
**UNIVERSIDAD CARLOS III DE MADRID**

**DEPARTAMENTO DE INGENIERÍA TELEMÁTICA**

TESIS DOCTORAL

# OPTIMIZACIÓN DE RUTAS PARA REDES MÓVILES EN ENTORNOS IPv6 HETEROGÉNEOS

Autor: **Carlos Jesús Bernardos Cano**
Ingeniero de Telecomunicación

Directora: **María Calderón Pastor**
Doctora Ingeniera Informática

Leganés, Septiembre de 2006


**UNIVERSIDAD CARLOS III DE MADRID**

**DEPARTMENT OF TELEMATICS ENGINEERING**

PhD THESIS

# ROUTE OPTIMISATION FOR MOBILE NETWORKS IN IPv6 HETEROGENEOUS ENVIRONMENTS

Author: **Carlos Jesús Bernardos Cano, MsC**

Supervisor: **María Calderón Pastor, PhD**

Leganés, September 2006

# OPTIMIZACIÓN DE RUTAS PARA REDES MÓVILES EN ENTORNOS IPv6 HETEROGÉNEOS

## ROUTE OPTIMISATION FOR MOBILE NETWORKS IN IPv6 HETEROGENEOUS ENVIRONMENTS

**Autor:** Carlos Jesús Bernardos Cano
**Directora:** Prof. Dra. María Calderón Pastor

Tribunal nombrado por el Mgfco. y Excmo. Sr. Rector de la Universidad Carlos III de Madrid, el día ___ de _____ de _____.

Firma del tribunal calificador:

Firma:

Presidente:

Vocal:

Vocal:

Vocal:

Secretario:

Calificación:

Leganés, ___ de _____ de _____.

A mis padres, José Luis y Elena,
y a mi hermano, Josete,
sin los cuales me habría sido
imposible llegar hasta aquí.

A veces nuestro destino semeja un árbol frutal en invierno.
¿Quién pensaría que esas ramas reverdecerán y florecerán?
Mas esperamos que así sea, y sabemos que así será.

La originalidad no consiste en decir cosas nuevas,
sino en decirlas como si nunca hubiesen sido dichas por otro.

– Johann Wolfang Von Goethe (1749-1832)

# Agradecimientos

No puedo empezar de otra manera que agradeciendo a mis padres, José Luis y Elena, y a mi hermano, Josete, la dedicación y esfuerzo que me han dedicado siempre. Es imposible expresar con palabras en este espacio lo que les quiero y lo que les agradezco que siempre hayan estado ahí, aunque no sepa demostrarlo como ellos se merecen en el día a día. Tampoco puedo olvidar a mi cuñada, Cris, la cual ha hecho posible que tenga un sobrino maravilloso al que espero ver crecer rodeado de tanta felicidad y con la misma ilusión por las cosas que lo hice yo. Espero poder contribuir para que así sea.

Esta tesis no hubiera sido posible sin la inestimable ayuda de dos personas fundamentales: Ignacio Soto y María Calderón. Ambos me han demostrado una generosidad con su tiempo y conocimientos que es imposible de describir. Debo darle mis más sinceras gracias a María, por haberme guiado de la mejor manera posible, y por conseguir que mantuviera siempre una ilusión y confianza enorme en el trabajo que hacía.

El destino ha querido que concluyamos a la vez esta etapa. No se me ocurre nadie mejor para ello. Gracias Pablo, por todos los buenos que ratos pasamos diariamente. Espero que nos queden muchos más.

La inmensa mayoría de las aportaciones realizadas en esta tesis – si no todas – han sido fruto colectivo del grupo de trabajo que cariñosamente denominamos *"NEMO"*: María Calderón, Ignacio Soto, Marcelo Bagnulo, y el *'main developer'*: Antonio de la Oliva. No puedo imaginarme una manera más enriquecedora, agradable, fructífera y divertida de trabajar. ¡Gracias por dejarme formar parte del mismo! Debo también agradecerle sinceramente a Albert Banchs que me haya transmitido su seriedad (que roza a veces la solemnidad) y meticulosidad en el trabajo diario.

Quiero extender mi agradecimiento a la Universidad Carlos III de Madrid y al Departamento de Ingeniería Telemática, por brindarme un ambiente de trabajo inmejorable y por mantener viva en mi la idea de que no hay mejor enseñanza posible que la pública. En especial, quiero expresar mi agradecimiento a: Arturo Azcorra, Alberto García, David Larrabeiti, Jaime García, José Félix Kukielka, Carmen Guerrero, Carlos García García, Rubén y Ángel Cuevas, Guillermo Ibáñez, Mónica Cortés, Elvira Pompa, Ana Medina, Carlos Izquierdo, Carlos García Rubio, Pablo Basanta y Goyo Corral. También quiero agradecer sinceramente a Paco Valera la comida a la que me va a invitar.

Esta tesis, como todo proyecto importante en la vida, no hubiera sido posible sin el apoyo de los amigos. No puedo por lo tanto olvidar a ese maravilloso y pintoresco grupo de gente con el que he compartido tantos buenos y divertidos momentos: ¡los Glotones!, véase Manolo, Raquel, Isaac, Tere, Iván, Mar, Isaías, Richi y Antonio.

Quiero también dar las gracias al resto de personas con las que he tenido el honor de po-

der colaborar: Fernando Boavida, por ofrecerme la oportunidad de trabajar con él y de hacer una breve estancia en la Universidad de Coimbra; Jon Crowcroft, por permitirme aprender otras formas de trabajar y ayudarme durante mi estancia en el Computer Lab. de la Universidad de Cambridge; a Pablo Vidales y Javier Baliosian por hacerme tan fácil trabajar con ellos durante mi periplo en Cambridge; a Susana Sargento y Javier Baliosian (de nuevo) por aceptar generosamente informar sobre esta Tesis; a Telemaco Melia, Paolo Ferrer y Marco Liebsch, por los momentos que hemos compartido juntos trabajando en el proyecto Daidalos.

# Abstract

The Internet is evolving towards a more ubiquitous network, accessible anytime, anywhere. Users do not only expect to have Internet access available from fixed locations, such as their home, work, or even at other locations where hotspots are deployed (e.g., cafeterias, hotels, airports, etc), but also at mobile platforms. Internet access from aircrafts and trains is becoming a reality nowadays, starting to be widely offered.

While the Network Mobility (NEMO) Basic Support protocol defined by the IETF provides a first mechanism to support moving networks, it presents limited performance, since it requires data traffic to follow a detour route. This has triggered the necessity of the so-called *NEMO Route Optimisation* support.

In this PhD thesis we propose a set of mechanisms that enables Route Optimisation for Mobile Networks in heterogeneous environments. The contribution is twofold: on one hand a generic Route Optimisation solution for NEMO, called *MIRON: Mobile IPv6 Route Optimisation for NEMO* is proposed. This mechanism enables direct path communication between a node of a mobile network – supporting any kind of node, with and without mobility capabilities – and any other node in the Internet, without requiring any upgrade or modification neither in the Internet nodes nor in the nodes attached to the moving network. On the other hand, given the increasing relevance of vehicular scenarios and the importance of Route Optimisation in car-to-car communications (where the performance degradation is even more severe when a plain Network Mobility solution is used), a second mechanism suited for vehicular environments is proposed. This mechanism, called *VARON: Vehicular Ad-hoc Route Optimisation for NEMO*, combines in a secure way Network Mobility and Ad-hoc concepts to enable direct communication among neighbouring cars that are able to set-up a Vehicular Ad-hoc Network (VANET).

The proposed mechanisms are validated experimentally by means of a Linux implementation and simulations with the OPNET tool.

**Keywords:** IPv6, Network Mobility, Route Optimisation, Vehicular communications, Ad-hoc, Mobile Router.

# Resumen

Internet está evolucionando hacia una red ubicua, accesible en cualquier momento y desde cualquier lugar. Los usuarios no sólo esperan poder acceder a Internet desde lugares fijos, como sus casas, puestos de trabajo, o incluso otros lugares dónde se han desplegado *hotspots* (p.e., cafeterías, hoteles, aeropuertos, etc), sino también desde plataformas móviles. La provisión de acceso a Internet en aviones y trenes se está convirtiendo en una realidad actualmente y empieza a ser ampliamente ofrecida.

Aunque el protocolo básico de soporte de movilidad de redes definido por el IETF proporciona un primer mecanismo para soportar redes móviles, dicho protocolo presenta un rendimiento limitado, debido a que requiere que el tráfico sea encaminado por una ruta subóptima. Esto ha propiciado la necesidad de lo que se ha dado en llamar soporte de *Optimización de Rutas para Redes Móviles*.

En la presente Tesis Doctoral proponemos un conjunto de mecanismos que hacen posible la optimización de rutas en entornos heterogéneos. La contribución tiene dos vertientes: por un lado, se propone una solución de optimización de rutas genérica, llamada *MIRON: Mobile IPv6 Route Optimisation for NEMO*. Este mecanismo hace posible la comunicación directa entre un nodo de la red móvil – soportando nodos con o sin capacidades de movilidad – y cualquier otro nodo en Internet, sin requerir ningún cambio, actualización o modificación en los nodos de Internet ni en los nodos conectados a la red móvil. Por otro lado, dada la creciente relevancia de los escenarios vehiculares y la importancia de la optimización de rutas en comunicaciones inter-vehiculares (dónde la degradación en el rendimiento es aún más severa cuando se utiliza una solución no optimizada de movilidad de redes), se propone un segundo mecanismo adecuado para entornos vehiculares. Este mecanismo, llamado *VARON: Vehicular Ad-hoc Route Optimisation for NEMO*, combina de una forma segura los conceptos de movilidad de redes y redes ad-hoc para hacer posible la comunicación directa entre coches vecinos que son capaces de establecer una red ad-hoc vehicular.

Los mecanismos propuestos han sido validados experimentalmente mediante una implementación en Linux y simulaciones empleando la herramienta OPNET.

**Palabras clave:** IPv6, Movilidad de Rutas, Optimización de Redes, Comunicaciones Vehiculares, Ad-hoc, Router Móvil

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

The **Internet** is evolving towards a more ubiquitous network, accessible anytime, anywhere. Users do not only expect to have Internet access available from fixed locations, such as their home, work, or even at other locations where hotspots are deployed (e.g., cafeterias, hotels, airports, etc), but also at mobile platforms. Internet access from airplanes and trains is becoming a reality nowadays, starting to be widely offered.

The number of wireless IP terminals keeps on growing, and it is expected that this number will increase even more with the convergence of wireless telecommunications networks (supporting over 1.5 billion devices) and the Internet. This convergence is supported by the Internet Protocol[1] (IP), but IP was not designed to support a key requirement in today's networks: **mobility.**

Triggered by the previous requirement and users' demands, the Internet research community designed some mechanisms to enable true transparent IP mobility for single-roaming nodes, and to benefit from the **heterogeneous technologies** expected in future 4G networks. On the other hand, as the Internet access becomes more and more ubiquitous, demands for mobility are no longer restricted to single terminals.

There are several mobility scenarios that involve a moving network as opposed to a host: what is known as **network mobility** in IP networks. For example, a user can be mobile while carrying a number of devices – forming a Personal Area Network (PAN) –, such as a mobile phone, a laptop, and a Personal Digital Assistant (PDA). From the various scenarios where a network mobility solution is required, another relevant and representative scenario is the transparent provision of Internet access from mobile platforms, such as trains, planes, buses or cars.

The basic mechanism defined to enable Network Mobility support (the Network Mobility Basic Support protocol) is an extension of the protocol defined to enable mobility of single hosts (Mobile IPv6), but without some of the optimisations that Mobile IPv6 provides. One of these **missing parts** is the **Route Optimisation** support: in order to provide transparent mobility support, data traffic between a moving network and any other node in the Internet does not follow a direct path between them, but a detour one, through the Home Network (where the moving network belongs), causing additional delay and packet overhead. Route Optimisation becomes even more pertinent when considering

[1] It is expected that the new version of IP: IPv6, will be widely adopted in order to support the growth in the number of wireless devices. Therefore, this PhD thesis focuses on IPv6 mechanisms.

mobile networks, since the particular nature of moving networks poses some additional challenges more difficult to solve than they were in single-node mobility scenarios. The suboptimal routing introduced by the Network Mobility Basic Support protocol can lead even to prevent communications from taking place, and therefore this problem should be tackled if it is desired to deploy moving networks in practice.

Provided that Route Optimisation is crucial for Mobile Networks, one of the main contributions of this PhD thesis consists in the design of a **generic Route Optimisation mechanism for Network Mobility**, called **MIRON: Mobile IPv6 Route Optimisation for NEMO**. MIRON provides significant performance improvements over the NEMO Basic Support protocol, and it is implemented only modifying the software in the (mobile) routers that provide connectivity to a Mobile Network. Neither the nodes attached to the Mobile Network, nor any node located at the Internet that is communicating to a node of the moving network, need to be modified for MIRON to work, which facilitates the deployment of the solution. The proposed mechanism is validated and evaluated experimentally by means of an implementation. Alternative approaches that do require changes on additional nodes than the Mobile Router are also explored in this PhD thesis.

There is a scenario that is receiving quite a lot of attention from the research and industrial communities: **vehicular communications**. So far, this scenario has been addressed by using a terminal centric approach, but since the vehicular scenario involves a group of devices (e.g., sensors, music players, on-board computers, passengers' devices and so on) moving together, a network mobility approach seems more appropriate than a solution that relies on every device managing its own mobility. Furthermore, there is an opportunity for **optimisation in vehicular environments** when communication occurs between vehicles that are close enough to communicate through an **ad-hoc network** formed by those vehicles and perhaps other vehicles in their surroundings. The second main contribution of this PhD thesis consists in the combination of the Network Mobility and Ad-hoc concepts – in a secure way – to optimise local car-to-car communications. The designed solution, called **VARON: Vehicular Ad-hoc Route Optimisation for NEMO**, is validated through heavy simulation, proving that an improvement in the performance of the communication is achieved by deploying VARON in vehicles.

The PhD thesis is structured in four main parts. Part I reviews the current state of the art regarding network mobility and vehicular communications. Chapter 2 provides a detailed description of the network mobility topic[2] and presents the Route Optimisation issue as well as a survey of the existing proposals that address this problem, highlighting their limitations. Next, an analysis of the research within the vehicular communications field is included in Chapter 3, classifying into three different categories the possible approaches that may be followed to provide vehicles with communication capabilities. This analysis shows the weaknesses of classical mechanisms and introduces the benefits that may be obtained from using an approach that combines Network Mobility and ad-hoc concepts in a secure way.

Part II includes the main contributions of this PhD thesis. Chapter 4 shows the goals of the thesis and presents the design considerations that have been followed in the development

[2] In [BSC+05b] and [BSC+05a], we provide an overview of this research.

of the mechanisms resulting from this PhD thesis.

Chapter 5 describes in detail the mechanism designed to provide generic Route Optimisation support for Network Mobility: MIRON. MIRON enables direct path communication between a node of the mobile network – supporting any kind of node, with and without mobility capabilities – and any other node in the Internet. To achieve that, MIRON has two modes of operation: the Mobile Router performing all the Route Optimisation tasks on behalf of those nodes that are not mobility capable and an additional mechanism, based on PANA and DHCP, enabling mobility-capable nodes (i.e. Mobile Nodes attached to a NEMO) and routers (i.e. nested Mobile Networks). A validation and evaluation of the solution is included, based on experimental tests using an implementation of MIRON. Security and scalability analyses are also included to evaluate the feasibility of the solution. Finally, alternative approaches – based on a secure delegation of signalling rights to the Mobile Router and which require changes on other nodes than the Mobile Router (therefore aimed at being deployed in a longer-term or in more restricted environments) – are explored. The contents of this chapter have been published in [CBB+06], [BBC04], [BBCS05], [BOC+06] and [CBBS05].

Chapter 6 describes in detail the mechanism proposed to provide Route Optimisation of local communications in vehicular environments: VARON. VARON enables to optimise car-to-car communications in a secure way by combining a Network Mobility approach to support car-to-Internet communications with a vehicular ad-hoc approach. Since security is the main issue in these environments, an analysis of potential exploits is provided first, describing and classifying the attacks that VARON aims at avoiding. The designed mechanism is checked to verify whether it avoids those possible attacks, and validated experimentally, by means of extensive simulation. Simulations enable the analysis of VARON performance (comparing it to the use of a plain Network Mobility approach and a generic Route Optimisation solution). This part of the thesis have been submitted for publication in [BCS+06].

Part III concludes the PhD thesis. Chapter 7 presents the conclusions resulting from the main contributions of the thesis, while Chapter 8 introduces some relevant future work topics that are still open and are worth to be explored in a later work.

Part IV includes some appendixes. Appendix A provides a brief summary of the PANA protocol (which is used by MIRON to enable Route Optimisation in some scenarios) and Appendix B describes in detail the protocol message format of VARON.

Other publications of the author highly related with the content of this thesis can be found in [dlOBC05][3], [vHKBC06], [BGMBA06], [BC05], [BC06], [BSM+05], [VBM+05], [VBS+06], [ABB+06] and [CSM+05].

This PhD Thesis is applying for an “European Mention” in the PhD Diploma. In order to fully comply with the Spanish (Arts. 11 a 14 del R.D. 56/2005 de 21 de Enero) and university regulations, all the thesis is written in English and some parts are also translated into Spanish (Abstract and Chapters 1, 2, 3, 4, 7 and 8).

[3] It also appears as [dlOBC06].

# Capítulo 1

# Introducción

**Internet** está evolucionando hacia una una red ubicua, accesible en cualquier momento y desde cualquier lugar. Los usuarios no sólo esperan poder acceder a Internet desde lugares fijos, como sus casas, puestos de trabajo, o incluso otros lugares dónde se han desplegado *hotspots* (p.e., cafeterías, hoteles, aeropuertos, etc), sino también desde plataformas móviles. La provisión de acceso a Internet en aviones y trenes se está convirtiendo en una realidad actualmente y empieza a ser ampliamente ofrecida al gran público.

El número de terminales inalámbricos IP continúa creciendo, y se espera que dicho número crezca aún más con la convergencia de las redes de telecomunicaciones inalámbricas (soportando más de 1500 millones de dispositivos) e Internet. Esta convergencia está soportada por el protocolo de Internet[1] (IP), pero IP no fue diseñado para soportar un requisito clave en las redes actuales: la **movilidad**.

Propiciado por este requisito y las demandas de los usuarios, la comunidad investigadora de Internet diseñó algunos mecanismos que habilitaban la movilidad transparente para terminales que se movían individualmente y que permitían obtener beneficio de las **heterogeneidad de las tecnologías de acceso** que se prevé en las futuras redes de 4ª generación (4G). Por otro lado, debido a que el acceso a Internet es más ubicuo cada vez, la demandas de movilidad ya no están restringidas sólo a terminales individuales.

Existen varios escenarios de movilidad que involucran redes móviles en lugar de terminales: lo que se conoce como **movilidad de redes**. Por ejemplo, un usuario puede ser móvil llevando consigo múltiples dispositivos – formando una red de área personal (Personal Area Network, PAN) –, como un teléfono móvil, un ordenador portátil y un asistente digital personal (Personal Digital Assistant, PDA). De los múltiples escenarios dónde se requiere una solución de movilidad de redes, otro ejemplo relevante y representativo es la provisión transparente de acceso a Internet en plataformas móviles, como trenes, aviones, autobuses o coches.

El mecanismo básico definido para proporcionar soporte de movilidad de redes (el protocolo de Soporte Básico de Movilidad de Redes) es una extensión del protocolo definido para habilitar la movilidad de terminales individuales (IPv6 Móvil), pero sin algunas de las optimizaciones que proporciona IPv6 Móvil. Una de estas **piezas que faltan** es el soporte de **Optimización de Rutas**: de cara a proporcionar soporte de movilidad transparente, el

[1] Se espera que la nueva versión de IP: IPv6, será adoptada globalmente de cara a soportar el crecimiento en el número de dispositivos inalámbricos. Debido a esto, esta Tesis Doctoral se centra en mecanismos IPv6.

tráfico de datos intercambiado entre una red móvil y cualquier otro nodo en Internet no sigue el camino directo entre ambos, sino una ruta ineficiente, a través de la Red Hogar (a la que pertenece la red móvil), originando un retardo adicional y una sobrecarga de cabeceras en los paquetes. La optimización de rutas es aún más pertinente cuando consideramos redes móviles, debido a que la naturaleza particular de las redes móviles impone retos adicionales que son más complicados de resolver que lo eran para el caso de terminales móviles individuales. El encaminamiento subóptimo introducido por el protocolo de Soporte Básico de Movilidad de Redes puede llegar incluso a impedir que ciertas comunicaciones lleguen a establecerse, y por lo tanto este problema debe ser resuelto de cara a poder desplegar redes móviles en la práctica.

Dada la importancia de la optimización de rutas para redes móviles, una de las contribuciones principales de esta Tesis Doctoral consiste en el diseño de un **mecanismo genérico de Optimización de Rutas para Redes Móviles**, llamado ***MIRON: Mobile IPv6 Route Optimisation for NEMO***. MIRON proporciona mejoras significativas en el rendimiento sobre el protocolo de Soporte Básico de Movilidad de Redes, y está implementado modificando únicamente el software de los routers (móviles) que proporcionan conectividad a la red móvil. Ni los nodos conectados a la red móvil ni ningún nodo de la Internet que se esté comunicando con un dispositivo de la red móvil, necesitan ser modificados para que MIRON funcione, lo cual facilita enormemente el despliegue de la solución. El mecanismo propuesto ha sido validado y evaluado experimentalmente mediante una implementación. Otros enfoques alternativos, que requieren cambios en más nodos además del router móvil, son también explorados en esta Tesis Doctoral.

Hay un escenario que está recibiendo una gran cantidad de atención por parte de las comunidades investigadora e industrial: las **comunicaciones vehiculares**. Hasta ahora, este tipo de escenario ha sido tratado utilizando enfoques centrados en el terminal, pero dado que el escenario vehicular involucra a un grupo de nodos (p.e., sensores, reproductores de música, ordenadores de abordo, dispositivos diversos de los pasajeros, etc.) que se mueven juntos, un enfoque basado en movilidad de redes parece mucho más apropiado que una solución que confía a cada dispositivo la gestión de su propia movilidad. Además, existe una oportunidad de **optimización en entornos vehiculares** cuando la comunicación transcurre entre vehículos que están lo suficientemente cerca como para comunicarse a través de una **red ad-hoc** formada por dichos vehículos y quizás otros en las cercanías. La segunda contribución principal de esta tesis consiste en la combinación – de forma segura –de los conceptos de movilidad de redes y ad-hoc para optimizar comunicaciones entre vehículos locales. La solución diseñada, llamada ***VARON: Vehicular Ad-hoc Route Optimisation for NEMO***, ha sido validada mediante simulación exhaustiva, probando que se consigue un incremento del rendimiento en las comunicaciones mediante el despliegue de VARON en los vehículos.

La Tesis Doctoral está estructurada en cuatro partes principales. La Parte I revisa el estado del arte actual relativo a la movilidad de redes y las comunicaciones vehiculares. El capítulo 2 proporciona una descripción detallada en materia de movilidad de redes[2] y presenta la problemática de la optimización de rutas así como una clasificación de las propuestas

[2] En [BSC+05b] y [BSC+05a], proporcionamos una panorámica de la investigación en este campo.

existentes que abordan dicho problema, resaltando sus limitaciones. Después de esto, se incluye un análisis de la investigación en el campo de las comunicaciones vehiculares en el Capítulo 3, clasificando en tres diferentes categorías las posibles aproximaciones que pueden seguirse para proveer a los vehículos con capacidades de comunicación. Este análisis muestra los puntos débiles de los mecanismos clásicos e introduce los beneficios que pueden obtenerse si se emplea un enfoque que combine los conceptos de movilidad de redes y ad-hoc de tal forma que proporcione garantías de seguridad.

En la Parte II se incluyen las contribuciones principales de la presente Tesis Doctoral. El Capítulo 4 describe los objetivos de la Tesis y presenta las consideraciones de diseño que se han seguido en el desarrollo de los mecanismos que han resultado de esta Tesis Doctoral.

El Capítulo 5 describe en detalle el mecanismo diseñado para proporcionar un soporte genérico de optimización de rutas para redes móviles: MIRON. MIRON hace posible la comunicación directa entre un nodo de la red móvil – soportando cualquier tipo de nodo, con o sin capacidades de movilidad – y cualquier otro nodo de Internet. Para lograr esto, MIRON tiene dos modos de funcionamiento: uno en el que el router móvil realiza todas las tareas de optimización de rutas en nombre de los nodos que no tienen soporte de movilidad alguno, y otro mecanismo adicional, basado en DHCP y PANA, que habilita que los nodos (p.e., aquellos nodos móviles que se conecten a la red móvil) y routers (p.e., redes móviles anidadas) con soporte de movilidad gestionen su propia optimización de rutas. Se incluye una validación y evaluación de la solución, basada en pruebas experimentales empleando una implementación de MIRON. Se incluyen también unos análisis de la seguridad y escalabilidad de la solución, de cara a evaluar si es factible desplegar la la solución propuesta o no. Finalmente, algunos enfoques alternativos – basados en una delegación segura de los derechos de señalización al router móvil (este tipo de solución está enfocado por lo tanto a ser desplegado en un plazo mayor de tiempo o en escenarios más restrictivos) – son explorados. Los contenidos de este capítulo han sido publicados en [CBB+06], [BBC04], [BBCS05], [BOC+06] y [CBBS05].

El Capítulo 6 describe en detalle el mecanismo propuesto para proporcionar optimización de rutas en comunicaciones locales en entornos vehiculares: VARON. VARON combina de forma segura el enfoque de movilidad de redes para soportar comunicaciones vehículo-Internet con un enfoque ad-hoc vehicular para optimizar comunicaciones inter-vehiculares. Dado que la seguridad es el problema principal en este tipo de entornos, primero se proporciona un análisis de los ataques potenciales, describiendo y clasificando los ataques que VARON trata de evitar. Se comprueba que el mecanismo diseñado evita dichos posibles ataques y se procede a su evaluación experimental, mediante simulaciones exhaustivas. Las simulaciones permiten realizar un estudio del rendimiento de VARON (comparándolo con el uso de una solución simple de movilidad de redes y una optimización genérica de optimización de rutas). Esta parte de la tesis ha sido enviada para consideración de su publicación en [BCS+06].

La Parte III concluye la Tesis Doctoral. El Capítulo 7 presenta las conclusiones más importantes que han resultado de las contribuciones principales de la Tesis, mientras que el Capítulo 8 introduce algunos temas de investigación relevantes que están todavía abiertos y que merecen la pena ser explorados en trabajos futuros.

En la Parte IV se incluyen algunos apéndices. El Apéndice A resume brevemente el protocolo PANA (usado por MIRON para habilitar la optimización de rutas en algunos es-

cenarios) y el Apéndice B describe en detalle el formato de mensajes del protocolo definido por VARON.

Otras publicaciones del autor altamente relacionadas con el contenido de la tesis pueden encontrarse en [dlOBC05][3], [vHKBC06], [BGMBA06], [BC05], [BC06], [BSM+05], [VBM+05], [VBS+06], [ABB+06] y [CSM+05].

La presente Tesis Doctoral va a aplicar para obtener la mención europea en el título de doctor. De cara a cumplir todas las normas vigentes del Gobierno Español (Arts. 11 a 14 del R.D. 56/2005 de 21 de Enero) y la Universidad Carlos III de Madrid, toda la tesis está originalmente escrita en inglés y posteriormente se han traducido al español el Resumen y los Capítulos 1, 2, 3, 4, 7 y 8.

[3] También publicado en [dlOBC06].

# Part I

# State of the art

# Estado del Arte

# Chapter 2

# Network Mobility: bringing ubiquity to the Internet access

This chapter provides a detailed description of the network mobility problem, describing current proposed solutions, as well as identifying open issues and unexplored problems.

## 2.1. Introduction

Driven by the success of cellular technologies, mobility has changed the way users communicate. Ubiquity and heterogeneity [CSB+04], [CSM+05], [ABB+06] will be two key concepts of forthcoming 4G [HY03] networks, which are expected to enable users to communicate almost anytime, anywhere.

Triggered by these needs and the fact that deployed Internet protocols did not support mobility of any kind, the technical community designed several solutions that addressed the problem of mobility [Hen03]. There are several approaches that may be followed, although a first classification could be done based on the layer at which mobility is managed. Cellular networks enable roaming of users between different radio cells, by managing the mobility with specific layer 2 protocols. On the one hand, this kind of solution performs quite well but on the other hand, it is limited to mobility within the same technology. To exploit network heterogeneity, mobility should be managed at a technology-independent layer (that is, IP or above). Although it is possible to handle mobility at the application or transport layer [SB00], [SBK01], doing that would require developing different solutions for each application or transport protocol. Therefore, the IP layer seems to be the most appropriate one to manage mobility.

IP networks were not designed for mobile environments. Both in IPv4 and IPv6, IP addresses play two different roles. On the one hand, they are locators that specify, based on a routing system, how to reach the node that is using that address. The routing system keeps information on how to reach different set of address that have a common network prefix. This address aggregation in the routing system provides scalability guarantees. On the other hand, IP addresses are also part of the end-point identifiers of a communication, and upper layers use the identifiers of the peers of a communication to identify them [Chi99], [LD03].

This dual role played by IP addresses imposes some restrictions on mobility, because

when a terminal moves from one network (IP subnet) to another, we would like, on the one hand to maintain the IP address associated to the node that moves (associated to one of its network interfaces) in order not to change the identifier that upper layers are using in their ongoing sessions, but, on the other hand we need to change the IP address to make it topologically correct in the new location of the terminal, allowing in this way the routing system to reach the terminal.

Protocols such as Dynamic Host Configuration Protocol (DHCP) [Dro97], [DBV+03] enabled the *portability* of terminals, but this was not enough to achieve real and transparent mobility, as it required ongoing transport sessions to be restarted after a change of the point of attachment. The problem of terminal *mobility* in IP networks has been studied for a long time within the IETF[1], and there exist IP-layer solutions for both IPv4 [Per02] and IPv6 [JPA04] that enable the movement of terminals without stopping their ongoing sessions.

As the Internet access becomes more and more ubiquitous, demands for mobility are not restricted to single terminals anymore. There exists also the need of supporting the movement of a complete network that changes its point of attachment to the fixed infrastructure, maintaining the sessions of every device of the network: what is known as *network mobility* in IP networks. In this case, the mobile network will have at least a (mobile) router that connects to the fixed infrastructure, and the devices of the mobile network will obtain connectivity to the exterior through this mobile router.

Supporting the roaming of networks that move as a whole is required in order to enable the transparent provision of Internet access in mobile platforms [LJP03], such as the following:

- Public transportation systems. That would enable passengers in trains, planes, ships, etc., to travel with their own terminals (for example, laptops, cellular phones, PDAs and so on) and obtain Internet access through a mobile router located at the transport vehicle, that connects to the fixed infrastructure.
- Personal Networks. Electronic devices carried by people, like PDAs, photo cameras, etc. obtain connectivity through a cellular phone acting as the mobile router of the personal network.
- Vehicular scenarios. Future cars will benefit from having Internet connectivity, not only to enhance safety (for example, by using sensors that could control multiple aspects of the vehicle operation, interacting with the environment, and communicating with the exterior), but also to provide personal communication and entertainment Internet-based services to passengers.

There are ongoing research and industrial projects addressing the challenges posed by some of the previous scenarios. The aircraft manufacturer Boeing has developed the *Connexion by Boeing* [2] technology [JdLC01], allowing airlines to provide IPv4 Internet access to passengers[3]. *Nautilus6*[4] is a working group within the *WIDE*[5] project that addresses the

[1] `http://www.ietf.org/`

[2] `http://www.connexionbyboeing.com/`

[3] The solution basically consists in using BGP as a mobility solution, by means of the use of the global routing table and selective route announcements and withdrawals as planes move [Dul05], [BB04], [Dul06].

[4] `http://www.nautilus6.org/`

[5] `http://www.wide.ad.jp/`

network mobility problem, by providing several implementations of network mobility software and performing real demonstrations in live environments. These are just two examples that show the real interest that exists on network mobility nowadays.

## 2.2. Network Mobility Basic Support protocol

The IP terminal mobility solution (Mobile IPv6 [JPA04]) does not support, as it is now defined, the movement of networks. As a result, the IETF NEMO (Network Mobility) Working Group (WG) was created to standardise a solution enabling network mobility at the IPv6 layer. The current solution, called Network Mobility Basic Support protocol, is defined in the RFC 3963 [DWPT05].

In this solution, a mobile network (known also as Network that Moves – NEMO[6]) is defined as a network whose attachment point to the Internet varies with time (see Figure 2.1). The router within the NEMO that connects to the Internet is called the Mobile Router (MR) [EL06]. It is assumed that the NEMO has a Home Network where it resides when it is not moving. Since the NEMO is part of the Home Network, the Mobile Network has configured addresses belonging to one or more address blocks assigned to the Home Network: the Mobile Network Prefixes (MNPs). These addresses remain assigned to the NEMO when it is away from home. Of course, these addresses only have topological meaning when the NEMO is at home. When the NEMO is away from home, packets addressed to the Mobile Network Nodes (MNNs) will still be routed to the Home Network. Additionally, when the NEMO is away from home, that is, it is in a visited network, the MR acquires an address from the visited network, called the Care-of Address (CoA), where the routing architecture can deliver packets without additional mechanisms.

There are different types of Mobile Network Nodes: Local Fixed Node (LFN), that is a node that has no mobility specific software; Local Mobile Node (LMN), that is a node that implements the Mobile IP protocol and whose home network is located in the mobile network; and Visiting Mobile Node (VMN) that is a node that implements the Mobile IP protocol, has its home network outside the mobile network, and it is visiting the mobile network.

The goal of the network mobility support mechanisms [Ern05] is to preserve established communications between the MNNs and external Correspondent Nodes (CNs) despite movement. Packets of such communications will be addressed to the MNNs' addresses, which belong to the MNP, so additional mechanisms to forward packets between the Home Network and the NEMO are needed.

The network mobility basic solution (see Figure 2.1) for IPv6 [DWPT05] is conceptually similar to that of terminals. It is based in the set-up of a bidirectional tunnel between a special node located in the Home Network of the NEMO (the Home Agent, HA), and the Care-of Address of the MR. This tunnel is called MRHA tunnel. The HA is located in the Home Network of the mobile network, that is, in a location where the addressing of the mobile network is topologically correct. All the traffic addressed to the mobile network is delivered to its HA, that sends it towards the MR through the tunnel. The MR removes the tunnel header and forwards the traffic to its destination within the mobile network. The traffic

[6]NEMO can mean NEtwork MObility or NEtwork that MOves according to the context.

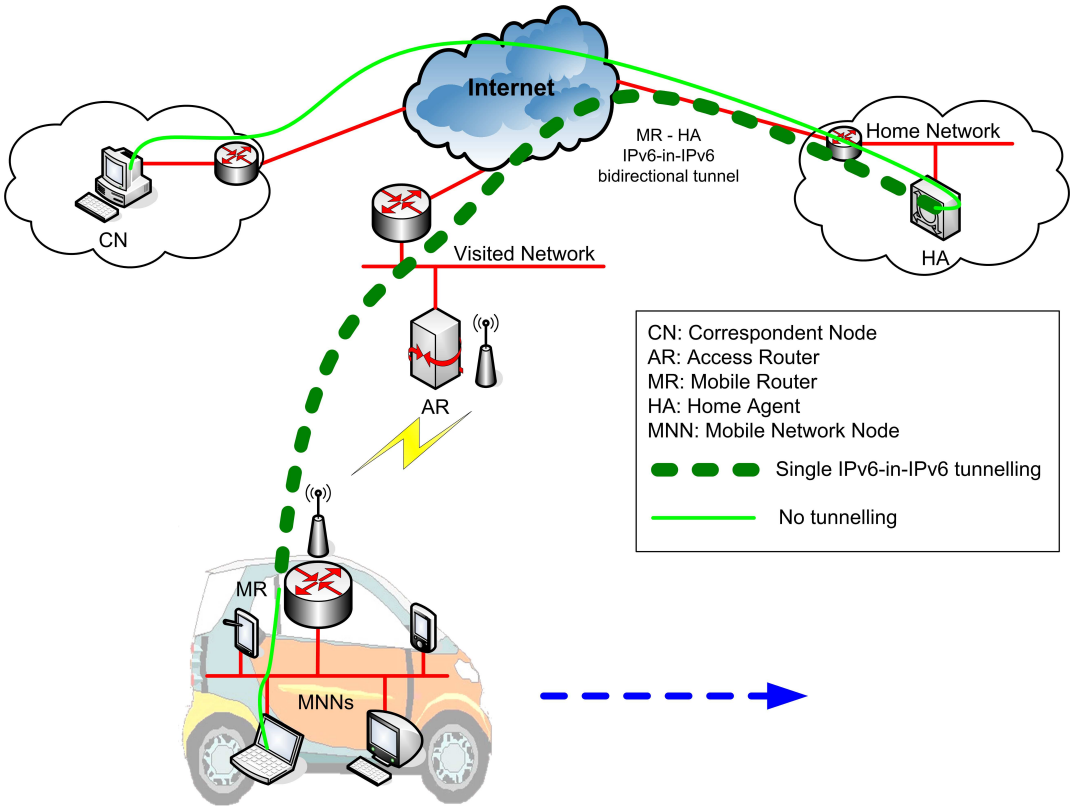


Figure 2.1: NEMO Basic Support protocol operation overview.

originated in the mobile network is sent by the MR towards the HA through the tunnel, the HA removes the tunnel header and forwards the packets to their destinations.

The protocol is quite similar to the solution proposed for host mobility support, Mobile IPv6 (MIPv6) [JPA04], without including the Route Optimisation (RO) support. Actually, the protocol extends the existing Binding Update (BU) message to inform the Home Agent of the IP address of the NEMO side of the tunnel (that is, the CoA of the MR), through which the HA has to forward packets addressed to the MNP. There are several ways for the HA to know the MR's MNP: by having it statically configured, by the MR adding the MNP information in a new option of the Binding Update, or by running a dynamic routing protocol with the MR through the tunnel.

The NEMO Basic Solution protocol enables the mobility of an entire network, but this is just the first step to allow the deployment of new ubiquitous connectivity configurations, solving only the very basic problem, and raising some other issues that need to be carefully looked at. Among the issues that are still open, it is worth mentioning the following:

- **Route Optimisation support.** When the NEMO Basic Support protocol is used, all communications to and from a node attached to the mobile network go through the MRHA bidirectional tunnel when the mobile network is away. As a result, the packet overhead and the length of the route followed by packets are increased, thus resulting in an increment of the packet delay in most cases. This issue may have a serious

impact on the performance of applications running on nodes within the NEMO and may even prevent communications from taking place.

- **Multihoming support.** The support of multihoming has shown to be very important in future 4G networks, in order to fully exploit the heterogeneity in the network access. This is even more relevant for mobile networks, since a loss of connectivity or a failure to connect to the Internet has a more significant impact than on a single node. Furthermore, typical deployment scenarios, such as the provision of Internet access from moving vehicles, will typically require the use of several interfaces (using different access technologies), since the mobile network may be moving within distant geographical locations where different access technologies are provided and governed by distinct access control policies [NPEB06]. Although there exist several works published regarding multihoming support for NEMO, such as [PCKC04], [PCEC04], [NE04], [MEN04], [KMI+04], [EC04], [SBGE05], [MIUM05] and [Esa04], there is no mechanism that fulfil all the requirements of a multihoming solution for mobile network environments. The applicability of the SHIM6 protocol [BN06] to provide NEMO multihoming support is one of the approaches that should be further investigated (an early attempt can be found in [Bag04]).

- **Multicast support.** Current Network Mobility basic specification does not support multicast traffic transmission to/from a mobile network. With some broadcast technology becoming popular, such as DVB, the support of multicast-like application would be required in future 4G platforms. Early attempts to provide such a support to mobile networks can be found in [SVK+04] and [vHKBC06].

- **Seamless handover support.** In order to support real-time applications, not only the end-to-end delay should be kept under certain values [KT01], but also the interruption time due to handovers. Owing to the additional complexity of the NEMO scenario, the handoff delay during handovers may be higher than for a single terminal. The applicability of some of the solutions for Mobile IPv6, such as Fast Handovers for Mobile IPv6 [Koo05], to alleviate the increase in handoff delay or the design of new ones should be investigated [PPLS06], [HCH06], [KMW06].

- **QoS support.** Mobile networks, because of their dynamic nature, pose additional challenges to the inherent difficulty of providing QoS over wireless links. Indeed, QoS provisioning in a NEMO involves additional mechanisms besides providing QoS to the various wireless links of the mobile network. Statistical analyses are required in order to guarantee the desired performance resulting from traversing several wireless links, each of which provides only statistical guarantees. In addition, novel signalling mechanisms need to be devised to perform QoS signalling over such a dynamic environment. An early attempt of reservation protocol adapted to NEMO can be found in [TL05].

- **Authentication, Authorisation and Accounting (AAA) support.** The NEMO scenario poses some challenges to classical Authentication, Authorisation and Accounting (AAA) schemes [ZEB+05]. This issue has to be carefully analysed, paying attention to real NEMO AAA deployment scenarios [FSK+06].

Although all the previously described topics are relevant, the Route Optimisation issue is the most critical one, since it may even prevent mobile networks from being deployed in real scenarios. Therefore, it is very important to address this issue. One of the main objectives of this PhD thesis is to tackle the Route Optimisation issue in realistic NEMO deployment scenarios, by analysing the problem, designing a solution, validating it and later evaluating its performance.

## 2.3. The Route Optimisation issue in Network Mobility

By using a bidirectional tunnel between the Mobile Router and the Home Agent, the NEMO Basic Support protocol [DWPT05] enables Mobile Network Nodes to reach and be reachable by any node in the Internet. However, such a solution presents also important performance limitations [NTWZ06], as it will be described in this section.

The network mobility basic solution forces – when a mobile network is not at home – all the traffic addressed to a MNN, to traverse the HA and to be forwarded to the mobile network through the tunnel established between the MR and the HA. The inverse path is followed by packets sent by a MNN. This phenomenon (see Figure 2.1) raises some inefficiency, both in terms of latency and effective throughput, and can be unacceptable for certain applications. More precisely, we can highlight the following limitations of the basic solution [DWPT05]:

- It forces **suboptimal routing** (known as angular or triangular routing), that is, packets are always forwarded through the HA following a suboptimal path and therefore adding a delay in the packet delivery. This delay can be negligible if the mobile network or the Correspondent Node are close to the Home Agent (that is, close to the Home Network). On the other hand, when the mobile network and/or the Correspondent Node are far away from the Home Agent, the increase in the delay could be very large. This may have a strong impact on real-time applications where delay constraints are very important. In general, an increase in the delay may also impact the performance of transport protocols such as TCP, since the sending rate of TCP is partly determined by the round-trip-time (RTT) perceived by the communication peers. A representative example of how large the impact on the delay could be, can be found on aircraft communications, where a tunnelled mobile IP communication takes almost 2 seconds to complete a TCP 3-way handshake [BB04], [Dul06].

- It introduces non-negligible **packet overhead**, reducing the Path MTU (PMTU) and the bandwidth efficiency. Specifically, an additional IPv6 header (40 bytes) is added to every packet because of the MRHA bidirectional tunnel.

  The effect of this overhead can be analysed for example by looking at a VoIP communication using the widely utilised Skype[7] application. Skype [BS04] uses the iLBC (internet Low Bitrate Codec) [ADA+04] codec, which is a free speech codec suitable for robust voice communication over IP. If an encoding frame length of 20 ms (as in RFC 3550 [SCFJ03]) is used, it results in a payload bit rate of 15.20 kbps. Because of the additional IPv6 header (that is, 320 extra bits per packet, 50 packets per second

[7] `http://www.skype.com/`

with this codec) the bit-rate used by the voice communication is increased in 16 kbps (more than the actual VoIP payload).

- The HA becomes a **bottleneck** of the communication as well as a potential single point of failure. Even if a direct path is available between a MNN and a CN, if the HA (or the path between the CN and the HA or between the HA and the MR) is not available, the communication is disrupted. Congestion at the HA or at Home Network may lead to additional packet delay, or even packet loss. The effect of congestion is twofold: on the one hand, it affects data packets by making them to be delayed or even discarded. On the other hand, delayed or discarded signalling packets (e.g., Binding Updates) may affect the set-up of the bidirectional tunnels, causing disruption of the data traffic through these tunnels.

Ref. [NTWZ06] describes also additional limitations, such as increased processing delay, increased chances of packet fragmentation and increased susceptibility to link failures.

Most of these concerns also exist in terminal mobility when using Mobile IPv6 [JPA04]. In order to solve them, a *Route Optimisation* mechanism was developed and included as a part of the base protocol. In Mobile IPv6, Route Optimisation is achieved by allowing the Mobile Node (MN) to send Binding Update messages also to the CNs. In this way the CN is also aware of the CoA where the MN's Home Address (HoA) is currently reachable. The Return Routability (RR) procedure is defined to prove that the Mobile Node has been assigned (that is, *owns*) both the Home Address and the Care-of Address at a particular moment in time [NAA+05].

The Network Mobility scenario brings a number of additional issues, making the problem more complex and difficult to solve[8].

The aforementioned problems are exacerbated when considering what has been called *nested mobility*. A mobile network is said to be nested when a mobile network attaches to another mobile network and obtains connectivity through it (see Figure 2.2). An example is a user that gets into a vehicle with his Personal Area Network (Mobile Network 2) and that connects, through a MR – like a WiFi enabled PDA – to the car's network (Mobile Network 1), that is connected to the fixed infrastructure.

The NEMO WG has defined some useful terminology [EL06] related to the nested scenario. The mobile network at the top of the hierarchy connecting the aggregated nested mobile network to the Internet is called *root-NEMO* (for example, Mobile Network 1 in Figure 2.2). Likewise, the Mobile Router of that root-NEMO is called *root-MR*[9] (for example, MR 1 in Figure 2.2). In a mobile network hierarchy, the upstream mobile network providing Internet access to another mobile network further down in the hierarchy is named *parent-NEMO* and the downstream mobile network is called *sub-NEMO* (in Figure 2.2, Mobile Network 1 is a parent-NEMO of Mobile Network 2 – which is therefore a sub-NEMO of the former). Similarly, the MRs of the parent-NEMO and the sub-NEMO are called, *parent-MR* and *sub-MR* respectively (for example, MR 1 and MR 2 in Figure 2.2).

[8] This situation made the IETF decide to address the Route Optimisation problem in Network Mobility separately, not including the development of a RO solution as an item of the NEMO WG charter, but the analysis of the problem and solution space.

[9] Some authors alternatively use "Top Level Mobile Router" (TLMR) to refer to the root-MR.

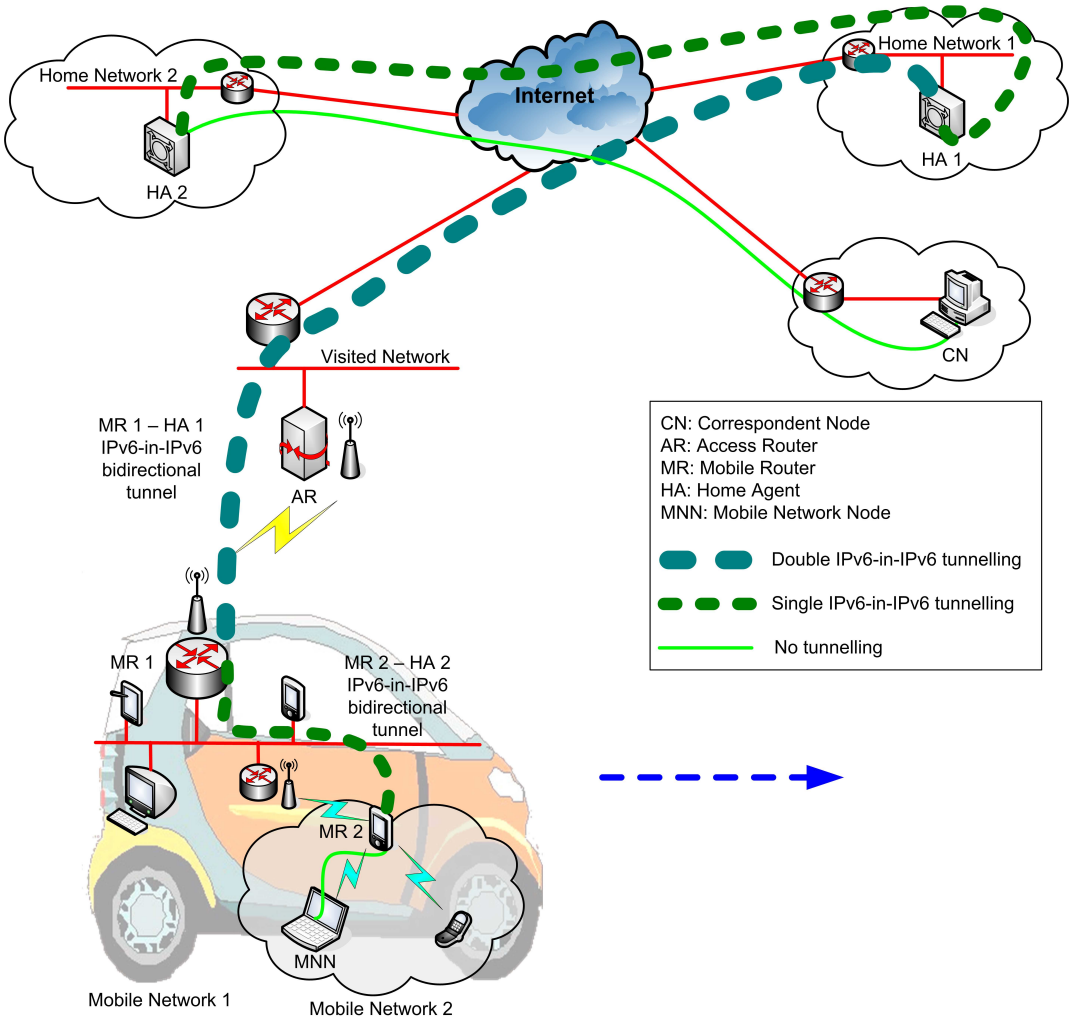


Figure 2.2: Nested mobile network. Operation of the NEMO Basic Support protocol (multi-angular routing).

The use of the NEMO Basic Support protocol in nested configurations amplifies the sub-optimality of the routing and decreases the performance of the solution, since in these scenarios packets are forwarded through all the HAs of all the upper level mobile networks involved (known as multi-angular or pinball routing, see Figure 2.2). This is because each sub-NEMO obtains a CoA that belongs to the Mobile Network Prefix of its parent NEMO. Such a CoA is not topologically meaningful in the current location, since the parent-NEMO is also away from home, and packets addressed to the CoA are tunnelled – thus increasing packet overhead – to the HA of the parent-NEMO.

There is an additional particular NEMO scenario that needs to be addressed, namely when a Mobile IPv6 host attaches to a mobile network (becoming a Visiting Mobile Node, VMN). Traffic sent to and from a VMN has to be routed not only via the Home Agent of the VMN, but also via the HA of the MR of the mobile network, therefore suffering from the

same performance problems than in a 1-level nested mobile network[10]. Even if the VMN performs the Mobile IPv6 Route Optimisation procedure, this will only avoid traversing the VMN's HA, but the resulting route will not be optimal at all, since traffic will still have to be routed through the MR's HA.

Because of all the limitations identified in this section, it is highly desirable to provide Route Optimisation support for NEMO [NTWZ06], [NZWT06], [PSS04b], enabling direct packet exchange between a CN and a MNN without passing through any HA and without inserting extra IPv6 headers.

## 2.4. Route Optimisation for NEMO proposed solutions

This section provides a survey of existing proposals on Route Optimisation for NEMO, studying the scope of the solutions, their benefits and their requirements. This analysis will help us identify unsolved problems and existing issues, that will be tackled in this PhD thesis.

Since the very beginning of the research on Network Mobility, even before the IETF NEMO Working Group had been created, Route Optimisation was a hot-topic[11]. A plethora of solutions trying to enable network mobility support in an optimal way has been proposed since the beginning of the NEMO research. Next, most relevant proposals are briefly summarised, classifying them by the type of Route Optimisation they target at.

### 2.4.1. Angular Route Optimisation

Angular routing is caused by the MRHA bidirectional tunnel introduced by the NEMO Basic Support protocol, since packets of a communication involving a MNN have to be forwarded through the HA of the NEMO (see Figure 2.1). Depending on the type of the target MNN, two different Route Optimisation types of schemes for angular routing are considered: Angular Route Optimisation for Local Fixed Nodes and for Visiting Mobile Nodes.

#### 2.4.1.1. Angular Route Optimisation for Local Fixed Nodes

Since LFNs do not have any mobility support, attempts to optimise their traffic should be developed without requiring support from the LFN itself.

Authors of [LJP03], [EOB+02] propose to allow the Mobile Router directly to inform the CN of the location of the Mobile Network Prefix (using the so-called Prefix Scope Binding Update, PSBU) [EMU03]. So far, this is simply a direct extension of the MIPv6 Route Optimisation procedure to the NEMO case. However, the security mechanism used for

[10] Some authors [NTWZ06], [NZWT06] consider this case as a particular one of nested mobility.

[11] Before the IETF NEMO WG was finally created, it was thought that the working group would be chartered to work on Route Optimisation issues. However, given the complexity of this topic (the design of a secure but still deployable Route Optimisation solution for Mobile IPv6 delayed the standardisation process several years), the IETF considered that it was too early to standardise a Route Optimisation protocol, so it focused the NEMO WG charter on the base specification. On the other hand, there are some researchers that claim that current Mobile IPv6 standard [JPA04] would support network mobility without any modification (although this is because there are some parts of the Mobile IPv6 specification that are not well defined and gives some room to the developer understanding).

securing Route Optimisation in Mobile IPv6 cannot be directly applied to this case. In Mobile IPv6, Binding Update messages are secured through the Return Routability procedure [JPA04], [NAA+05], that verifies the collocation of the HoA and the CoA. In the case of a prefix, it is unfeasible to verify that all the addresses contained in the prefix ($2^{64}$ addresses) are collocated with the CoA contained in a Binding Update message. In order to overcome this difficulty, a Return Routability Procedure for Network Prefix (RRNP) [NH04a] has been proposed, which consists in performing the MIPv6 Return Routability procedure with a randomly selected address from the Mobile Network Prefix. The main problem of this solution is that it requires changing the operation of the CNs (that is, all the nodes of the Internet) to support the new option. This, of course, has a serious impact on the deployment of the solution.

A different approach to enable Angular Route Optimisation in NEMO is based on the Mobile Router performing Route Optimisation with Correspondent Routers (CRs) located at the Internet infrastructure. This approach is basically an extension of the NEMO Basic Support protocol, allowing the MR to send location update messages (kind-of Binding Updates) to a CR as well. When a CR receives the Binding Update, it can set up a bidirectional tunnel with the Mobile Router (using the MR's CoA as the end-point address) and add a route to its routing table (and even scatter the route to small portions of Internet), so packets with destination the Mobile Network Prefix of the MR will be routed through this bidirectional tunnel, instead of through the Home Network of the MR. The main drawback of this approach is related to scalability. There is a trade-off, depending on the specific scenario. If there is a CR that is very close to the CN, the resulting route would be optimal, but in that case, if a MNN is communicating to several CNs located in different physical locations, then several CRs would be needed (so there is here a scalability problem, in terms of number of CRs needed). On the other hand, if the CR is not so close to the CNs, there may be less CRs, but then the optimisation would be not so optimal. Optimized Route Cache (ORC) [WW04], [WKUM03] and Path Control Header (PCH) [NCK+04] are examples of proposals following this approach.

The Global HA to HA (HAHA) protocol [TWD05], [WTD06] follows a very similar approach that enables to distribute geographically several HAs serving to the same Mobile Network, so when a NEMO – such as one deployed in an airplane – moves within a geographically large area, the MR is able to dynamically switch to the topologically closest Home Agent, avoiding the overhead of the basic NEMO protocol. There is also an approach, called Virtual Mobility Control Domain (VMCD) [WOM05], that uses HAHA and ORC together as an optimal combination to provide Route Optimisation, load balancing and path redundancy. Again, the main drawback of this kind of approach is related to scalability and deployment, as it requires (to be effective) special nodes to be deployed on the Internet at a significant number of locations. An alternative approach, suited specifically for globally moving networks (such as aircrafts), presented in [BGMBA06], proposes a mechanism to support globally distributed HAs, but without impacting on the global routing table (as HAHA does).

#### 2.4.1.2. Angular Route Optimisation for Visiting Mobile Nodes

When a Mobile IPv6 enabled host attaches to a mobile network, the Care-of Address it obtains and uses belongs to the Mobile Network Prefix of that NEMO, so although the mobile node may be performing Route Optimisation with the CNs it is communicating to, there still exists a tunnel – between the NEMO's MR and the MR's HA – introduced by the NEMO Basic Support protocol (see Figure 2.3).

Several proposals to mitigate the performance limitations of the NEMO Basic Support protocol when used to provide connectivity to Visiting Mobile Nodes are based on Prefix Delegation [TD03]. The basic idea is that a Mobile Router, when attaches to a visited network, is delegated a prefix from the access network using DHCP Prefix Delegation [TD03]. In this way, a Visiting Mobile Node may also autoconfigure its Care-of Address from this delegated prefix, and use standard Mobile IPv6 mechanism to bind its Home Address to this Care-of Address. This is the approach followed by [PSS04a], [PHS03], [PL03], [LJPK04], [PPLS06]. In [POD+04] and [aIMY05], optimisations based on hierarchical address management are proposed to reduce the signalling load but still use an optimal route.

A different approach is based on the Mobile Router acting as a Neighbour Discovery [NNS98] proxy for its Visiting Mobile Nodes. It basically works as follows, the MR configures a Care-of Address belonging to the IPv6 network prefix advertised in the visited network by its Access Router (AR), and also rely (that is, advertise) this prefix to the mobile network [JLPK04a], [JLPK04b]. In this way, by the MR acting as a Neighbour Discovery proxy on behalf of connected nodes, the entire NEMO and the visited network form a logical multi-link subnet. This enables optimal routing to a VMN attached to the NEMO, since the VMN configures as its CoA an address that belongs to the IPv6 address space from the network that the NEMO is visiting, thus avoiding the MRHA tunnel.

The main problem of both – Prefix Delegation and Neighbour Discovery proxy based – solutions, is that they break network mobility transparency to attached Local Fixed Nodes, since a new prefix is advertised in the NEMO every time the MR moves to a new visited network.

### 2.4.2. Multi-angular Route Optimisation

Multi-angular routing is caused in nested NEMOs by the chain of nested MRHA bidirectional tunnels that packets should traverse. The different Multi-angular Route Optimisation target scenarios that we may have in Network Mobility are analysed next.

#### 2.4.2.1. Multi-angular Route Optimisation for nested-NEMO-to-Internet communications

When a MNN attached to a nested NEMO communicates to a CN located in the Internet, the packets of such communication traverse a chain of MRHA tunnels because of the nesting of MRs (see Figure 2.2).

Ref. [TM04a] proposes a solution to alleviate this inefficiency. The proposal requires modifications in MRs and HAs, but not in LFNs, VMNs, or CNs. The idea is the following: for packets going out of the nesting, the first MR in the path, in addition to tunnelling the packet to its HA with a header with source address its own CoA and destination address its

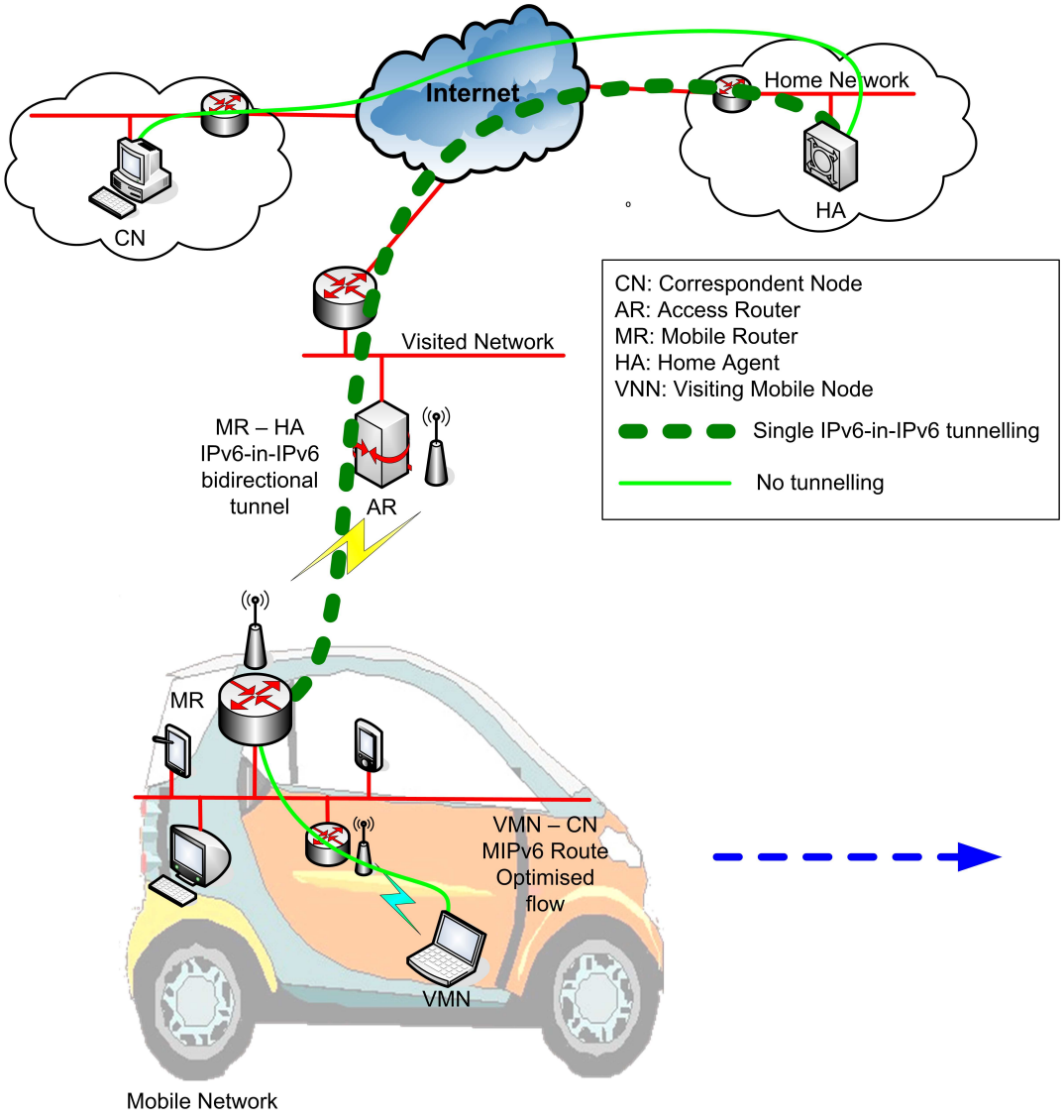


Figure 2.3: Mobile IPv6 enabled host (performing Mobile IPv6 Route Optimisation with a Correspondent Node) inside a mobile network.

Home Agent address, it also includes in the outer header of packets a new type of Routing Header, called Reverse Routing Header (RRH), where it inserts its own Home Address and empty slots where the rest of the MRs in the path can introduce their respective CoAs. This proposal requires the use of Tree Discovery [TM04b] to allow the MRs to find out the level of hierarchy within the nesting where the MR is (that is, the number of slots required).

The rest of the MRs change the source address of the outer header and include their own CoAs, but put the old source address (the CoA of the previous MR) in the Reverse Routing Header. When the packets leave the nesting, they are forwarded to the HA of the first MR in the path. This HA decapsulates the packets and sends them to their destination (it uses the Home Address included in the RRH to find out or create the right Binding Cache Entry),

but also keeps associated to the respective Binding Cache Entry the information contained in the Reverse Routing Header. This information allows the HA to include in the outer header of packets addressed to a node in the nesting, a Routing Header indicating how the packet must be routed inside the nesting (the CoAs of the MRs in the nesting in the order that must be traversed). The final result is that packets in each direction go through only one tunnel and one Home Agent, although some processing is added in the HA and MRs, plus the extra overhead of the information added to the packets.

A similar approach is proposed in [NH04b]. Each MR sends a Binding Update towards its HA with an Access Router Option (ARO) including the Home Address of the access router (that can be a fixed or a Mobile Router) it is currently attached to (the HoA is learnt from a new Router Advertisement – RA – option included in RA messages sent by routers supporting the ARO mechanism). This signalling allows HAs to learn the actual chain of Mobile Routers towards a certain MR. This enables forwarding packets from the MR's HA to the MR without traversing the HAs of the parent-MRs of the nested NEMO hierarchy, but directly to the root-MR's CoA. This is done by using an extended (so that it can store more than one address) Type 2 Routing Header [JPA04] containing the CoAs of all MRs in the nested path. In the other direction, the MR changes the source address of the packets to its CoA and sends them to their destinations.

Authors of [NCK+03] claim the the ARO solution is very complex and that RRH has security vulnerabilities, so they propose a similar solution that make use of concepts already present in both previous solutions. Basically, a MR attached to a nested NEMO is able to learn the CoA of every MR in the chain of parent-MRs from the root-MR, by means of a new Router Advertisement option (flooded from the root-MR to sub-MRs in the nesting hierarchy), and then send a Binding Update to its HA with a new option, called Nested Path Information (NPI), that contains the previously learnt array of parent-MR's CoAs.

There are several proposals that follow a Hierarchical Mobility management, based on the Hierarchical Mobile IPv6 (HMIPv6) protocol [SCMB05], such as [CPC04] and [OST03]. Basically, in these mechanisms the root-MR acts as a kind-of HMIPv6 Mobility Anchor Point (MAP), to which sub-MRs register (using their CoAs as Local Care-of Addresses, LCoAs). Each sub-MR of the nested NEMO uses the root-MR's CoA as a Regional Care-of Address (RCoA) when registering to its HA, so packets from external CNs are directly tunnelled from the destination MR's HA to the root-MR (without traversing any other sub-MR's HA) and then tunnelled to the destination MR. At the root-MR, packets tunnelled from sub-MRs are tunnelled directly to the CN. A similar HMIPv6-like approach is also proposed in [KKH+03]. Authors of [CKC06] follow an approach similar to NPI and HMIPv6-like approaches, but avoiding BU signalling storms and proposing a mechanism to reduce handoff latencies.

There exist some other NEMO Route Optimisation approaches targeting at nested scenarios. In [GYK04], the PSBU approach [LJP03], [EOB+02] is modified to support nesting, by extending the PSBU message to carry a list of MR's CoAs. In [WWEM05], extensions to the ORC protocol [WW04], [WKUM03] are proposed to support nested configurations.

It is worth mentioning that some of the mechanisms proposed to enable Angular Route Optimisation for Visiting Mobile Nodes attached to a NEMO are also applicable to the multi-angular routing problem when several nested mobile networks are considered [NH04b], [OST03].

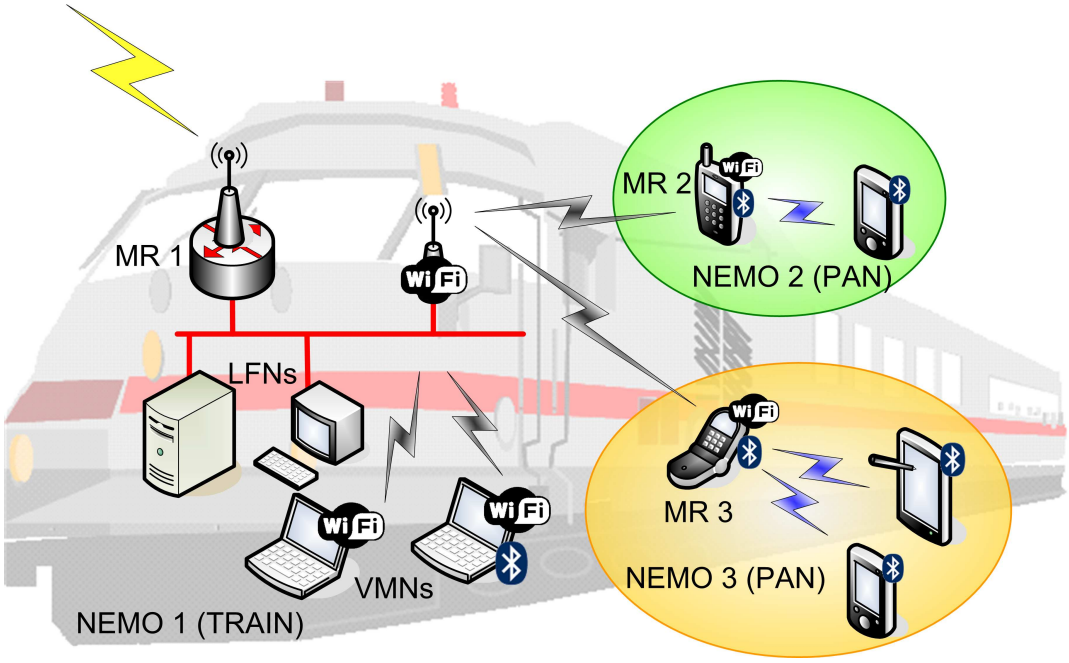


Figure 2.4: Example of intra-nested NEMO scenario: train.

The main drawback of all of these solutions is their high complexity. Another problem is that many of them are not compatible with the NEMO Angular Route Optimisation mechanisms proposed so far, thus making impossible to remove all MRHA tunnels involved in a communication, and forcing packets to traverse at least one.

#### 2.4.2.2. Multi-angular Route Optimisation for intra-nested-NEMO communications

There are several scenarios in which MNNs from different mobile networks belonging to the same nested NEMO communicate. Using the NEMO Basic Support protocol, such communications go through the infrastructure (traversing involved HAs), although MNNs would communicate far more efficiently if they did directly. Furthermore, if there was a communication problem with any of the HAs, the communication would stop, even though a direct communication between the mobile networks was possible. An example to understand the importance of such scenario is two passengers that get into the same train with their respective personal area networks and want to play with each other or exchange documents (see Figure 2.4).

In order to avoid traffic being injected out of the nested mobile network in this kind of scenario (and therefore reducing the delay and improving the reliability), some mechanisms have been proposed that try to route packets directly within the nested NEMO.

Basically, the approach followed by most of the existing proposals consists in making MRs of a nested NEMO be aware of all the MNPs that are reachable within the NEMO. One way of achieving that is by running a routing protocol among the MRs within the nested NEMO. In this way, information about the MNPs of every NEMO is exchanged, allowing MRs to learn direct routes to all the MNPs that are reachable in the nested

NEMO. Usually, an ad-hoc [AWW05], [CCL03], [CM99] routing protocol is used, such as in [CBW05]. Other proposed solutions that suggest using some kind of routing protocol within a nested NEMO to provide intra-NEMO Route Optimisation are [WWEM05], [PPK+04] and [BYK+05]. The main problem of this kind of solution is that it has security vulnerabilities, allowing several attacks to be easily performed.

# Capítulo 2

# Movilidad de Redes: haciendo ubicuo el acceso a Internet

Este capítulo presenta una descripción detallada del problema de la movilidad de redes, describiendo las soluciones actualmente propuestas, así como identificando problemas abiertos y aspectos aún no explorados.

## 2.1. Introducción

De la mano del éxito de las comunicaciones celulares, la movilidad ha cambiado la forma en que los usuarios se comunican. Ubicuidad y Heterogeneidad [CSB+04], [CSM+05], [ABB+06] serán dos aspectos clave en las futuras redes de 4ª Generación (4G) [HY03], las cuales se espera permitan que los usuarios se puedan comunicar en todo momento y desde casi cualquier lugar.

Impulsada por esas necesidades y el hecho de que los protocolos de Internet actualmente implantados no soportaban movilidad de ningún tipo, la comunidad científico-técnica diseñó varias soluciones dirigidas a solventar el problema de la movilidad [Hen03]. Se pueden seguir diferentes aproximaciones, aunque una primera clasificación podría hacerse en base a la capa de la torre de protocolos en la que se gestiona la movilidad. Las redes celulares permiten la movilidad de los usuarios entre diversas celdas, mediante una gestión de la movilidad basada en soluciones específicas de nivel 2. Por un lado, este tipo de solución tiene un rendimiento bastante bueno, si bien, por otro, limita la movilidad a una única tecnología de acceso. Si se quiere explotar la heterogeneidad de las futuras redes, la movilidad debe gestionarse en una capa que sea independiente de la tecnología (esto es, IP o superior). Aunque es posible gestionar la movilidad en los niveles de aplicación o transporte [SB00], [SBK01], esto obligaría a desarrollar diferentes soluciones, una para cada aplicación o protocolo de transporte. Por lo tanto, la capa IP parece ser la más adecuada para gestionar la movilidad.

Las redes IP no fueron pensadas para entornos de movilidad. Tanto en IPv4 como en IPv6 las direcciones IP cumplen dos papeles. Por un lado son un localizador que indica, en base a un sistema de encaminamiento, cómo llegar al terminal que la está usando. El sistema de encaminamiento mantiene información de cómo llegar a conjuntos de direcciones que comparten un prefijo de red. Esta agregación de direcciones en el sistema de encamina-

miento sirve para garantizar su escalabilidad. Pero por otro lado, las direcciones IP también actúan como parte de los identificadores de los extremos de una comunicación, y los niveles superiores usan los identificadores de los dos extremos de una comunicación para identificarla [Chi99], [LD03].

Este doble papel de las direcciones IP impone restricciones a la movilidad, pues al mover un terminal de una parte de la red (una subred IP) a otra, querríamos por un lado mantener la dirección IP asociada al terminal que se mueve (a una de sus interfaces de red) para no cambiar el identificador que los niveles superiores están usando en sus sesiones (comunicaciones) abiertas, pero por otro lado necesitamos cambiar la dirección IP para utilizar una que sea topológicamente correcta para la nueva localización del terminal en la red y que así permita al sistema de encaminamiento llegar a él.

Protocolos como el Protocolo de Configuración Dinámica de Terminales (Dynamic Host Configuration Protocol, DHCP) [Dro97], [DBV+03] hicieron posible la *portabilidad* de terminales, pero esto no era suficiente para lograr una movilidad real y transparente, ya que era necesario reiniciar las sesiones de transporte existentes tras cambiar de punto de conexión a la red. El problema de la *movilidad* de terminales en redes IP ha sido estudiado durante mucho tiempo en el IETF[1], y existen soluciones que la hacen posible a nivel IP, tanto para IPv4 [Per02] como para IPv6 [JPA04], sin que sea necesario interrumpir las sesiones existentes.

A medida que la Internet se hace más y más ubicua, la demanda de movilidad deja de estar restringida a terminales individuales. Existe también la necesidad de soportar el movimiento de toda una red que cambia su punto de acceso a la infraestructura fija, manteniendo las sesiones de todos los dispositivos que están en la red: es lo que se conoce con el nombre de *movilidad de redes* IP. En este caso la red móvil contará al menos con un router (móvil) que se conecte a la infraestructura fija y a través del cual obtendrán conectividad hacia el exterior los dispositivos de la red móvil.

El soporte de movilidad de redes completas es necesario para hacer posible la provisión transparente de acceso a Internet en plataformas móviles [LJP03], como por ejemplo:

- Medios de transporte colectivos. Haría posible que los usuarios de trenes, aviones, barcos, etc. puedan subir con sus propios terminales (portátiles, teléfonos, PDAs, etc.) y obtener acceso a Internet a través del router móvil proporcionado por el medio de transporte, que es el que se encargará de la conectividad con la infraestructura fija.

- Redes Personales. Los dispositivos electrónicos que los usuarios pueden llegar a llevar encima: PDAs, cámaras de fotos, etc. pueden obtener conectividad a través de un teléfono móvil que actuaría como router móvil de la red personal.

- Escenarios vehiculares. Los coches en el futuro se beneficiarán de tener conectividad a Internet, no sólo para mejorar la seguridad (por ejemplo, mediante la utilización de sensores que pudieran controlar múltiples aspectos del funcionamiento del vehículo, interactuando con el entorno y comunicándose con el exterior), sino también para proporcionar servicios de comunicación personal y entretenimiento a través de Internet a los pasajeros.

[1] `http://www.ietf.org/`

En la actualidad, existen múltiples proyectos de investigación e industriales en funcionamiento dirigidos a estudiar y solventar los retos que propician los escenarios anteriores. La compañía constructora de aviones Boeing ha desarrollado la tecnología *Connexion by Boeing* [2] [JdLC01], que permite a las compañías aéreas proporcionar acceso IPv4 a Internet a sus pasajeros[3]. *Nautilus6*[4] es un grupo de trabajo dentro del proyecto *WIDE*[5] que está focalizado en la problemática de la movilidad de redes, proporcionando diversas implementaciones de software de movilidad de redes y realizando demostraciones de uso en entornos reales. Estos son tan sólo dos ejemplos que demuestran el interés real que existe en la actualidad en la movilidad de redes.

## 2.2. Protocolo de Soporte Básico de Movilidad de Redes

La solución de movilidad de terminales en IP – IPv6 Móvil (Mobile IPv6 [JPA04]) – por sí sola no soporta la movilidad de redes. Por ello se creó el grupo NEMO del IETF que está estudiando soluciones a nivel IP para soportar movilidad de redes en IPv6. La solución actual, llamada protocolo de Soporte Básico de Movilidad de Redes (Network Mobility Basic Support protocol) se encuentra especificada en la RFC 3963 [DWPT05].

En esta solución, una red móvil[6] es definida como una red cuyo punto de conexión a Internet varía con el tiempo (véase la Figura 2.1). Al router que da conectividad a la red móvil se le denomina Router Móvil (Mobile Router, MR) [EL06]. Se asume que la NEMO tiene una Red Hogar (Home Network) dónde reside cuando no se está moviendo. Dado que la NEMO es parte de la Red Hogar, la red móvil tiene configuradas direcciones pertenecientes a uno o más bloques de direcciones asignados a la Red Hogar: los Prefijos de Red Móvil (Mobile Network Prefixes, MNPs). Estas direcciones permanecen asignadas a la red móvil cuando ésta se encuentra fuera de su Red Hogar. Por supuesto, estas direcciones sólo tienen sentido topológico cuando la NEMO en encuentra conectada a su Red Hogar. Cuando la red móvil está fuera, los paquetes dirigidos a los Nodos de Red Móvil (Mobile Network Nodes, MNNs) siguen siendo encaminados hacia la Red Hogar. Adicionalmente, cuando la red móvil se encuentra fuera de su hogar, es decir se encuentra visitando una red foránea, el MR obtiene una dirección temporal perteneciente a la red visitada, llamada Care-of Address (CoA), dónde la infraestructura de encaminamiento puede entregarle paquetes sin necesidad de ningún mecanismo adicional.

Existen diferentes tipos de Nodos de Red Móvil: Nodo Local Fijo (Local Fixed Node, LFN) que es un nodo que no tiene software específico de movilidad; Nodo Móvil Local (Local Mobile Node, LMN) que es un nodo que implementa el protocolo de movilidad IP de terminales y tiene su red hogar en la red móvil; y Nodo Móvil Visitante (Visiting Mobile

[2] `http://www.connexionbyboeing.com/`

[3] La solución consiste básicamente en emplear BGP como solución de movilidad, mediante el uso de la tabla de rutas global y el anuncio y borrado selectivo de rutas a medida que se mueven los aviones [Dul05], [BB04], [Dul06].

[4] `http://www.nautilus6.org/`

[5] `http://www.wide.ad.jp/`

[6] La terminología anglosajona utiliza el termino NEMO para referirse tanto a 'Movilidad de Redes' (NEtwork MObility), como a 'Red que se Mueve' (NEtwork that MOves). En la presente Tesis, se empleará en ocasiones dicho término para referirse a cualquiera de sus dos posibles acepciones.

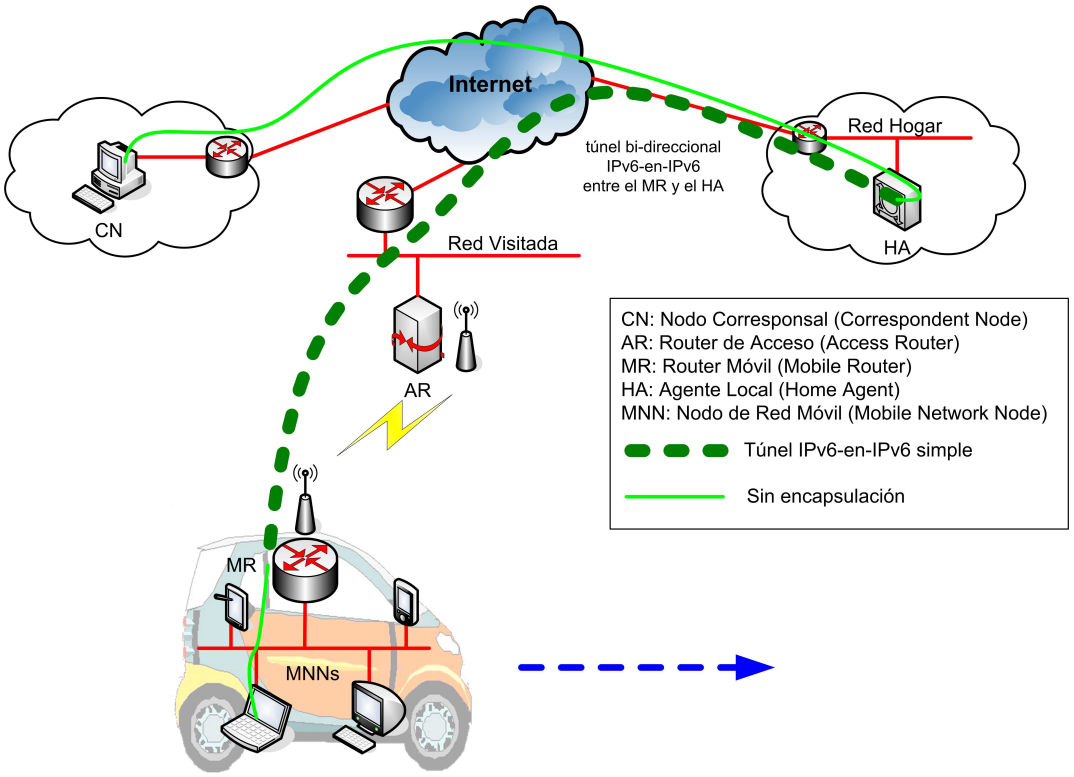


Figura 2.1: Funcionamiento del protocolo de Soporte Básico de Movilidad de Redes.

Node, VMN) que es un nodo que implementa el protocolo de movilidad de terminales, tiene su red hogar fuera de la red móvil, y está visitando la red móvil.

El objetivo de los mecanismos de soporte de movilidad de redes [Ern05] es preservar las comunicaciones establecidas entre MNNs y Nodos Corresponsales (Correspondent Nodes, CNs) externos, a pesar del movimiento de la red. Los paquetes pertenecientes a dichas comunicaciones serán dirigidos hacia las direcciones de los MNNs, las cuales pertenecen al MNP, por lo que se requieren mecanismos adicionales para reenviar dichos paquetes desde la Red Hogar hacia la red móvil.

La solución básica (ver la Figura 2.1) para el soporte de movilidad de redes en IPv6 [DWPT05] es conceptualmente similar a la de movilidad de terminales. Se basa en la creación de un túnel bi-direccional entre el MR y su Agente Local (Home Agent, HA). El HA está situado en la Red Hogar de la red móvil, es decir en un punto donde el direccionamiento de la red móvil es correcto topológicamente. Todo el tráfico destinado a la red móvil llega a su HA que lo reenvía por el túnel hacia el MR. El MR elimina la cabecera del túnel y reenvía el tráfico hacia su destinatario dentro de la red móvil. El tráfico que sale de la red móvil es enviado por el MR a través del túnel hacia el HA, el HA elimina la cabecera del túnel y reenvía los paquetes hacia su destino.

El protocolo es bastante similar a la solución propuesta para soportar movilidad de terminales, IPv6 Móvil (MIPv6) [JPA04], sin incluir el soporte de optimización de rutas (Route Optimisation, RO). De hecho, el protocolo extiende el mensaje Binding Update (BU) para

informar al Agente Local sobre la dirección IP del extremo del túnel del lado de la NEMO (es decir, la CoA del MR), a través de la cual el HA tiene que reenviar los paquetes dirigidos al MNP. Hay varias maneras por las cuales el HA puede conocer el MNP del MR: porque lo tiene configurado de forma estática, porque el MR añade la información acerca del MNP en una nueva opción del mensaje BU, o mediante la ejecución de un protocolo de encaminamiento entre el MR y el HA a través del túnel.

El protocolo de Soporte Básico de Movilidad de Redes permite que una red completa pueda moverse, pero es tan sólo el primer paso para hacer posible el despliegue de nuevas configuraciones de conectividad ubicua, que solventa solamente el problema más básico y produce algunos otros problemas que tienen que ser estudiados detenidamente. De entre estos problemas que todavía están abiertos, merece la pena mencionar los siguientes:

- **Soporte de Optimización de Rutas.** Cuando se utiliza el protocolo de Soporte Básico de Movilidad de Redes, todas las comunicaciones desde y hacia un nodo conectado a la red móvil deben ir a través del túnel bi-direccional entre el MR y el HA cuando la NEMO está fuera de casa. Debido a esto, la sobrecarga de cabeceras por paquete y la longitud de la ruta que siguen los paquetes se incrementa, lo cual implica un aumento del retardo por paquete en la mayoría de los casos. Esto puede impactar seriamente en el rendimiento de las aplicaciones que se ejecutan en los nodos de la red móvil, pudiendo incluso llegar a impedir que las comunicaciones puedan efectuarse.

- **Soporte multihoming.** Soportar configuraciones multihomed es muy importante en las futuras redes 4G, de cara a poder explotar completamente la heterogeneidad de las redes de acceso. Esto es incluso más relevante para las redes móviles, en la medida en que una pérdida de conectividad o un fallo al conectar a Internet tiene un mayor impacto que para el caso de un sólo nodo individual. Además, los escenarios de despliegue típicos, tal y como el de la provisión de acceso a Internet desde vehículos móviles, habitualmente requerirán el uso de diferentes interfaces (empleando diferentes tecnologías de acceso), ya que la NEMO puede estar moviéndose a través de localizaciones geográficas distantes, en las cuales se empleen diferentes tecnologías de acceso y estén gobernadas por distintas políticas de control de acceso [NPEB06]. Aunque existen varios trabajos publicados relativos al soporte de multihoming para redes móviles, como [PCKC04], [PCEC04], [NE04], [MEN04], [KMI+04], [EC04], [SBGE05], [MIUM05] y [Esa04], no hay ningún mecanismo que cumpla todos los requisitos de una solución de multihoming para escenarios de movilidad de redes. La aplicación del protocolo SHIM6 [BN06] para proporcionar soporte de multihoming a una NEMO es uno de los enfoques que deben ser estudiados en profundidad (un primer intento en esta línea puede encontrarse en [Bag04]).

- **Soporte multicast.** La especificación actual del protocolo de Soporte Básico de Redes Móviles no incluye el soporte necesario para la transmisión de tráfico multicast desde y hacia una red móvil. Debido a la creciente popularidad de las tecnologías broadcast, como DVB, será necesario soportar aplicaciones multicast en las futuras plataformas 4G. Unos primeros intentos de proporcionar tal soporte multicast en redes móviles puede encontrarse en [SVK+04] y [vHKBC06].

- **Soporte de traspasos eficientes.** De cara a soportar aplicaciones con requisitos de

tiempo real, no sólo el retardo extremo a extremo debe mantenerse por debajo de ciertos valores [KT01], sino también el tiempo de interrupción introducido por los traspasos. Debido a la complejidad adicional que presenta el escenario NEMO, el retardo en los traspasos puede ser mayor que para el caso de terminales individuales. La aplicación de algunas de las soluciones utilizadas para IPv6 Móvil, tal y como Traspasos Rápidos para IPv6 Móvil (Fast Handovers for Mobile IPv6 [Koo05]), para mitigar el incremento en el tiempo de traspaso, o el diseño de nuevos mecanismos debe ser investigado [PPLS06], [HCH06], [KMW06].

- **Soporte de QoS.** Las redes móviles, debido a su naturaleza dinámica, imponen retos adicionales a la dificultad inherente de proporcionar Calidad de Servicio (Quality of Service, QoS) sobre enlaces inalámbricos. De hecho, la provisión de QoS en una NEMO requiere de mecanismos adicionales además de proporcionar QoS a los diferentes enlaces inalámbricos de la red móvil. Es necesario realizar análisis estadísticos de cara a garantizar el rendimiento requerido después de atravesar diferentes enlaces inalámbricos, cada uno de los cuales proporciona sólo garantías estadísticas. Además, es necesario diseñar nuevos mecanismos de señalización que permitan señalizar la QoS sobre un escenario tan dinámico. Una primera propuesta de protocolo de reserva adaptado a una red móvil puede encontrarse en [TL05].

- **Soporte de Autenticación, Autorización y Contabilidad (AAA).** El escenario de movilidad de redes propicia nuevos retos en los esquemas clásicos de Authentication, Authorisation and Accounting (AAA) [ZEB+05]. Este aspecto debe ser analizado detenidamente, prestando especial atención a escenarios reales de despliegue de AAA en redes móviles [FSK+06].

Si bien todos los aspectos descritos anteriormente son relevantes, la problemática de la optimización de rutas es la más crítica, ya que puede llegar incluso a impedir que las redes móviles se implanten en escenarios reales. Por lo tanto, es muy importante trabajar en este problema. Uno de los objetivos principales de la presente Tesis Doctoral es solventar el problema de la optimización de rutas para escenarios de despliegue de redes móviles reales, mediante un análisis exhaustivo del problema, el diseño de una solución, su validación y una posterior evaluación de su rendimiento.

## 2.3. El problema de la Optimización de Rutas en Redes Móviles

Mediante el uso de un túnel bi-direccional entre el Router Móvil y el Agente Local, el protocolo de Soporte Básico de Movilidad de Redes [DWPT05] posibilita que los Nodos de Red Móvil puedan alcanzar y sean alcanzables desde cualquier nodo en Internet. Sin embargo, esta solución presenta importantes limitaciones de rendimiento [NTWZ06], tal y como será descrito en esta sección.

La solución básica para el soporte de movilidad de redes obliga a que – siempre que la red móvil esté fuera de su red hogar – todo el tráfico con destino a un nodo de la red móvil tenga que pasar por su HA y ser reenviado a la red móvil por el túnel establecido entre el MR y el HA. El mismo trayecto, pero en sentido inverso, es seguido por el tráfico originado en la red móvil. Esta configuración, conocida como encaminamiento triangular, impone

ciertas ineficiencias tanto en latencia como en caudal, que pueden no ser aceptables para algunas aplicaciones. De manera más precisa, podemos resaltar las siguientes limitaciones de la solución básica [DWPT05]:

- Fuerza un **encaminamiento subóptimo** (conocido también como encaminamiento triangular), es decir, los paquetes son siempre enviados a través del HA, siguiendo un camino subóptimo y añadiendo por lo tanto un retardo en la entrega de los paquetes. Este retardo puede ser despreciable si la red móvil o el Nodo Corresponsal están cerca del Agente Local (es decir, cerca de la Red Hogar). Por otro lado, cuando la red móvil y/o el Nodo Corresponsal están lejos del Agente Local, el incremento en el retardo puede llegar a ser muy grande. Esto puede tener un impacto muy serio en las aplicaciones con requisitos de tiempo real, en las cuales las condiciones temporales del retardo son muy importantes. En general, un incremento en el retardo puede también afectar al rendimiento de protocolos de transporte como TCP, debido a que la tasa de envío de TCP está parcialmente determinada por el tiempo de ida y vuelta (Round Trip Time, RTT) percibido por los participantes de la comunicación. Un ejemplo representativo sobre cuánto de grande puede ser el impacto en el retardo puede encontrarse en las comunicaciones desde aviones, dónde una comunicación con IP móvil empleando un túnel necesita de casi 2 segundos para completar un inicio de conexión en 3 mensajes (triple handshake) de TCP [BB04], [Dul06].

- Introduce una **sobrecarga de cabeceras** por paquete no despreciable, reduciendo el PMTU (Path MTU) y la eficiencia en el uso del ancho de banda. En concreto, se añade una cabecera IPv6 (40 octetos) a cada paquete debido al túnel bi-direccional entre MR y HA.

  El efecto de esta sobrecarga puede ser analizado por ejemplo examinando una comunicación de Voz sobre IP (Voice over IP, VoIP) que utilice la famosa aplicación Skype [7]. Skype [BS04] emplea el códec iLBC (internet Low Bitrate Codec) [ADA+04], que es un códec de voz abierto adecuado para comunicaciones robustas de voz sobre IP. Si se utiliza una longitud de trama de codificación de 20 ms (como en la RFC 3550 [SCFJ03]), la tasa de carga útil es 15.20 kbps. Debido a la cabecera IPv6 adicional (320 bits extra por paquete, 50 paquetes por segundo usando este códec), la tasa binaria empleada por esta comunicación es incrementada en 16 kbps (que es más que la carga útil de VoIP).

- El HA se convierte en un **cuello de botella** para la comunicación, así como un punto único de fallo. Incluso si existe un camino de comunicación directo entre un MNN y un CN, si el HA (o el camino entre el CN y el HA o entre el HA y el MR) falla, la comunicación se interrumpe. Un HA o una Red Hogar congestionados pueden ser causa de retardo adicional o incluso de pérdida de paquetes. El efecto de la congestión es doble: por un lado afecta a los paquetes de datos, haciendo que sean retrasados o incluso descartados. Por otro lado, el retraso o descarte de paquetes de señalización (p.e., mensajes BU) puede afectar al establecimiento de los túneles bi-direccionales, originando que el tráfico de datos que atraviesa dichos túneles sufra interrupciones.

[7] `http://www.skype.com/`

Ref. [NTWZ06] describe también más limitaciones, como el incremento en el retardo de procesamiento, el aumento de las posibilidades de que los paquetes sean fragmentados y el aumento en la susceptibilidad de fallos en los enlaces.

La mayoría de estos problemas existe también para el caso de movilidad de terminales usando IPv6 Móvil [JPA04]. Para solventarlos, un mecanismo de *Optimización de Rutas* fue diseñado e incluido como parte del protocolo básico. En IPv6 Móvil, la optimización de rutas se consigue permitiendo que el Nodo Móvil (Mobile Node, MN) pueda enviar también mensajes BU a los CNs. De esta forma, el CN conoce también la dirección CoA en la que la Dirección Hogar (Home Address, HoA) del MN está alcanzable. El procedimiento de comprobación del Camino de Retorno (Return Routability, RR) se definió para probar que un MN realmente tenía asignadas (es decir, *poseía*) tanto la Dirección Hogar como la dirección CoA en un momento concreto de tiempo [NAA+05].

El escenario de Movilidad de Redes tiene una serie de aspectos adicionales que hacen el problema más complejo y difícil de resolver[8].

Estos problemas de rendimiento se ven amplificados en el caso de que la red móvil esté *anidada*. Se dice que una red móvil está anidada cuando una red móvil se conecta a otra red móvil y obtiene conectividad a través de la misma (ver Figura 2.2). Un ejemplo de aplicación de esto último es un usuario que entra en un vehículo con su red de área personal (Red Móvil 2) y esa red se une, a través de un MR, por ejemplo una PDA con acceso WiFi, a la red del vehículo (Red Móvil 1) que a su vez se une a la infraestructura fija de la red.

El grupo de trabajo NEMO ha definido cierta terminología de utilidad [EL06] relativa al escenario anidado. La red móvil que se encuentra más arriba en la jerarquía, proporcionando conectividad a Internet a la red móvil anidada agregada recibe el nombre de *root-NEMO* (por ejemplo, la Red Móvil 1 en la Figura 2.2). De manera similar, el Router Móvil de la root-NEMO se denomina *root-MR*[9] (por ejemplo, MR1 en la Figura 2.2). En una configuración anidada, la red móvil que proporciona acceso a Internet a otra red se llama *parent-NEMO* y la red que recibe la conectividad *sub-NEMO* (en la Figura 2.2, la Red Móvil 1 es una parent-NEMO de la Red Móvil 2 – que por lo tanto es una sub-NEMO de la primera). Análogamente, los MRs de la parent-NEMO y la sub-NEMO se denominan, *parent-MR* y *sub-MR* respectivamente (por ejemplo, MR 1 y MR 2 en la Figura 2.2).

La utilización del protocolo de Soporte Básico de Movilidad de Redes en configuraciones anidadas amplifica los efectos subóptimos en el encaminamiento y disminuye el rendimiento de la solución, debido a que en estos escenarios los paquetes son enviados a través de todos los HAs de todos los MRs de niveles superiores en el anidamiento (lo que se conoce como encaminamiento multi-angular o pinball, véase la Figura 2.2). Esto es debido a que cada sub-NEMO obtiene una CoA que no es topológicamente válida, ya que la parent-NEMO tampoco está en su Red Hogar y los paquetes destinados a la dirección CoA son encapsulados – aumentando la sobrecarga de cabeceras – hacia el HA de la parent-NEMO.

Hay un escenario particular de movilidad de redes más que debe ser analizado. Dicho escenario se da cuando un terminal con soporte de IPv6 Móvil se conecta a una red móvil

[8] Esta situación hizo que el IETF decidiera afrontar el problema de la optimización de rutas para redes móviles de forma separada, no incluyendo el desarrollo de una solución de optimización de rutas como uno de los puntos del chárter del grupo de trabajo NEMO, sino tan sólo el análisis del problema y el espacio de soluciones.

[9] Algunos autores utilizan de forma alternativa el término TLMR (Top Level Mobile Router) para referirse al root-MR.

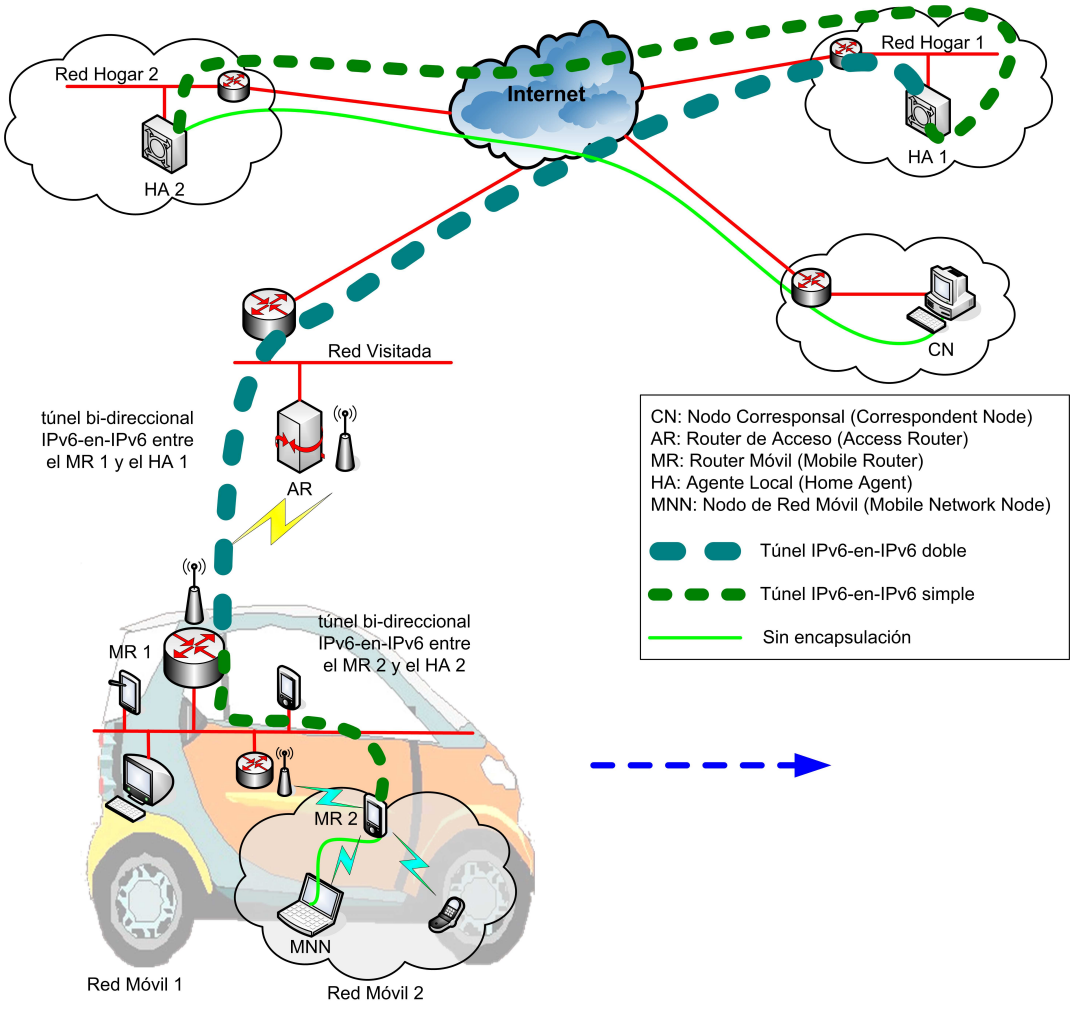


Figura 2.2: Red Móvil anidada. Funcionamiento del protocolo de Soporte Básico de Movilidad de Redes (encaminamiento multi-angular).

(convirtiéndose por tanto en un Nodo Móvil Visitante, VMN). El tráfico enviado hacia y desde un VMN tiene que ser encaminado no sólo a través del Agente Local del VMN, sino también a través del HA del MR de la red móvil, por lo tanto experimentando los mismos problemas de rendimiento que en una red anidada de 1 nivel[10]. Incluso si el VMN realiza el proceso de optimización de encaminamiento de IPv6 Móvil, esto solamente evitaría atravesar el HA del VMN, pero la ruta resultante seguiría sin ser óptima, ya que el tráfico continuaría siendo encaminado a través del HA del MR.

Debido a que existen varios escenarios en los que una solución de optimización de rutas podría hacer posible la conectividad – que no existiría de otra forma –, el denominado soporte de *Optimización de Rutas para Redes Móviles* es más crítico para el protocolo de Soporte Básico de Movilidad de Redes que para el protocolo IPv6 Móvil.

A la vista de todas las limitaciones identificadas en esta sección, es altamente necesario

[10] Algunos autores [NTWZ06], [NZWT06] lo consideran como un caso particular de movilidad anidada.

proporcionar soporte de optimización de rutas para redes móviles [NTWZ06], [NZWT06], [PSS04b], habilitando la comunicación directa entre un CN y un MNN, evitando atravesar HA alguno y sin añadir cabeceras IPv6 extra.

## 2.4. Soluciones propuestas para la Optimización de Rutas para redes móviles

Esta sección proporciona una clasificación de propuestas existentes de optimización de rutas para redes móviles, estudiando el ámbito de las soluciones, sus beneficios y sus requisitos. Este análisis nos ayudará a identificar problemas sin resolver, que posteriormente serán atacados en la presente Tesis Doctoral.

Desde que se comenzó a investigar en movilidad de redes, incluso antes de que se hubiera creado el grupo de trabajo NEMO en el IETF, la optimización de rutas fue un tema de investigación muy relevante[11]. Desde los comienzos de la investigación en movilidad de redes, una gran cantidad de soluciones que tratan de habilitar el soporte de movilidad de redes de forma óptima ha sido propuestas. A continuación resumimos las propuestas más relevantes, clasificándolas por el tipo de optimización de rutas a la que están dirigidas.

### 2.4.1. Optimización de Rutas Angulares

El encaminamiento angular está causado por el túnel bi-direccional entre el MR y el HA introducido por el protocolo de Soporte Básico de Movilidad de Redes, debido a que los paquetes de una comunicación de un MNN tienen que ser reenviados a través del HA de la NEMO (ver Figura 2.1). Dependiendo del tipo de MNN al que van dirigidas, se consideran dos tipos diferentes de esquemas de optimización de rutas angulares.

#### 2.4.1.1. Optimización de Rutas Angulares para Nodos Locales Fijos

Dado que los LFNs no tienen ningún tipo de soporte de movilidad, cualquier intento para optimizar su tráfico debe ser desarrollado sin necesitar soporte del propio LFN.

Los autores de [LJP03], [EOB+02] proponen permitir que Router Móvil informe directamente al CN sobre la localización del Prefijo de Red Móvil (utilizando el denominado Prefix Scope Binding Update, PSBU) [EMU03]. Hasta ahora, esto es simplemente una extensión directa del procedimiento de optimización de rutas de IPv6 Móvil para el caso de redes móviles. Sin embargo, los mecanismos de seguridad empleados para asegurar la optimización de rutas en IPv6 Móvil no pueden aplicarse directamente a este caso. En IPv6

[11] Antes de que el grupo de trabajo NEMO del IETF fuera creado, se pensaba que éste iba a trabajar en la problemática de optimización de rutas. Sin embargo, dada la enorme complejidad de este tema (el diseño de una solución de segura, pero aún así desplegable, de optimización de rutas para el caso del protocolo IPv6 Móvil retrasó el proceso de estandarización del protocolo varios años), el IETF consideró que era demasiado pronto para estandarizar un protocolo de optimización de rutas en el caso de movilidad de redes, así que centró los objetivos del chárter del grupo de trabajo en la especificación básica. Por otro lado, ciertos investigadores afirman que la solución actualmente estandarizada del protocolo IPv6 Móvil [JPA04] soportaría la movilidad de redes sin ningún cambio (aunque esto es así debido a que hay algunas partes de la especificación de IPv6 Móvil que no están definidas del todo y dejan algo de espacio a interpretación del desarrollador).

Móvil, los mensajes BU son asegurados mediante el procedimiento de comprobación de Camino de Retorno (Return Routability [JPA04], [NAA+05]), que se encarga de verificar la colocación de la HoA y la CoA. En el caso de un prefijo, no es factible verificar que todas las direcciones contenidas en el prefijo ($2^{64}$ direcciones) están colocadas en la CoA incluida en el mensaje BU. Para resolver este problema, se ha propuesto un procedimiento de comprobación de Camino de Retorno para Prefijos de Red Móvil (Return Routability Procedure for Network Prefix, RRNP [NH04a]), el cual consiste en realizar el procedimiento de comprobación de Camino de Retorno de IPv6 Móvil utilizando como CoA una dirección aleatoria perteneciente al Prefijo de la Red Móvil. El principal problema de esta solución es que requiere cambios en el funcionamiento de los CNs (es decir, virtualmente todos los nodos de Internet) para soportar la nueva opción del BU y el procedimiento RR extendido para MNPs. Esto, obviamente afecta seriamente al despliegue de la solución.

Un enfoque diferente para habilitar la optimización de rutas angulares en NEMO está basado en que el Router Móvil realice la optimización de rutas con Routers Corresponsales (Correspondent Routers, CRs) localizados en la infraestructura de Internet. Este enfoque es básicamente una extensión del protocolo de Soporte Básico de Movilidad de Redes que permite que el MR envíe también mensajes de actualización de localización (BUs) a un CR. Cuando un CR recibe el mensaje BU, establece un túnel bi-direccional con el MR (utilizando la dirección CoA del MR como dirección del otro extremo) y añade una entrada a su tabla de rutas (e incluso anuncia dicha ruta a pequeñas porciones de Internet), de forma tal que aquellos paquetes con destino el Prefijo de Red Móvil del MR serán encaminados a través del túnel bi-direccional, en lugar de a través de la Red Hogar del MR. El principal problema de esta aproximación está relacionado con la escalabilidad, ya que existe un cierto compromiso, dependiendo del escenario particular, entre rendimiento y escalabilidad. En aquellos casos en los que exista un CR que esté localizado muy cerca del CN, la ruta resultante será óptima, pero en ese caso, si un MNN está comunicándose con múltiples CNs localizados en diferentes localizaciones físicas, entonces se necesitarían múltiples CRs (por lo tanto hay un problema de escalabilidad, en términos del número de CRs requerido). Por otro lado, en aquellos casos en los que no se desplieguen CRs cercanos a los CNs, habría menos CRs, pero la optimización resultante no sería tan óptima. ORC (Optimized Route Cache) [WW04], [WKUM03] y PCH (Path Control Header) [NCK+04] son dos ejemplos de propuestas que siguen este enfoque.

El protocolo HAHA Global (Global HA to HA) [TWD05], [WTD06] sigue un enfoque muy similar, facilitando la distribución geográfica de varios HAs que sirven a una misma red móvil, de forma que cuando una NEMO – como la desplegada en un avión – se mueve dentro de un área geográfica muy grande, el MR es capaz de conmutar dinámicamente al Agente Local más cercano, evitando toda la sobrecarga del protocolo básico de NEMO. Existe también una propuesta, llamada Virtual Mobility Control Domain (VMCD) [WOM05], que emplea HAHA y ORC de forma combinada para proporcionar optimización de rutas, balanceo de carga y redundancia de caminos. De nuevo, el principal problema de este tipo de aproximación está relacionado con la escalabilidad y despliegue de la solución, ya que requiere (para ser efectiva) el despliegue de nodos especiales en un número significativo de localizaciones en la Internet. Un enfoque alternativo, diseñado específicamente para redes que se mueven globalmente (como los aviones), presentado en [BGMBA06], propone un mecanismo para soportar HAs globalmente distribuidos, pero sin que esto impacte en la tabla global

de rutas (como HAHA hace).

#### 2.4.1.2. Optimización de Rutas Angulares para Nodos Móviles Visitantes

Cuando un nodo ejecutando IPv6 Móvil se conecta a una red móvil, la dirección CoA que obtiene y utiliza pertenece al Prefijo de Red Móvil de dicha NEMO, por lo que aunque el nodo móvil pueda estar realizando una optimización de rutas con los CNs con los que se está comunicando, existe todavía un túnel – entre el MR de la NEMO y el HA del MR – introducido por el protocolo de Soporte Básico de Movilidad de Redes (ver Figura 2.3).

Se han propuesto diversas alternativas basadas en Delegación de Prefijos (Prefix Delegation [TD03]) para mitigar los problemas de rendimiento ocasionados cuando el protocolo de Soporte Básico de Movilidad de Redes es utilizado para proporcionar conectividad a Nodos Móviles Visitantes. La idea básica consiste en que al Router Móvil, cuando se conecta a una red visitada, se le delegue un prefijo utilizando la delegación de prefijos de DHCP [TD03]. De esta forma, los Nodos Móviles Visitantes puede configurar también una dirección CoA perteneciente al prefijo delegado, y usar el mecanismo estándar de IPv6 Móvil para asociar su dirección HoA con su dirección CoA. Este es el enfoque seguido en [PSS04a], [PHS03], [PL03], [LJPK04], [PPLS06]. In [POD$^+$04] y [aIMY05], todas ellas optimizaciones basadas en una gestión jerárquica de las direcciones para reducir la carga de señalización pero aún así conseguir una ruta óptima.

Una aproximación diferente se basa en que el Router Móvil actúe como un proxy Neighbour Discovery [NNS98] para sus Nodos Móviles Visitantes. Este enfoque funciona básicamente como sigue, el MR configura una dirección CoA perteneciente al prefijo IPv6 anunciado en la red visitada por el Router de Acceso (Access Router, AR) del que obtiene conectividad, y también anuncia dicho prefijo en la red móvil [JLPK04a], [JLPK04b]. De esta forma, mediante el MR actuando como proxy de Neighbour Discovery en nombre de los nodos conectados, la NEMO y la red visitada forman una red lógica con múltiples enlaces. Esto hace posible un encaminamiento óptimo hacia un VMN conectado a la NEMO, ya que el VMN obtiene y configura como su CoA una dirección que pertenece al espacio de direcciones IPv6 de la red que la NEMO está visitando, evitando de esta forma atravesar el túnel entre el MR y el HA.

El principal problema de ambas soluciones – las basadas en la Delegación de Prefijos y las que hacen proxy de Neighbour Discovery – es que rompen la transparencia de la movilidad de la red para los Nodos Fijos Locales conectados, ya que se anuncia en la NEMO un nuevo prefijo cada vez que que el MR se mueve a una nueva red visitada.

### 2.4.2. Optimización de Rutas Multi-angulares

El encaminamiento multi-angular en redes móviles anidadas es originado por la cadena de túneles bi-direccionales anidados entre MR y HA que los paquetes tienen que atravesar. A continuación, se analizan los diferentes escenarios de optimización de rutas multi-angulares que podemos tener en la práctica.

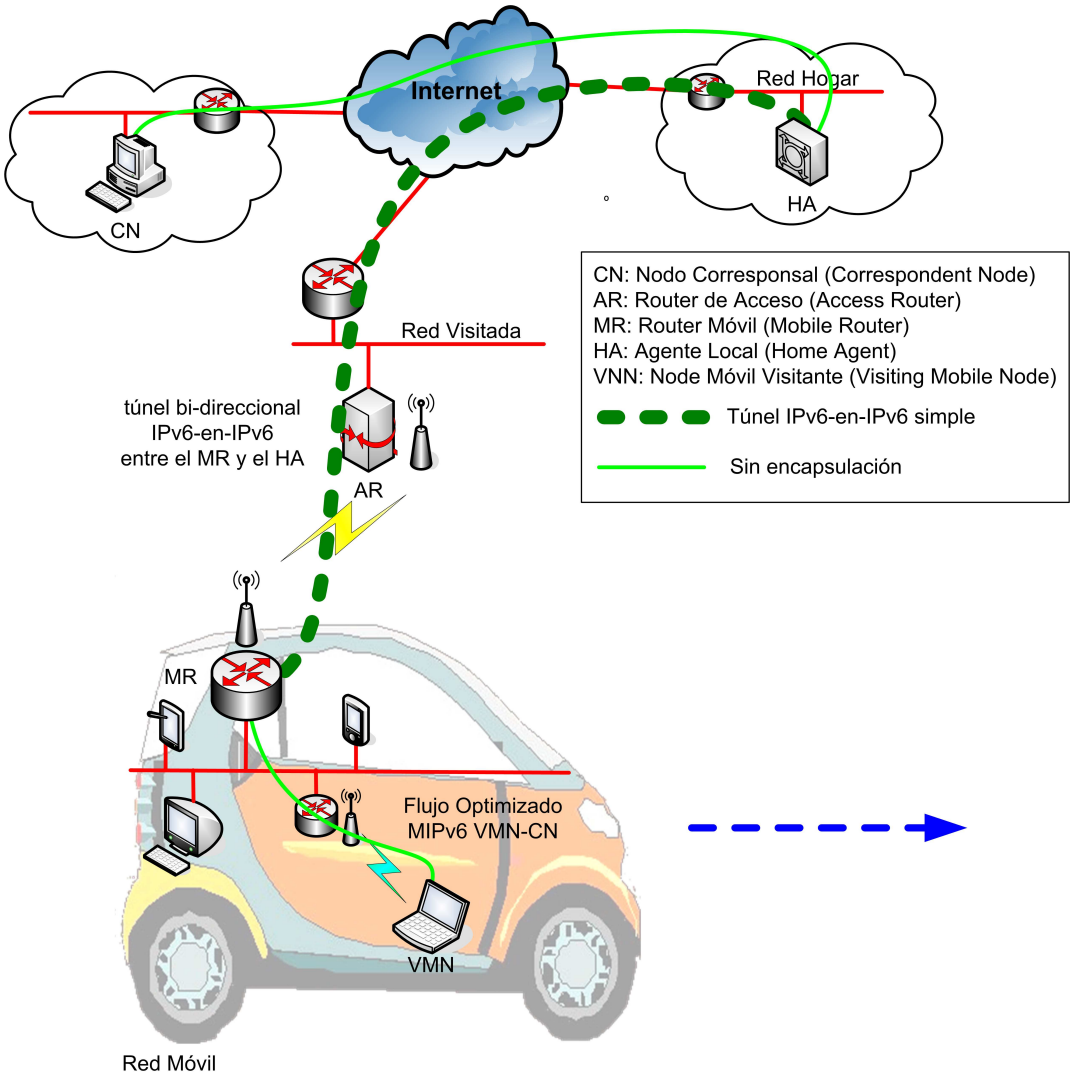


Figura 2.3: Nodo Móvil Visitante (realizando una optimización de rutas con un Nodo Corresponsal) dentro de una red móvil.

#### 2.4.2.1. Optimización de Rutas Multi-angulares para comunicaciones entre una NEMO anidada e Internet

Cuando un MNN conectado a una NEMO anidada se comunica con un CN localizado en la Internet fija, los paquetes de dicha comunicación atraviesan una cadena de túneles entre MR y HA debido al anidamiento de los MRs (ver Figura 2.2).

Ref. [TM04a] propone una solución para aliviar estas ineficiencias. La propuesta requiere modificar el funcionamiento de los MRs y los HAs, pero no de los LFNs, VMNs o CNs. La idea es la siguiente: para aquellos paquetes abandonando el anidamiento, el primer MR en el camino, además de encapsular el paquete hacia su HA con una cabecera que tiene como dirección origen su propia CoA y dirección destino la dirección de su HA, también añada en

la cabecera externa de los paquetes un nuevo tipo de Cabecera de Encaminamiento (Routing Header), llamada Reverse Routing Header (RRH), en la cuál inserta su propia Dirección Hogar y ranuras vacías en las cuales el resto de MRs en el camino introducirán sus direcciones CoA respectivas. Esta propuesta requiere el uso del protocolo Tree Discovery [TM04b] para permitir que los MRs averigüen el nivel dentro de la jerarquía en el que se encuentran (es decir, el número de ranuras que deben introducir en la cabecera RRH).

El resto de los MRs cambia la dirección origen de la cabecera exterior e incluyen sus propias CoAs, pero ponen la dirección origen anterior (la CoA del MR anterior) en la cabecera RRH. Cuando los paquetes abandonan el anidamiento, son encaminados al HA del primer MR en el camino. Este HA desencapsula el paquete y lo envía a su destino (utiliza la Dirección Hogar incluida en la RRH para averiguar o crear la entrada apropiada en la Binding Cache), pero también mantiene junto a la entrada correspondiente en la Binding Cache la información contenida en la cabecera RRH. Esta información permite al HA incluir en la cabecera exterior de los paquetes dirigidos a un nodo del anidamiento una Cabecera de Encaminamiento indicando como tiene que ser encaminado el paquete dentro del anidamiento (las CoAs de los MRs en el anidamiento en el orden en el que tienen que ser atravesados). El resultado final es que los paquetes atraviesan sólo un único túnel en cada sentido, aunque se añade cierta carga de procesamiento adicional en el HA y los MRs, además de la sobrecarga debida a la información añadida en cada paquete.

Un enfoque similar es propuesto en [NH04b]. Cada MR envía un mensaje BU a su HA incluyendo una nueva opción, llamada Access Router Option (ARO), que contiene la Dirección Hogar del router de acceso (que puede ser móvil a su vez o fijo) al que se encuentra conectado (dicha HoA se aprende mediante una nueva opción de anuncio de routers – Router Advertisement, RA – incluida en los mensajes de RA enviados por los routers que soportan el mecanismo ARO). Esta señalización permite a los HAs aprender la cadena de routers móviles hacia un determinado MR. Esto permite que el HA de un MR pueda reenviarle los paquetes directamente al MR sin atravesar los HAs de los parent-MRs en la jerarquía de la NEMO anidada, enviándolos a la CoA del root-MR. Esto se hace empleando una Cabecera de Encaminamiento de Tipo 2 extendida (de forma que pueda contener más de una dirección) [JPA04] que incluye las direcciones CoA de todos los MRs en el camino anidado. En el otro sentido, el MR cambia la dirección origen de los paquetes por su CoA y los envía hacia su destino.

Los autores de [NCK+03] afirman que la solución ARO es demasiado compleja y que RRH tiene vulnerabilidades de seguridad, por lo que proponen una solución muy similar que utiliza conceptos presentes en ambas soluciones previas. Básicamente, un MR conectado a una NEMO anidada es capaz de aprender la dirección CoA de cada MR en la cadena de parent-MRs desde el root-MR, por medio de una nueva opción de RA (distribuida desde el root-MR hacia todos los sub-MRs en la jerarquía anidada), y enviar después un mensaje BU a su HA con una nueva opción llamada Nested Path Information (NPI), conteniendo el array previamente aprendido de las CoAs de los parent-MRs.

Existen diversas propuestas que siguen un enfoque de gestión de la movilidad jerárquico, basados en el protocolo IPv6 Móvil jerárquico (Hierarchical Mobile IPv6, HMIPv6) [SCMB05], como por ejemplo [CPC04] y [OST03]. Básicamente, en estos mecanismos el root-MR actúa como una especie de HMIPv6 Mobility Anchor Point (MAP), en el cual todos los sub-MRs se registran (usando sus direcciones CoA como Direcciones CoA Locales

– Local Care-of Addresses – LCoAs). Cada sub-MR de la NEMO anidada utiliza la CoA del root-MN como Dirección CoA Regional (Regional Care-of Address, RCoA) cuando se registran con su HA respectivo, de forma que el tráfico que proviene de CNs externos es encapsulado directamente desde el HA del MR destino al root-MR (sin atravesar el HA de ningún otro sub-MR), el cuál lo encapsula hasta el MR destino. En el root-MR, los paquetes encapsulados desde los sub-MRs se encapsulan directamente al CN. Un enfoque similar a este es propuesto en [KKH+03]. Los autores de [CKC06] utilizan un enfoque similar a NPI y las soluciones basadas en HMIPv6, pero evitando las denominadas tormentas de señalización y proponiendo además un mecanismo para reducir la latencia de traspaso.

Existen otros tipos de soluciones de optimización de rutas para redes móviles anidadas. En [GYK04], el enfoque PSBU [LJP03], [EOB+02] es modificado para soportar anidamiento, extendiendo el mensaje PSBU para que contenga la lista de las CoAs de los MRs. En [WWEM05], se proponen extensiones al protocolo ORC [WW04], [WKUM03] para soportar configuraciones anidadas.

Merece la pena mencionar que algunos de los mecanismos propuestos para habilitar la Optimización de Rutas Angular para Nodos Móviles Visitantes conectados a una NEMO son también aplicables al caso del encaminamiento multi-angular producido en redes anidadas [NH04b], [OST03].

El mayor problema de todas estas soluciones es su elevada complejidad. Otro problema es que muchas de ellas no son compatibles con los mecanismos de optimización de rutas angulares propuestos hasta ahora, por lo que hacen imposible eliminar todos los túneles entre MR y HA involucrados en una cierta comunicación, forzando a que al menos se atraviese uno.

#### 2.4.2.2. Optimización de Rutas Multi-angulares para comunicaciones intra-NEMO anidada

Existen algunos escenarios en los que se comunican entre sí MNNs de diferentes redes móviles, pertenecientes todas ellas a la misma NEMO anidada. Si se emplea el protocolo de Soporte Básico de Movilidad de Redes, dicha comunicación se realiza a través de la infraestructura (pasando por los HAs que sea necesario), si bien los MNNs podrían comunicarse de una forma mucho más eficiente directamente. Además, si hubiera un problema con alguno de los HAs implicados, la comunicación se vería interrumpida, aunque existiera una comunicación directa entre las redes móviles. Un ejemplo para entender la importancia de este escenario consiste en dos pasajeros que suben al mismo tren llevando sus respectivas redes de área personal y quieren jugar entre ellos o intercambiar documentos (ver Figura 2.4).

Con objeto de evitar que el tráfico tenga que abandonar la red móvil anidada para soportar este tipo de escenario (y de esta forma reducir el retardo y mejorar la fiabilidad), se han propuesto algunos mecanismos que tratan de hacer que los paquetes se encaminen directamente dentro de la NEMO anidada.

Básicamente, la aproximación que siguen la mayoría de las propuestas consiste en hacer que los MRs de una red móvil anidada tengan conocimiento de todos los MNPs que pueden ser alcanzados dentro de la NEMO. Una manera de lograr esto consisten en ejecutar un protocolo de encaminamiento dinámico entre todos los MRs de la NEMO anidada. De esta forma, la información acerca de los MNPs de cada red móvil es distribuida, per-

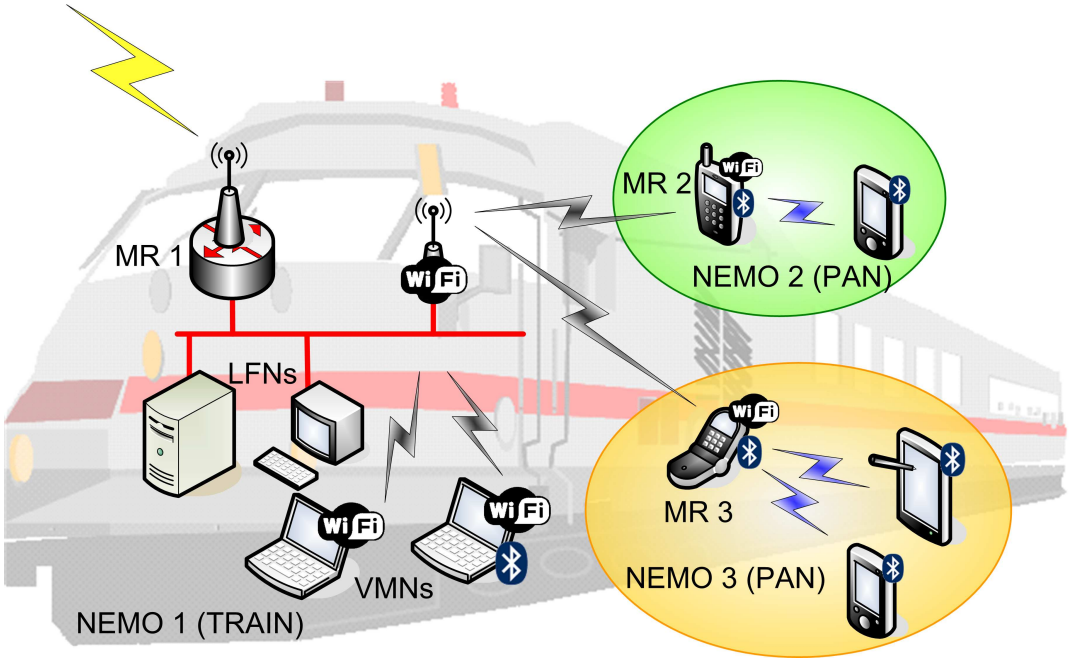


Figura 2.4: Ejemplo de escenario de comunicaciones intra-NEMO: un tren.

mitiendo que los MRs aprendan rutas directas hacia todos los MNPs que pueden ser alcanzados dentro de la NEMO anidada. Normalmente se utilizan protocolos de encaminamiento ad-hoc [AWW05], [CCL03], [CM99], como en [CBW05]. Otras soluciones propuestas que sugieren emplear alguna clase de protocolo de encaminamiento dentro de la NEMO anidada para proporcionar optimización de rutas intra-NEMO son [WWEM05], [PPK+04] y [BYK+05]. El mayor problema de esta clase de soluciones es que tienen vulnerabilidades de seguridad, haciendo posible que se puedan realizar ataques fácilmente.

# Chapter 3

# Optimising Mobile Network communications in the car-to-car scenario

In the previous chapter, several scenarios that could benefit from a network mobility approach have been presented. It is clear that the provision of Internet access from mobile platforms (such as trains, planes or buses) may be the most relevant one. Furthermore, the vehicular scenario is receiving a lot of attention from the academic and industrial research.

The particular scenario of vehicular communications is becoming more and more popular, since there are many potential applications that would benefit from having Internet connectivity capabilities in cars. Two main issues should be tackled: Internet access from cars (the so-called car-to-Internet scenario) and inter-vehicle communications (car-to-car scenario). Given the nature of vehicular scenarios and their relevance, the applicability of an optimised NEMO-based approach should be studied.

This chapter first introduces the vehicular scenario, presenting the specific challenges posed by it and analysing the approaches that are currently being proposed for this particular scenario.

## 3.1. Introduction

Many people in modern societies spend a lot of time in their cars. Communication possibilities in vehicles have been restricted in the past mainly to cellular communication networks. Enabling broader communication facilities in cars [KBS+01] is an important contribution to the global trend towards ubiquitous communications. Cars should provide access to Internet and should be able to communicate among themselves, supporting new services and applications.

There is a significant number of potential services and applications that are of interest for automobile users. In Figure 3.1 some representative examples are shown, classified into five different – but still overlapping – categories:

- **Personal communication services.** Classical telecommunication applications, such as voice communications, have to be integrated in a car. Actually, some of them are

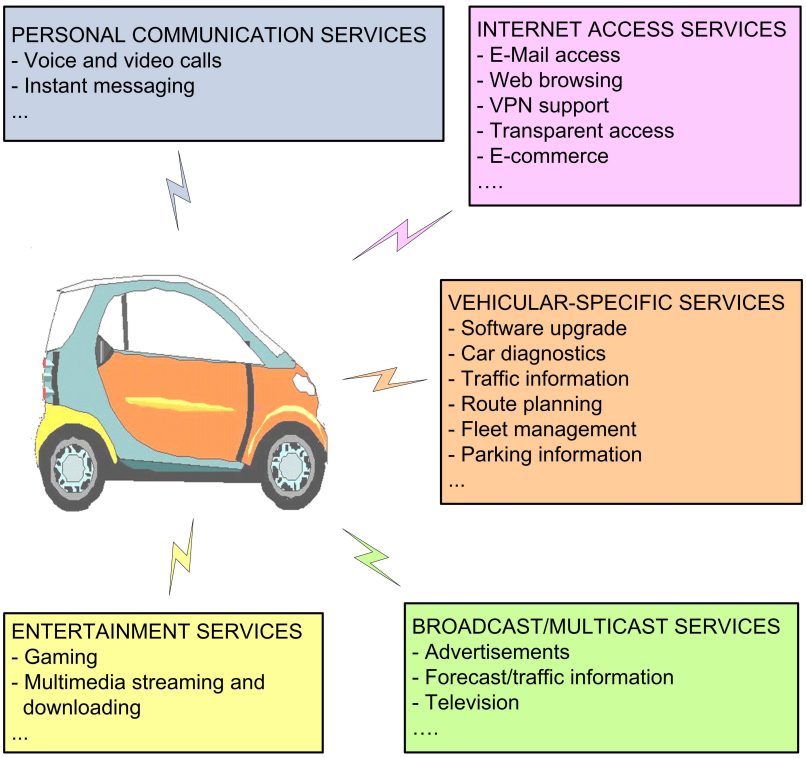


Figure 3.1: Some examples of applications and services in a vehicular scenario.

already available in cars today (e.g., hand-free communications using a car integrated cellular system). However, more complex applications are expected to be provided in forthcoming cars, taking advantage of the extended capabilities – compared to the ones of current portable communication terminals – that car's devices may have.

- **Internet access services.** Vehicles, specially public transportation systems, such as trains or buses, should enable the use of typical business applications (for example, e-mail, VPN software, etc.), by providing a transparent access to Internet, using either embedded devices or passengers' terminals.

- **Vehicular-specific services.** There exist several applications that are specific to the vehicular scenario, such as parking and traffic information retrieval, automobile monitoring and diagnostics, or upgrade and control of vehicle's software. In general, security is a key concern in some of these applications (e.g., in automobile diagnostics and software updates).

- **Entertainment services.** Multi-player gaming and multimedia streaming are already widely accepted applications, that will likely be also very important in vehicular scenarios (e.g., kids in the back-seat of a car, or commuters in a bus, playing while travelling). Besides, these services may benefit from location information.

- **Broadcast/multicast services.** Broadcasting/Multicasting of contents are also services of interest in the vehicular scenario. This kind of service will be likely provided

by using specific network technologies, such as DVB, so additional issues should be taken into account.

Therefore, cars soon will be no longer isolated systems [KBS+01], new services and applications will arise when cars are enabled to connect to the Internet and communicate among themselves [Ern06]. These new scenarios pose some challenging problems that have to be solved, mainly related to mobility management, but also to quality of service and security. Some of these problems are been addressed by projects and joint efforts, such as the following:

- The European project DRiVE[1] (1999) and its follow-up OverDriVE[2] (2001), that focused on enabling the delivery of in-vehicle multimedia services and the development of a vehicular router that provided a multi-radio access to a moving intra-vehicular network (IVAN) [LJP03], [LN03], [WS03].

- The InternetCAR project[3] (1996), investigated how vehicles could be transparently connected to the Internet. In some of the phases of the project, real trials were held (involving up to 1640 vehicles). Some results from these real experiments can be found in [EMU03], [EU02], [USM03], [WYT+05], [KLE05].

- The "Network On Wheels" (NOW) project[4] (2004) focusing on 802.11 technology and IPv6 to develop "inter-vehicle communication based on ad-hoc networking principles". Essentially, it is exploring ways so that moving vehicles can automatically set up temporary links with other cars, bikes and trucks in the vicinity, and share traffic information.

- The FleetNet ("Internet on the Road") project[5] (2000) was set up by a consortium of six companies and three universities in order to promote the development of inter-vehicle communication systems.

- The Daidalos project[6] (2002) is an EU Framework Programme 6 Integrated Project, currently in its second phase. One of its goals is to seamlessly integrate heterogeneous network technologies that allow network operators and service providers to offer new and profitable services. Mobile Networks is one of the heterogeneous network technologies that has been considered. So far, Daidalos has addressed three network mobility issues [BSC+05b], [BSC+05a]: the development of a NEMO Basic Support protocol implementation [dlOBC05], the extension of the NEMO Basic Support protocol to support also multicast traffic [vHKBC06] and the design of a Route Optimisation mechanism for NEMO [BBC04].

[1] `http://www.ist-drive.org/`
[2] `http://www.ist-overdrive.org/`
[3] `http://www.sfc.wide.ad.jp/InternetCAR/`
[4] `http://www.network-on-wheels.de/`
[5] `http://www.et2.tu-harburg.de/fleetnet/index.html`
[6] `http://www.ist-daidalos.org/`

The previously described projects are just some of the most relevant ones. There are other research efforts, such as the InternetITS project[7] [MUM03], the Car2Car Communication Consortium[8] or the CarTALK 2000[9] project. Given the amount of research efforts related to vehicular communications, it is clear that the vehicular scenario is currently a hot-topic research. Most of these major research efforts are basically working on providing solutions for the two main scenarios considered in vehicular communications:

- **Car-to-Internet communications.** This is a very common scenario, since many of the applications that are expected to be required in a vehicle involve communications between a node within the car and a peer located in the Internet (e.g., web browsing, e-mail, etc.). Initially, to address this scenario, basically only cellular radio technologies were taken into account [AVN00]. More recently, with the success of the IEEE 802.11 WLAN technology, other technologies are also being considered. It is being investigated how to overcome the limitations of existing cellular radio networks (e.g., cost, low bandwidth, high delay, etc.), by making use of IEEE 802.11 WLAN ( [LG04] presents a study about the feasibility of using IEEE 802.11 WLAN to connect trains to the Internet) and WiMAX.

- **Car-to-car communications.** There exist several vehicular applications, such as multi-player games, instant messaging, traffic information or emergency services, that might involve communications among vehicles that are relatively close to each other and may even move together (e.g., military convoys). Besides, there are several emerging applications that are unique to the vehicular environment. As an example, driver information services could intelligently inform drivers of congestion, businesses and services in the vicinity of the vehicle. These emerging services are currently not well supported. Numerous research challenges need to be addressed before inter-vehicular communications are widely deployed. These scenarios have been mostly addressed by the ad-hoc research community, since ad-hoc protocols are very well suited for targeting this kind of problem (i.e. rapidly changing topology as cars move around, no pre-established infrastructure, etc.).

Enabling connectivity in both scenarios can be done by following a generic Network Mobility solution (e.g., NEMO Basic Support protocol [DWPT05]). However, as it will be described later, the vehicular case presents some particularities making the performance of basic NEMO solutions and Route Optimisation mechanisms poor, hence requiring new optimisations approaches to be explored.

## 3.2. Enabling vehicular communications

In this section an overview of the current state of the art regarding vehicular communications is provided, classifying existing proposals into three different categories.

[7] http://www.internetits.org/
[8] http://www.car-2-car.org/
[9] http://www.cartalk2000.net/

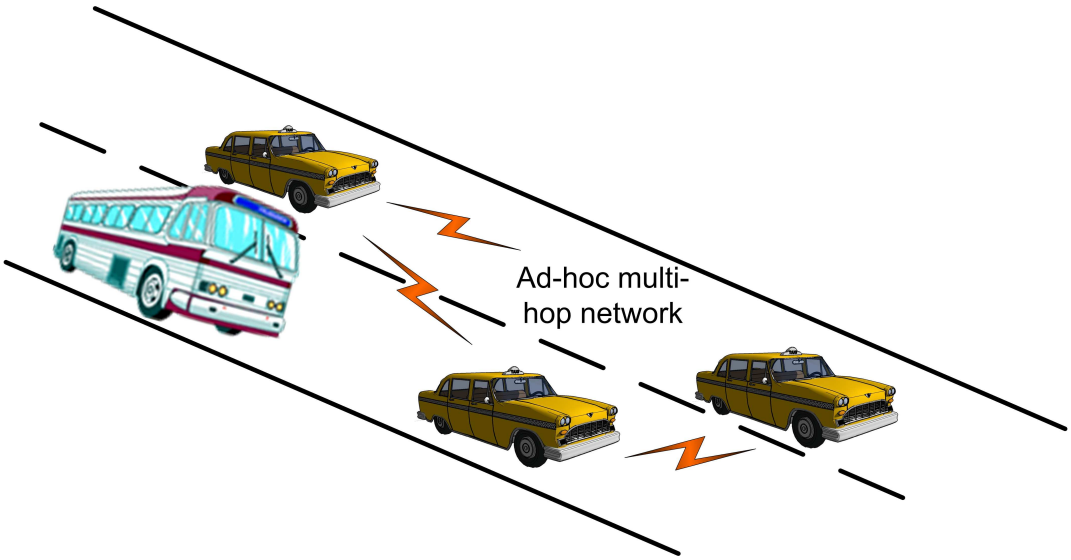


Figure 3.2: Vehicular Ad-hoc Network.

### 3.2.1. Ad-hoc centric approach

There is a large amount of research work done within the field of ad-hoc networking. Some of the mechanisms developed by the ad-hoc research community seem to be appropriate for the vehicular scenario, at least as starting point. Therefore, in the last years there have been proposed many mechanisms to enable vehicular communications based on the concept of Vehicular Ad-hoc Networks (VANETs). We classify those mechanisms that address the vehicular communications scenario by using ad-hoc solutions exclusively, without using Mobile IP mechanisms, as *ad-hoc centric*.

#### 3.2.1.1. Vehicular ad-hoc networks

Ad-hoc networking appears as an alternative to infrastructure-based networks, due to the demand of mobility and the challenge of deploying wireless access networks without *dead zones* (areas without coverage). In particular, a Mobile Ad-hoc Network (MANET) [CM99] is a group of wireless mobile devices that cooperate together to form an IP network. This network does not require any infrastructure to work, since in a MANET users' devices are the network, so a node communicates not only directly with nodes within its wireless coverage, but also with others using a multi-hop route through other MANET nodes.

A Vehicular Ad-hoc Network (VANET) is a type of ad-hoc network where nodes are located in vehicles [FTMT+05]. By setting a VANET, vehicles may communicate locally without relying on any infrastructure (see Figure 3.2).

The vehicular scenario has different characteristics from other communications networking problems. For example, on the one hand, because of the rapidly changing topology as cars move around, there are similarities with classical ad-hoc networking scenarios. However, on the other hand, the constraints and optimisations are different. First, power efficiency is not as important for inter-vehicular communications as it is for traditional ad-hoc

networking, since vehicles have a powerful and rechargeable source of energy. Second, vehicles in general are also constrained to move within roads (and within lanes most of the time).

In order to enable the scenario of Figure 3.2 to properly work, there are several challenging issues that have to be solved:

- *Routing.* In an ad-hoc network there is no pre-established routing infrastructure, so nodes have to collaborate in the set-up and maintenance of multi-hop routes. Therefore, specific routing protocols are needed for ad-hoc networks.
- *Security.* Because of the unmanaged nature of ad-hoc networks, security is a critical issue. Protocols aimed at working in ad-hoc networks have to be designed paying special attention to their possible security vulnerabilities.
- *IP address autoconfiguration.* Existing protocols for autoconfiguration of IP addresses (in infrastructure-based networks) do not work in ad-hoc networks, so new mechanisms have to be defined to support IP autoconfiguration for ad-hoc nodes.

If, in addition to car-to-car communications, it is wanted to provide Internet connectivity to VANET nodes (car-to-Internet scenario), then the following additional issue has to be addressed:

- *Internet Gateway discovery.* A special node (called Internet Gateway) connecting the ad-hoc network to the infrastructure is required. Enabling ad-hoc nodes to efficiently discover and use the Internet Gateway poses some challenges due to the nature of MANETs.

We next briefly analyse each of the previously enumerated issues.

#### 3.2.1.2. Ad-hoc routing

Ad-hoc networks have received a lot of attention in the last years [CCL03], [AWW05], [FJL00]. Due to the wireless, high mobility and multi-hop nature of the ad-hoc networks, traditional routing protocols (used in wired networks) do not perform well and therefore cannot be used in MANETs. A plethora of routing protocols have been proposed, most of them within the IETF. Some of them are known as *reactive*, because the process to find and set-up a route towards a destination is triggered when there are packets that need to be sent to that destination (such as Ad hoc On-Demand Distance Vector – AODV [PBRD03] – and Dynamic Source Routing – DSR [JMH04], [JMB01]).

There are also protocols known as *proactive* routing protocols, because the nodes proactively keep a routing entry for each reachable destination (such as Optimized Link State Routing – OLSR [CJ03]), reducing in this way the time needed to set-up a route towards a destination, though it increases the complexity of the protocol. More information about ad-hoc routing protocols can be found in [AWD04], [RT99] and [CCL03].

The performance of ad-hoc networks greatly depends on the routing protocol used and on the radio technology used for the communication. Most of the first research works related to ad-hoc networking have been done through simulation [KCC05], although there have been

also some experimental works, studying the real performance of prototypes of ad-hoc networks [MBJ01]. Some of them focus on vehicular scenarios [SBSC02], [SBS+05], showing the feasibility of deploying ad-hoc networks using IEEE 802.11b WLAN equipment. On the other hand, some authors claim that using IEEE 802.11 WLAN, going beyond 3 hops and 10 nodes is challenging [TLN03]. Further research has to be done to study the performance of real ad-hoc networks. Besides, the availability of new DSRC (Dedicated Short Range Communication) technologies [ZR03] will impulse even more ad-hoc networking.

#### 3.2.1.3. Security

Security is a critical issue in ad-hoc networking. Given the wireless and dynamic nature of MANETs, their lack of predeployed infrastructure, centralised policy and control, providing this kind of network with a security level such as the one that typical Internet infrastructure-based networks have, is challenging. All the previously enumerated functionalities (that is, routing, IP address autoconfiguration and Internet connectivity) share this severe security concern. There are quite a lot of ad-hoc security related papers, some of them analysing the threats, such as [ZH99] and [SA99], and others proposing solutions to particular problems.

Although there are several security issues in ad-hoc networks that have been addressed, such as stimulating cooperation among nodes, addressing malicious packet dropping [SBR03] and providing a secure and reliable certification authority in ad-hoc networks [HBC01], [CBH03], the issue of secure routing is the one that has received more attention.

Several of the currently proposed ad-hoc routing protocols, such as AODV [PBRD03], DSDV [PB94] and DSR [JMH04], have security vulnerabilities and exposures that allow to perform routing attacks easily. Because of the important differences between infrastructure-based IP networks and ad-hoc networks, developing new security mechanisms is needed.

There exist several types of attacks against existing ad-hoc routing protocols [SDL+02]. Next, we summarise the most relevant ones:

- *Modification attacks.* A malicious node can cause redirection of data traffic or DoS attacks by introducing changes in routing control packets or by forwarding routing messages with falsified values.

- *Impersonation attacks.* A malicious node can spoof the IP address of a legitimate node, and therefore *steal* its identity, and then perform this attack combined with a modification attack. The main problem of these attacks is that it is difficult to trace them back to the malicious node.

- *Fabrication attacks.* A malicious node can create and send false routing messages. This kind of attack can be difficult to detect, since is not easy to verify that a particular routing message is invalid, specially when it is claiming that a neighbour cannot be reached.

Authors of [SDL+02], [SLD+05] provide the following requirements as the ones that a good secure routing algorithm should meet:

1. Route signalling cannot be spoofed.

2. Fabricated routing messages cannot be injected into the network.

3. Routing messages cannot be altered in transit (except according to the normal functionality of the routing protocol).

4. Routing loops cannot be formed through malicious action.

5. Routes cannot be redirected from the shortest path by malicious action.

The research community has addressed the previous security problems in ad-hoc routing protocols, trying to propose mechanisms that meet some, if not all, of the aforementioned requirements. Numerous solutions have been proposed. Next we briefly describe some representative solutions.

Ref. [HPJ05] proposes a secure version of DSR (called ARIADNE), by using predeployed symmetric keys or predeployed asymmetric cryptography for authentication.

SEAD [HJP02] is a secure proactive routing protocol based on DSDV [PB94], which is based on the use of hash chains.

SAODV [ZA02] is a proposal to secure AODV [PBRD03]. Two mechanisms are used to secure AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the mutable information in the messages (that is, the hop count). For the non-mutable information, authentication is performed in an end-to-end manner. However, the same kind of technique cannot be applied to the mutable information, allowing a intermediate malicious node to spoof the identity of a legitimate node and illegally modify the hop count on route request messages. So, hash chains are used to protect mutable information.

In SRP [PH02] a Security Association (SA) is assumed between any source and destination in order to set-up a multi-hop route. This protocol is vulnerable to attacks such as fabrication of route error messages.

An interesting approach is ARAN [SDL+02], [SLD+05]. This proposal uses public-key cryptography mechanisms to defeat all the previously enumerated attacks. However, it has the drawback of requiring certificates issued by a third party. This requirement may affect the deployment of the solution, specially if vehicular environments are considered.

In brief, we can conclude that any mechanism aimed at working in an ad-hoc scenario should consider security issues, although many MANET protocols are missing these security considerations today.

#### 3.2.1.4. IP address autoconfiguration

In order to enable MANETs to support IP services, every node of a MANET should be configured at least with an IP address. However, there is no standard mechanism to provide MANET nodes with IP configuration information, thus requiring nodes to be configured *a priori* and avoiding ad-hoc networks to be spontaneously created.

Existing IP configuration protocols [TN98] for traditional infrastructure-based networks assume the existence of a single multicast-capable link for signalling. Such a link does not

exist in multi-hop infrastructureless networks, making necessary to design new mechanisms that enable the autoconfiguration of IP addresses in a MANET [SKP+06], [RRGS05].

In order to address the IPv6 autoconfiguration issue in MANETs, a new Working Group, called AUTOCONF, was created within the IETF. This group has identified two main possible scenarios [RSCS06] of MANET where IP address autoconfiguration is required:

- *Stand-alone* ad-hoc network: an ad-hoc network not connected to any external network, such as conference networks, battlefield networks, surveillance networks, etc. Most likely neither pre-established or reliable address, nor prefix allocation agency will be present in the network. In this scenario, IPv6 addresses are not required to be global.

- *Hybrid* ad-hoc network (at the edge of an infrastructure network): a stand-alone network connected to the Internet. Nodes of hybrid networks should be provided with global IPv6 addresses, so they are able to communicate with any other node of the Internet. This usually requires discovering the global IPv6 prefix available in the MANET and configuring a unique address from this prefix [BC06].

Although the AUTOCONF WG is still working on the definition of a protocol, there are already many partial solutions proposed. A survey of the most relevant ones can be found in [BC05].

#### 3.2.1.5. Internet Gateway discovery

In order to provide connectivity to a hybrid MANET [RRGS05], in addition to global IP addressing, a special kind of node is needed in the ad-hoc network. An Internet Gateway (IGW) is a node that has connectivity to both an infrastructure access network and the ad-hoc network, and that provides connectivity to the nodes attached to the latter. An IGW can be mobile or fixed and it is of key importance in order to provide connectivity to the nodes that are on the MANET side. Due to the characteristics of MANETs, it is also desirable to deploy multiple IGWs (for example, to mitigate problems related to congestion).

Nowadays, a common proposal to support Internet connectivity in vehicles that only have ad-hoc connectivity consists in deploying IGWs on the roadside, so passing vehicles can make use of them to access the Internet. One of the challenges posed by this architecture is how to efficiently discover available Internet Gateways [BWSF03], since one of the key components affecting overall performance is the algorithm used to discover and select Internet Gateways [RGS04].

Deploying a network infrastructure consisting on several roadside IGWs and relying on the multi-hop forwarding within spontaneously created vehicular ad-hoc networks is not sufficient. There could exist “holes” in the connectivity, that would prevent vehicles from communicating (not only among themselves but also to the Internet). Furthermore, roadside IGWs may not belong all of them to the same provider, and therefore it may not be possible for a vehicle to maintain the same IPv6 address when switching from one IGW to another. Although there are solutions that mitigate the effect of this intermittent connectivity, such as the one described in [OK04] for a non-ad-hoc network (based on application gateways and proxies), the possibility of switching to a different available network interface (e.g., a

cellular one, such as GPRS or UMTS) while keeping transparent on-going sessions (that is, true mobility support) should be enabled.

The ad-hoc centric approach has several drawbacks. For example, there are some security concerns not yet solved and it does not provide global mobility management support. Therefore, this kind of approach is not valid to fulfil all the requirements of the vehicular scenario.

### 3.2.2. Host centric approach

A different approach to support vehicular communications consists in considering each car as a single host and using Mobile IP techniques to support mobility. We call this approach *host centric*.

This approach is based on just taking advantage from existing wireless and mobility related protocols, by making the necessary changes in order to improve their performance in a vehicular scenario. As a simple example, we can mention approaches based on 2.5/3G radio networks [AVN00].

Another example is the architecture defined in the Drive-thru project [OK04]. It is based on providing some useful Internet services in environments with intermittent connectivity. This intermittent connectivity is obtained by cars by attaching to roadside deployed WLAN Access Points.

There are several scenarios in which it is useful to combine ad-hoc and Mobile IP mechanisms to support vehicles roaming between ad-hoc and infrastructure networks. This requires to enable *global mobility* across different types of access networks (ad-hoc and infrastructure) to transparently preserve the vehicular connectivity. Most of the proposals of global mobility management for ad-hoc networks are based on adapting Mobile IP mechanisms to be used with particular ad-hoc routing protocols.

One of the most well-known approaches is MIPMANET [JAL+00], that basically proposes a solution based on Mobile IPv4 and AODV. In order to combine the reactive nature of AODV and the proactive nature of Mobile IPv4, Foreign Agents (FAs) periodically advertise themselves in the ad-hoc network. Foreign Agents are used as Internet Gateways to access to the Internet, in order to keep track of in which ad-hoc network a node is located and to direct packets to the border of that ad-hoc network. AODV is used to deliver packets between the FA and the mobile node. A layered approach with tunnelling is used for the outward data flow to separate the Mobile IPv4 functionality from the ad-hoc routing protocol. A similar mechanism is proposed in MEWLANA [EP02], but suited for the Destination-Sequenced Distance Vector (DSDV) routing protocol [PB94]. In [RK03], techniques such as limiting the flooding of Foreign Agent advertisements to an n-hop neighbourhood – by using a lifetime (TTL) field in the advertisement messages –, eavesdropping and caching agent advertisements are combined to improve the performance. Similarly, a mechanism integrating Mobile IPv4 and OLSR is proposed in [BMA+04].

Regarding IPv6 support, [PMW+02] describes how to provide ad-hoc networks with Internet connectivity supporting Mobile IPv6. Mobile IPv6 uses Neighbour Discovery as part of its movement detection mechanism with the acquisition of a globally routable address. This movement detection mechanism is modified in ad-hoc networks, where the Internet

Gateway plays the role of the local router and the Router Advertisements are replaced by the Gateway advertisements. The IPv6 address configured from the MANET routing prefix contained in the Gateway advertisements is used as the MN's Care-of Address. This way of performing the movement detection algorithm has the drawback that is more time-consuming than movement detection between points of attachment to the fixed Internet, since Gateway advertisements are not broadcast so frequently as Router Advertisements (to avoid wasting radio resources). Other proposed mechanisms for IPv6 global mobility support in ad-hoc networks are [HSFN04] – which adopts a hierarchical architecture (based on HMIPv6) to enable ad-hoc nodes to be registered to more than one AR/IGW at the same time (reducing handover delay and signalling) – and [HLWC05] – that proposes a protocol that automatically organises the ad-hoc network into a tree architecture in order to facilitate addressing and routing within the MANET.

There are also some solutions proposed that specifically address the car-to-car scenario. An example is [BW05], which is similar to MIPMANET [JAL+00], in the sense that it re-uses the concept of MIPv4 Foreign Agent (FA) – collocated in the IGW – to manage the global mobility of ad-hoc nodes. IPv4 communication is still used between the HA and the FA (using IPv6-in-IPv4 tunnelling), since the solution assumes IPv4-based Internet (authors also propose the use of a proxy-based communication architecture to support IPv6 enabled vehicles to communicate to IPv4 CNs in the Internet). As in [RK03], FAs actively announce their service, but limited to local areas, to avoid flooding the complete vehicular network.

The host centric approach has one main drawback, namely it does not take into account that in a vehicle there will be likely more than one device that could benefit from having Internet connectivity. Host-centric approaches require every device to manage its own connectivity and mobility (although they are moving together) and hence prevent nodes without mobility support from being deployed in cars.

### 3.2.3. NEMO centric approach

Since the vehicular scenario involves a group of devices that move together, both the car-to-Internet and car-to-car cases may be addressed by assuming that there is a Mobile Router deployed in each vehicle, managing the mobility of the group of devices within the moving vehicle (we call this approach *NEMO centric*). However, it is worth mentioning that after studying the related literature, we have found very few proposals considering network mobility approaches for vehicular scenarios, since most of the mechanisms just consider cars as single nodes.

The car-to-Internet particular scenario fits quite well into the general Network Mobility paradigm. Therefore, the applicability of a generic Network Mobility framework to the car-to-Internet scenario solution should be analysed. NEMO Route Optimisation solutions may be applied to improve the performance. Actually, this is a very good example of scenario where a Route Optimisation solution for NEMO is needed.

The car-to-car scenario may also be addressed by using a generic NEMO approach. However, this kind of solution does not perform well in a car-to-car communication, even when a generic Route Optimisation for NEMO solution is used. This is so because:

- The Home Networks of two cars that are communicating may not be the same or may

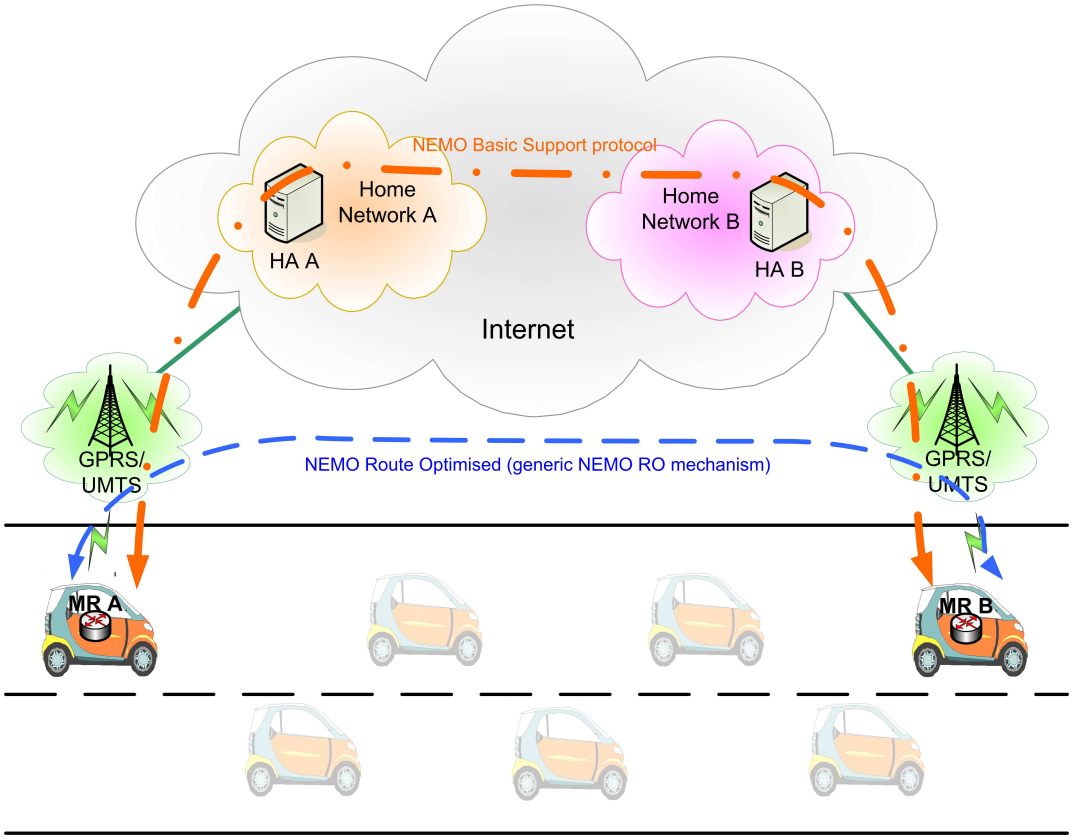


Figure 3.3: Operation of a generic Network Mobility solution in the car-to-car communication scenario.

be located far each other. This makes even more necessary the deployment of a Route Optimisation solution, in order to avoid the increased delay experienced due to use of the NEMO Basic Support protocol.

- Cars will likely obtain Internet global connectivity from a 2.5/3G cellular network. This kind of network usually presents high delays and provides low bandwidths [VBM+05], [VBS+06]. This has a strong impact on car-to-car communications when using a generic NEMO solution. An example of car-to-car scenario is shown in Figure 3.3. If the NEMO Basic Support protocol [DWPT05] is used, data traffic flows from one car's Mobile Router (MR A) to its Home Network (Home Network A), where packets are forwarded by HA A towards the correspondent car's Home Network (Home Network B) and then finally delivered to MR B. This is clearly a suboptimal route. If a general Route Optimisation solution is used in this scenario, data packets no longer traverse the Home Networks of involved NEMOs, but they still need to go to the infrastructure to be routed from one car to the other. This may still involve a high delay (GPRS networks have about 500 ms of one-trip delays [VBM+05], [VBS+06] while UMTS have about 150 ms [MdlOS+06], [OMV+06]) and a poor bandwidth. Therefore a different Route Optimisation approach should be explored.

Although automobiles can communicate with other vehicles through the infrastructure – by using the NEMO Basic Support protocol –, a conclusion from the previous discussion is that classical NEMO Route Optimisation schemes do not perform well in car-to-car scenarios. There is however an opportunity for optimisation that current research efforts within the field of inter-vehicular communication (IVC) systems are looking at. This optimisation is based on the use of vehicular ad-hoc networks (VANETs) to exploit connectivity between neighbouring cars and set-up a multi-hop network to support car-to-car services. How to apply this approach to a NEMO-based vehicular communications solution is one of the goals of this PhD thesis. We explore how to design a network mobility-based mechanism to optimise car-to-car communications, by taking advantage from the fact of MRs setting-up ad-hoc networks to directly communicate (bypassing the routing infrastructure).

According to our knowledge, there is only one proposal combining the NEMO and ad-hoc approaches [WOKN05], [WMK+05], [WMK+04], [OWUM04]. The solution (defined in [WOKN05], [WMK+05], [WMK+04]) basically considers MANETs that move together (for example, within a car) and integrates MANET and NEMO, by collocating the Internet Gateway and Mobile Router functionalities into the so-called *Mobile Gateway* (MG). The NEMO Basic Support protocol [DWPT05] is responsible for providing global Internet connectivity to the moving MANET (therefore, there is no need in the nodes belonging to the moving MANET to support Mobile IPv6), whereas a second MANET routing protocol is run also among Mobile Gateways, creating an overlay MANET for inter mobile network connectivity. This scheme enables direct communication between nodes of moving MANETs that belong to the same overlay MANET (*direct route*), whereas the NEMO Basic Support protocol is used otherwise (*nemo route*). Besides, the mechanism also supports a MG to borrow adjacent MG's Internet connectivity (*detour route*). It is proposed to use a proactive ad-hoc routing protocol for the overlay MANET, in particular OLSR is considered in [OWUM04].

The previously described solution is a first approach to optimally combine NEMO and ad-hoc to support vehicular communications. The authors have left as a future work the security analysis, therefore in their proposed architecture, as an example, nothing prevents malicious nodes from stealing traffic or making a Return-to-Home Flooding [NAA+05] attack. This lack of security is a critical issue, specially in car-to-car environments.

Designing a mechanism based on a Network Mobility solution combined with ad-hoc support in a *secure* way to optimally enable vehicular communications is one of the key objectives of this PhD thesis.