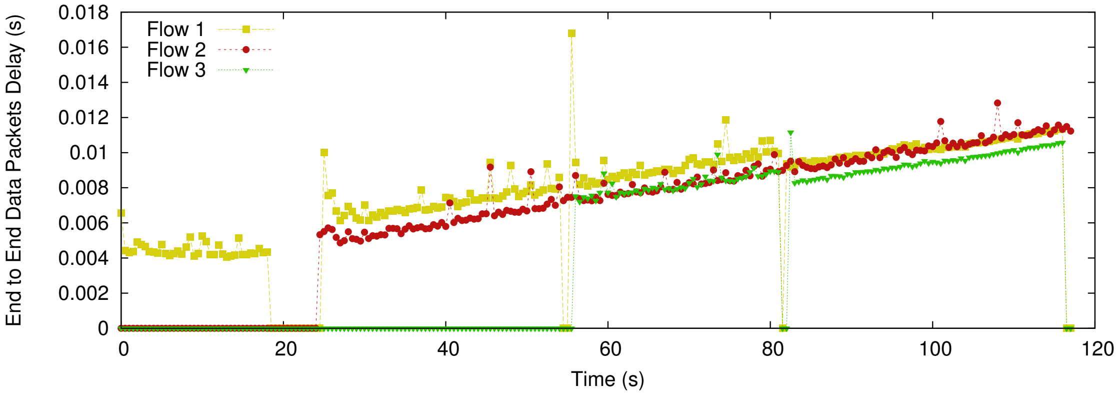

Figure 4.35: Delay of UDP Sessions (Matching Model - Scenario D).

Figure 4.34 shows the results of end-to-end delay. It can be seen an increase of the delay value of Session 1 (Flow 1), when de MN roams from the network with IP prefix P1::/64 to P2::/64. This behaviour is also verifed in the case of Session 2 (Flow 2) when the MN moves from the P2::/64 network to the domain of DMAR3 with the IP prefix of P3::/64. This increase of the delay value can be explained by the simple fact that the packets from both sessions are tunnelled from DMAR to another DMAR, which introduces a small delay to the data path. The Session 3 (Flow 3), which is initiated by the CN when the MN is attached to DMAR3, has a low delay value comparing to Session 1 and 2.

On the other hand, Figure 4.35 illustrates the results of delay for the multihoming Scenario D. Although the delay value increases during the test time for all sessions, which can be justified by a sudden change of the network usage by other users, it can be verified a decreasing of the delay value of Session 1 and Session 3 when they are moved from wlan0 interface to eth0 interface.

The same analysis can be made for the case of having TCP sessions. Figure 4.36 and 4.37 show the results of bitrate for both scenarios.

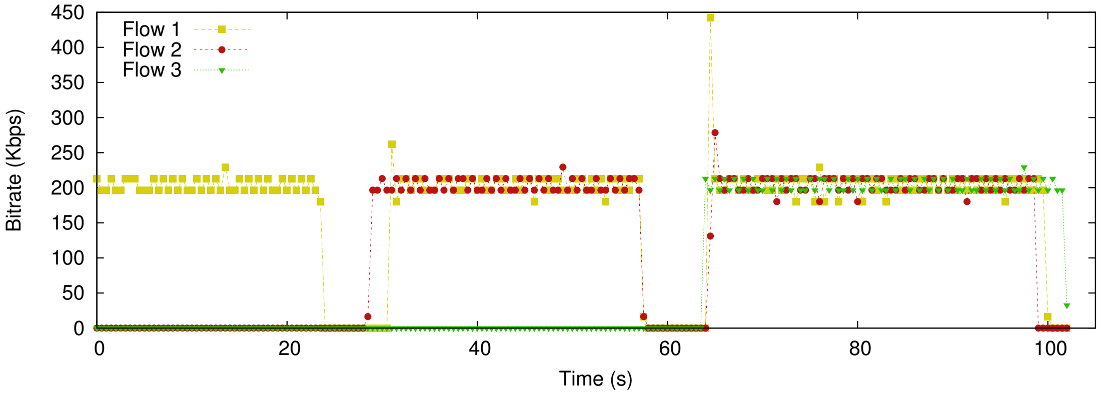

Figure 4.36: Bitrate of TCP Sessions (Reference Model - Scenario A).

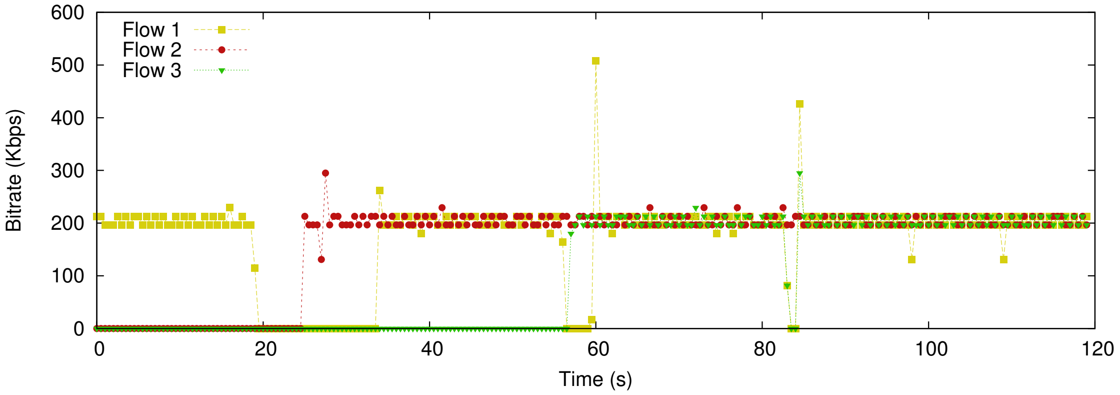

Figure 4.37: Bitrate of TCP Sessions (Matching Model - Scenario D).

Figure 4.38 illustrates the end-to-end packet delay of the test performed in Scenario A, and Figure 4.39 shows the end-to-end packet delay of the test performed in Scenario D.

The delay values experience a large variation in a wireless domain. However, as illustrated in Figure 4.39, when Session 1 and 3 are moved to the wired domain (Ethernet), the values become more stable and lower than before. The delay value of Session 1 is smoothly higher than the delay value of Session 3 because the packets belonging to Session 1 are tunnelled.

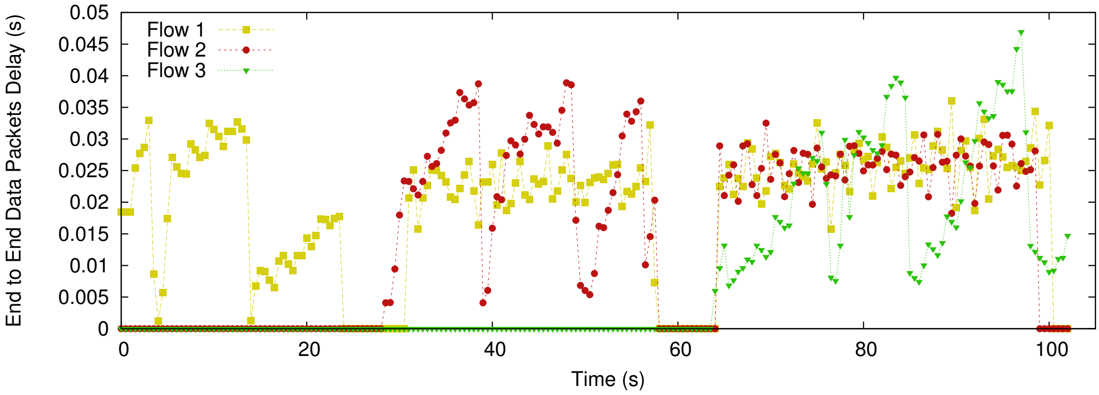

Figure 4.38: Delay of TCP Sessions (Reference Model - Scenario A).

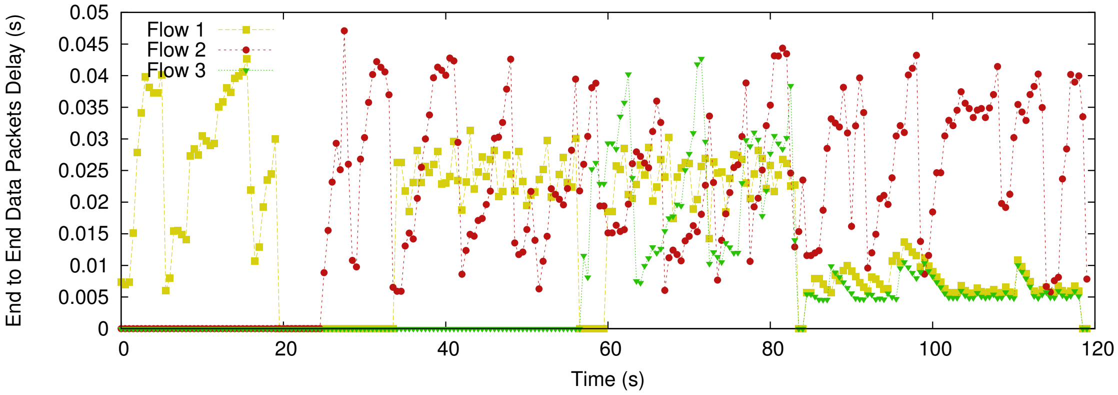

Figure 4.39: Delay of TCP Sessions (Matching Model - Scenario D).

4.6.5 Evaluating the performance of DMIPA with multihoming support in Scenario E

This subsection presents the results of the experiments performed in the context of Scenario E (Figure 4.9). Like in section 4.6.4, it is making a comparison between the results obtained in Scenario B (Figure 4.3) with the ones obtained in Scenario D.

The payload size is 1024 bytes and the packet rate is 25 packets per second. The Session 1 (Flow 1) is initiated when the MN is attached to DMAR1, and Session 2 (Flow 2) when the MN is attached to DMAR2.

The following Figures illustrate the results using TCP sessions. The bitrate is illustrated in Figure 4.40 and Figure 4.41. They are correct according with parameters that characterize the sessions. Focusing on Figure 4.41, at 97 seconds it can be observed the handover between interfaces.

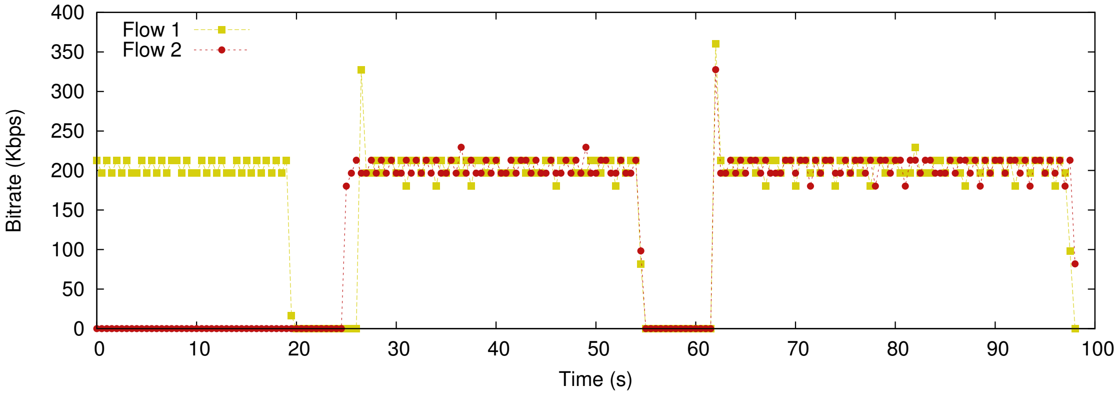

Figure 4.40: Bitrate of TCP Sessions (Reference Model - Scenario B).

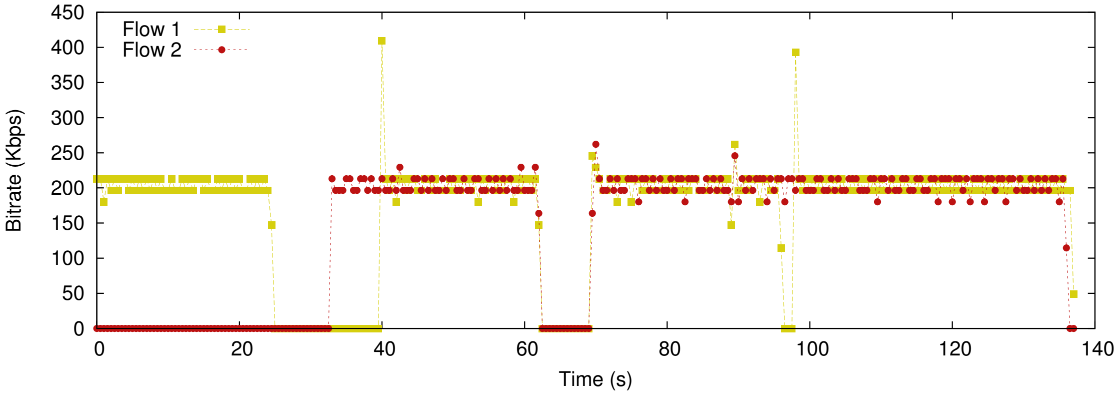

Figure 4.41: Bitrate of TCP Sessions (Matching Model - scenario E).

The end-to-end delay shown in Figure 4.42 and Figure 4.43 has a significant fluctuation.

Figure 4.43 illustrate the delay for the multihoming Scenario E. There is a constant decrease of the delay value. Besides this behaviour, it can be notice an increase of the delay value of Session 1 (Flow 1) at the instant 99 seconds that was caused by an increase of the traffic in the network. This time, the change of interface does not improve the delay values of Session 1.

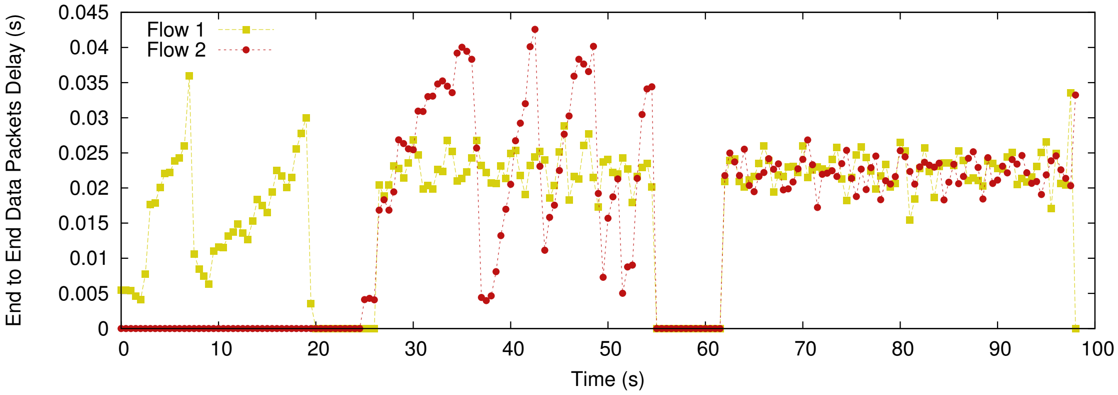

Figure 4.42: Delay of TCP Sessions (Reference Model - Scenario B).

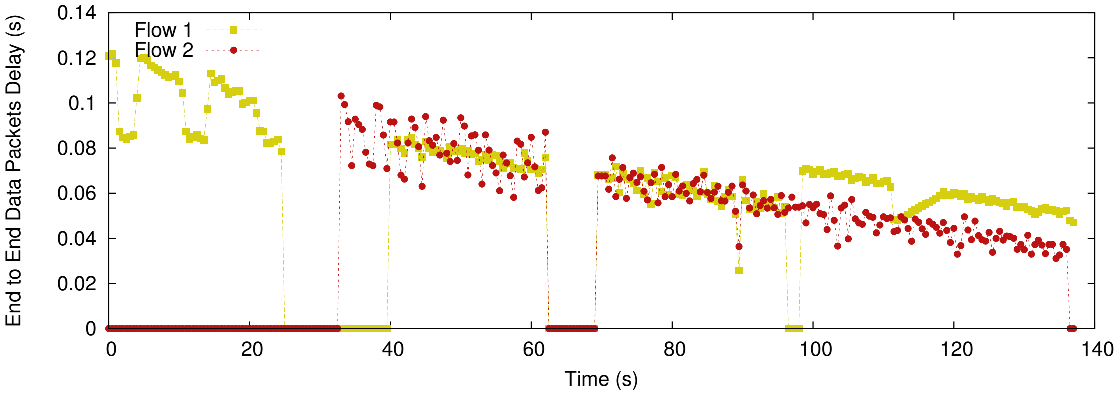

Figure 4.43: Delay of TCP Sessions (Matching Model - Scenario E).

4.7 Challenges

During the tests it was found several problems that have limited the execution of the tests mentioned on the above section.

One of the the main problems, which is also frequent when it is aimed to study the performance of the networks, is the constant change of the data traffic in the core network. In fact, the IT Aveiro network is a network which is used by other users to study and perform tests, and therefore, in some instants the network can be overloaded, or some core routers can be congested which result in the increase of the packet delay and more packet losses.

The use of the IT Aveiro network as a core network rises other issues. Since the IT Aveiro network is a local domain, the distance between DMARs is short, and consequently, the effects of tunnelling, such as the increase of delay value, are minimal.

The MN is an Asus Eee PC mobile computer, and due its low processing power, the mechanism of attaching to the SBCs becomes slower, resulting in a higher handover time.

In terms of software, the issue faced during the test was the clock synchronization. For the purpose it was used the PTPd application, but since the MN is constantly changing of network/interface domain, there is a lack of synchronization packets when handovers occur. So, the PTPd requires a recovery time to set both clock with the same value.

Nevertheless, some of the negative effects caused by the above issues were minimized. In order to minimize the impact of the high data traffic and possible congestions, the tests were performed in a period of the day that data traffic were more constant and with a low value. The PTPd was initiated in advance before testing each case. The other issues cannot be solved because they are intrinsic to available resources such as hardware and network.

4.8 Overall Discussion, Analysis and Conclusions

Along this chapter, it was implemented a real testbed and evaluated several scenarios to evolve a distribute mobility mechanism to provide session continuity in multihomed environments.

First of all, it was described the most relevant multihoming scenarios and the mobility scheme required to provide session continuity when the MN changes of network domain using the same technology/interface or a different one. Then, it was given a detailed explanation about the elements that integrate the testbed.

By allowing the access routers (SBCs) and the mobile node (laptop) with the required mobility management functions, it was possible to test DMIPA without multihoming support in a real environment. Furthermore, it was concluded that the testbed has its own limitations; therefore, it is important to choose reasonable parameters for the sessions in order to avoid bitrate crashes which will negatively affect the results. Thus, it was proved the proper operation of DMIPA in a real environment.

Finally, the multihoming use-case scenarios were validated in the real testbed and some analysis was made throughout session 4.6. The measurements indicate that user experience is improved when DMIPA takes advantage of multihomed mechanism. In some of the cases, it is possible to observe a decrease of the delay value. Even if some packets are lost and the delay value has the same average value, the multihoming scenario is still a better solution than the reference model, because it can ensure session continuity if a down link event occurs. This cannot be possible if the MN uses only one interface.

However, in some cases the delay value increases, thus, not all changes of interface in which the sessions are anchored have a better path.

Finally, service providers are implementing selective traffic offload strategies through the wireless local area network, where session continuity shall be guaranteed, which can be deployed through the distributed mobility solution for multihomed scenarios.

Chapter 5

Conclusion and Future Work

5.1 Conclusions

The networks are moving towards flat architectures; therefore, there is the requirement of dynamically distributing the mobility management among the elements of the network. So, the distributed and dynamic mobility management theme triggered the interest in the research community, specially in the problem statement and the definition of a framework. Moreover, distributed mobility management has been growing as a promising approach in the evolution of the network architectures and mobile data traffic. DMIPA is a new host-based approach which distributes the mobility management functionalities among the ARs and the MNs.

The aim of this dissertation was to study and to evaluate the impact of the new proposal based on the host that aims to provide distributed mobility management in a flat and heterogeneous networks, named DMIPA, and compare it with the centralized mobility management protocol, called MIPv6. We used vehicular and dynamic environments to evaluate the performance of those protocols and the impact that they will bring when deployed in such scenarios. For the purpose, we used three different scenarios, which it was performed simulations according to the vehicles' speed and to the number of vehicles. In addition, it was validated a distributed mobility management scheme for multihomed scenarios in order to ensure session continuity when the user roams between networks from the same or different technologies, using the same or different interfaces.

From the results shown in Chapter 3, we can take the following conclusions:

- In the Short Highway scenario, DMIPA provides low values of signalling cost, data cost, average data delay and binding update time. However, when the MNs move fast, which means that the relative speed is high, the results are similar to those obtained in MIPv6. Thus, for high speeds, a distributed mobility management scheme does not improve the mobility management.

- The number of DMARs was evaluated through the Long Highway scenario. When comparing the cases, we concluded that the best results are achieved when 5 DMARs are used. In opposite, the use of 9 DMARs decreases the performance of DMIPA.

- When testing DMIPA in the City scenario, we concluded that using 3 or 5 DMARs optimizes the overall performance of the protocol.

- Contrasting DMIPA against MIPv6, in the same scenario as the topic above, we concluded that DMIPA with 4 DMARs reduces the values of signalling cost, data cost, data loss, average data delay and binding update time.

It can be concluded that DMIPA improves the mobility management overall performance when compared with MIPv6 for dynamic vehicular environments. Therefore, we will opt for DMIPA to deploy a mobility management protocol in vehicular environments.

Despite the advances in distributing mobility management, it was described and evaluated a distributed mobility management for multihoming scenarios, with multiple interface' devices. There are several different cases in the users' daily routine, where the users' devices are connected through multiple and distinct interfaces at the same time. In this context, DMIPA with multihoming support should be able to provide session continuity, moving session between interfaces/networks.

The results performed in the real testbed demonstrate that:

- Regarding end-to-end packet delay, the DMIPA protocol with multihoming support provides lower values when compared with the legacy DMIPA.
- The results of packet loss have shown that DMIPA with multihoming support has a higher value than the legacy DMIPA; however, the first mechanism provides session continuity while it reduces the networks cost and improve the user experience.

Nevertheless, there must be an intelligent management scheme to deal with the change of session between networks/interfaces in order to improve QoS/QoE. In fact, some results show that, changing the sessions from one interface to another may result in higher delay values. Then, we can assume that such change is not desirable. To avoid this issue, the creation of a high level scheme to provide the best solution in mobility management mechanism with multihoming support is required.

5.2 Future Work

As future work, it is proposed to study the most recent evolution in vehicular networks, the communications between MNs and its applications.

As a first step towards the evaluation of DMIPA in real vehicular environments, it is essential to implement DMIPA on the available testbed of Figure 4.10. It is proposed the following tasks:

- Improve the implementation of DMIPA in the tesbed of Figure 4.10 and measure the performance in laboratory;
- Test DMIPA in a real and dynamic vehicular scenario, using the use-case scenarios described in section 4.2.1.

Moreover, it is essential to analyse the performance of DMIPA with the current protocols, per example MIPv6 and/or PMIPv6, in order to compare the improvements in such environments.

Also, it is proposed to improve the DMIPA with multihoming support on the testbed of Figure 4.10. In this context, two areas of study are proposed:

- The first one focuses its efforts in optimizing the handover mechanism by providing to the mobility management functionalities in multihoming scenarios with the proper implementation of the multihoming procedure, reducing the handover time.
- The second one is related with the creation of a high level mechanism that manages the procedures in multihoming scenarios. This means that it is required an element that manages, controls and decides when the MN should roam the session to another network/technology. The goal is to choose always for the best resources to improve the QoS and QoE.

Our research group have implemented a real-world testbed, in which taxis and buses are equipped with multi-network communication devices, supporting both vehicle-to-vehicle and vehicle-to-infrastructure communication. Then, for an ultimate evaluation, it is required to integrate DMIPA with multihoming support in these communication devices.

Bibliography

[1] H. Moustafa and Y. Zhang, *Vehicular Networks: Techniques, Standards, and Applications*, 1st ed. Boston, MA, USA: Auerbach Publications, 2009.

[2] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2012-2017," Cisco, White Paper, Feb. 2013.

[3] D. W. Group. (2013, October) Distributed mobility management wg.

[4] T. Condeixa, J. Carvalho, and S. S., "Dynamic offload anchoring with ip mobility," in *Mobile Network and Applications (MONET)*, Nov. 2013.

[5] J. Carvalho, C. T., and S. S., "Distributed mobility management in dynamic environments: V2i networks," in *IEEE ICC*, Nov. 2013.

[6] C. E. Perkins, A. F. Myles, and T. Watson, "Mobile ip," *IEEE Communications Magazine*, vol. 35, pp. 84–99, 1992.

[7] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the internet," *Commun. Surveys Tuts.*, vol. 8, no. 1, pp. 38–51, Jan. 2006. [Online]. Available: http://dx.doi.org/10.1109/COMST.2006.323441

[8] L. Budzisz, R. Ferrs, A. Brunstrom, K.-J. Grinnemo, R. Fracchia, G. Galante, and F. Casadevall, "Towards transport-layer mobility: Evolution of sctp multihoming." *Computer Communications*, vol. 31, no. 5, pp. 980–998, 2008. [Online]. Available: http://dblp.uni-trier.de/db/journals/comcom/comcom31.html#BudziszFBGFGC08

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), Internet Engineering Task Force, June 2002, updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621. [Online]. Available: http://www.ietf.org/rfc/rfc3261.txt

[10] J. Rosenberg, H. Schulzrinne, and G. Camarillo, "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)," RFC 4168 (Proposed Standard), Internet Engineering Task Force, October 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4168.txt

[11] E. Wedlund and H. Schulzrinne, "Mobility support using sip." in *WOWMOM*, 1999, pp. 76–82. [Online]. Available: http://dblp.uni-trier.de/db/conf/wowmom/wowmom1999.html#WedlundS99

[12] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson, “Stream Control Transmission Protocol,” RFC 2960 (Proposed Standard), Internet Engineering Task Force, October 2000, obsoleted by RFC 4960, updated by RFC 3309. [Online]. Available: http://www.ietf.org/rfc/rfc2960.txt

[13] W. Xing, H. Karl, A. Wolisz, and H. Müller, “M-SCTP: Design and prototypical implementation of an end-to-end mobility concept,” in *Proc. 5th Intl. Workshop The Internet Challenge: Technology and Applications*, Berlin, Germany, Oct. 2002.

[14] C. Perkins, “IP Mobility Support for IPv4, Revised,” RFC 5944 (Proposed Standard), Internet Engineering Task Force, Nov. 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5944.txt

[15] C. Perkinsa and D. B. Johnson, “Route Optimization in Mobile IP,” IETF, Individual Submission, Internet Draft Version 10, Nov. 2000, draft-ietf-mobileip-optim-10.txt. [Online]. Available: http://tools.ietf.org/html/draft-ietf-mobileip-optim-10

[16] C. Perkins, D. Johnson, and J. Arkko, “Mobility Support in IPv6,” RFC 6275 (Proposed Standard), Internet Engineering Task Force, Jul. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6275.txt

[17] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460 (Draft Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946. [Online]. Available: http://www.ietf.org/rfc/rfc2460.txt

[18] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” RFC 4861 (Draft Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 5942, 6980. [Online]. Available: http://www.ietf.org/rfc/rfc4861.txt

[19] S. Thomson, T. Narten, and T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” RFC 4862 (Draft Standard), Internet Engineering Task Force, Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4862.txt

[20] R. Koodli, “Fast Handovers for Mobile IPv6,” RFC 4068 (Experimental), Internet Engineering Task Force, Jul. 2005, obsoleted by RFC 5268. [Online]. Available: http://www.ietf.org/rfc/rfc4068.txt

[21] N. Kara, “Mobility management approaches for mobile ip networks: Performance comparison and use recommendations,” *IEEE Transactions on Mobile Computing*, vol. 8, no. 10, pp. 1312–1325, 2009.

[22] 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. [Online]. Available: http://doi.acm.org/10.1145/965732.965736

[23] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” RFC 4140 (Experimental), Internet Engineering Task Force, Aug. 2005, obsoleted by RFC 5380. [Online]. Available: http://www.ietf.org/rfc/rfc4140.txt

[24] J. Kempf, "Problem Statement for Network-Based Localized Mobility Management (NETLMM)," RFC 4830 (Informational), Internet Engineering Task Force, Apr. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4830.txt

[25] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFC 6543. [Online]. Available: http://www.ietf.org/rfc/rfc5213.txt

[26] J. Kempf, "Goals for Network-Based Localized Mobility Management (NETLMM)," RFC 4831 (Informational), Internet Engineering Task Force, April 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4831.txt

[27] P. Seite and P. Bertin, "Distributed mobility anchoring," IETF, Internet-Draft draft-seite-dmm-dma-06.txt, January 2013, work in progress.

[28] T. Condeixa and S. Sargento, "Dynamic mobile ip anchoring," in *IEEE ICC*, Jun. 2013.

[29] P. Bertin, S. Bonjour, and J.-M. Bonnin, "A distributed dynamic mobility management scheme designed for flat ip architectures." in *NTMS*, A. Aggarwal, M. Badra, and F. Massacci, Eds. IEEE, 2008, pp. 1–5. [Online]. Available: http://dblp.uni-trier.de/db/conf/ntms/ntms2008.html#BertinBB08

[30] I.-T. R. Y.2011, "General principles and general reference model for next generation networks," ITU-T, Recommendation, October 2004.

[31] "Ieee standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1," *IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004)*, pp. 01–822, 2006.

[32] D. J. S. Amit Kumar, Dr. Yunfei Liu and Divya, "Evolution of mobile wireless communication networks: 1g to 4g," vol. 1, pp. 68–72, 2010. [Online]. Available: http://www.iject.org/pdf/amit.pdf

[33] A. Ghosh, J. Zhang, J. G. Andrews, and R. Muhamed, *Fundamentals of LTE*, 1st ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.

[34] R. Kuntz, J. Montavont, and T. Nol, "Multihoming in ipv6 mobile networks: progress, challenges, and solutions." *IEEE Communications Magazine*, vol. 51, no. 1, pp. 128–135, 2013. [Online]. Available: http://dblp.uni-trier.de/db/journals/cm/cm51.html#KuntzMN13

[35] M. Blanchet and P. Seite, "Multiple interfaces and provisioning domains problem statement," IETF, Internet-Draft draft-ietf-mif-problem-statement-15.txt, May 2011, work in progress.

[36] T. E. C. N. N. Montavont, R. Wakikawa and K. Kuladinithi, "Analysis of multihoming in mobile ipv6," IETF, Internet-Draft draft-montavont-mobileip-multihoming-pb-statement-05.txt, October 2005, work in progress.

[37] M. Jeyatharan and C. Ng, “Multihoming problem statement in netlmm,” IETF, Internet-Draft draft-jeyatharan-netext-multihoming-ps-02, March 2010, informational.

[38] C. to Car Communication Consortium. (2013, September) Mission and objectives. [Online]. Available: http://www.car-to-car.org/

[39] X. Zeng, R. Bagrodia, and M. Gerla, “GloMoSim: A Library for Parallel Simulation of Large-Scale Wireless Networks,” in *Workshop on Parallel and Distributed Simulation*, 1998, pp. 154–161. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.48.4634

[40] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, “Advances in network simulation,” *Computer*, vol. 33, no. 5, pp. 59–67, 2000.

[41] S. N. Technologies. (2013, September) Qualnet simulation software. [Online]. Available: http://web.scalable-networks.com/content/qualnet

[42] Riverbed. (2013, September) Opnet modeler software. [Online]. Available: http://www.riverbed.com/products-solutions/products/network-planning-simulation/Network-Simulation.html

[43] NS-3. (2013, September) Ns-3.14. [Online]. Available: http://www.nsnam.org/ns-3-14/documentation

[44] A. Halati, H. Lieu, and S. Walker, “CORSIM-corridor traffic simulation model,” in *Proceedings of the Traffic Congestion and Traffic Safety in the 21st Century Conference*, 1997, pp. 570–576.

[45] J. Härri, F. Filali, C. Bonnet, and M. Fiore, “Vanetmobisim: generating realistic mobility patterns for vanets,” in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, ser. VANET ’06. New York, NY, USA: ACM, 2006, pp. 96–97. [Online]. Available: http://doi.acm.org/10.1145/1161064.1161084

[46] D. Krajzewicz, M. Bonert, and P. Wagner, “The open source traffic simulation package SUMO,” *RoboCup 2006 Infrastructure Simulation Competition*, 2006.

[47] P. America. (2013, September) Vissim traffic simulation software. [Online]. Available: http://vision-traffic.ptvgroup.com/en-us/products/ptv-vissim/

[48] O. developer team. (2013, September) Openwrt wireless freedom. [Online]. Available: https://openwrt.org/

[49] A. Botta, A. Dainotti, and A. Pescapè, “A tool for the generation of realistic network workload for emerging networking scenarios,” *Computer Networks*, vol. 56, no. 15, pp. 3531–3547, 2012.

[50] P. Project. (2013, September) Ptpd. Http://ptpd.sourceforge.net/.