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 poder 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 escenarios) 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.

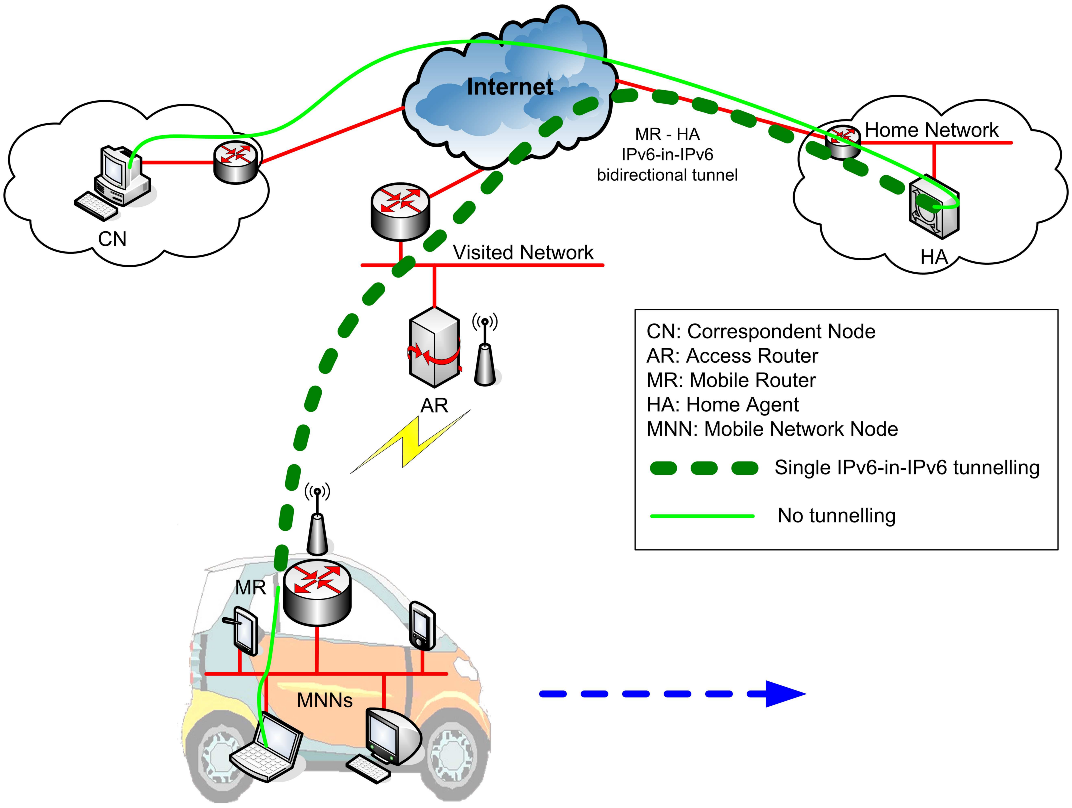


Figure 2.1: NEMO Basic Support protocol operation overview.

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.

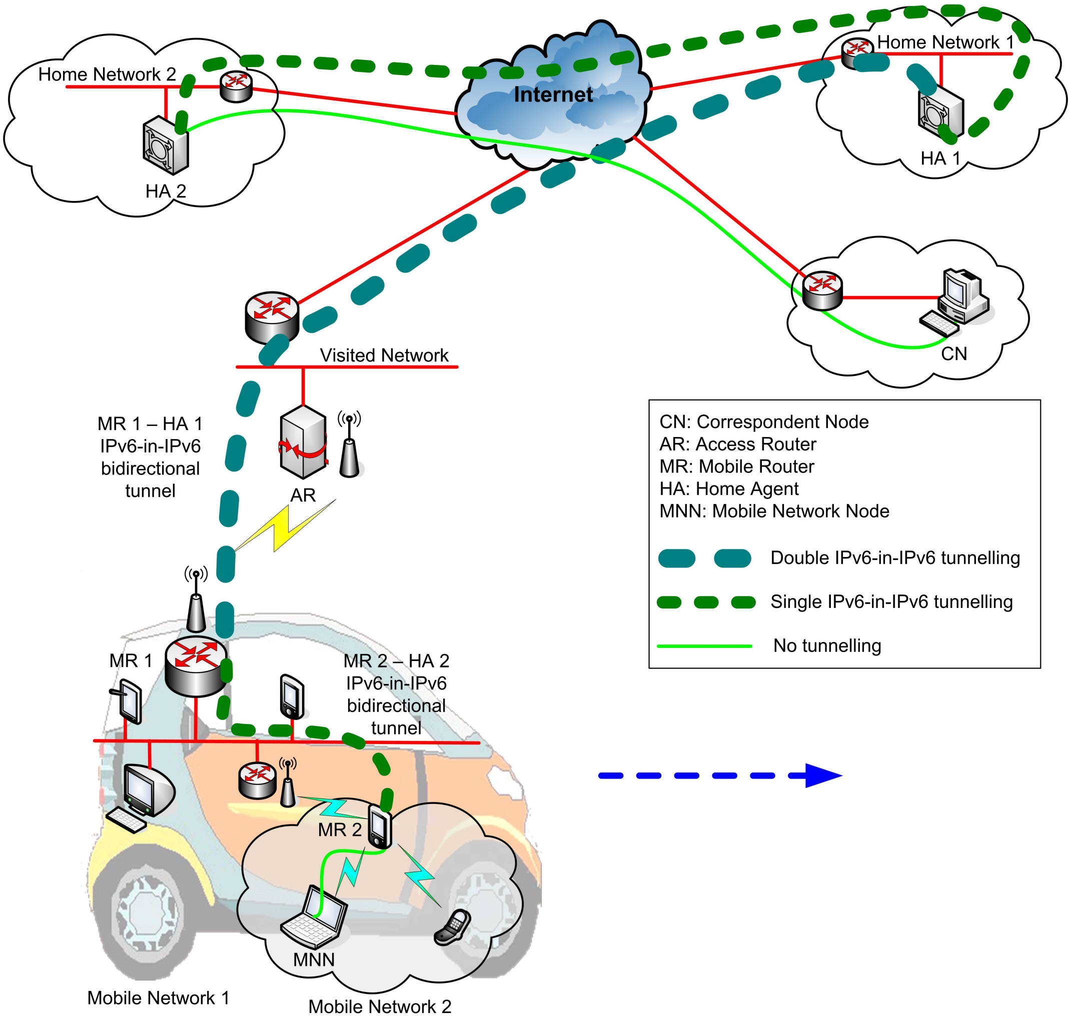


Figure 2.2: Nested mobile network. Operation of the NEMO Basic Support protocol (multi-angular routing).

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

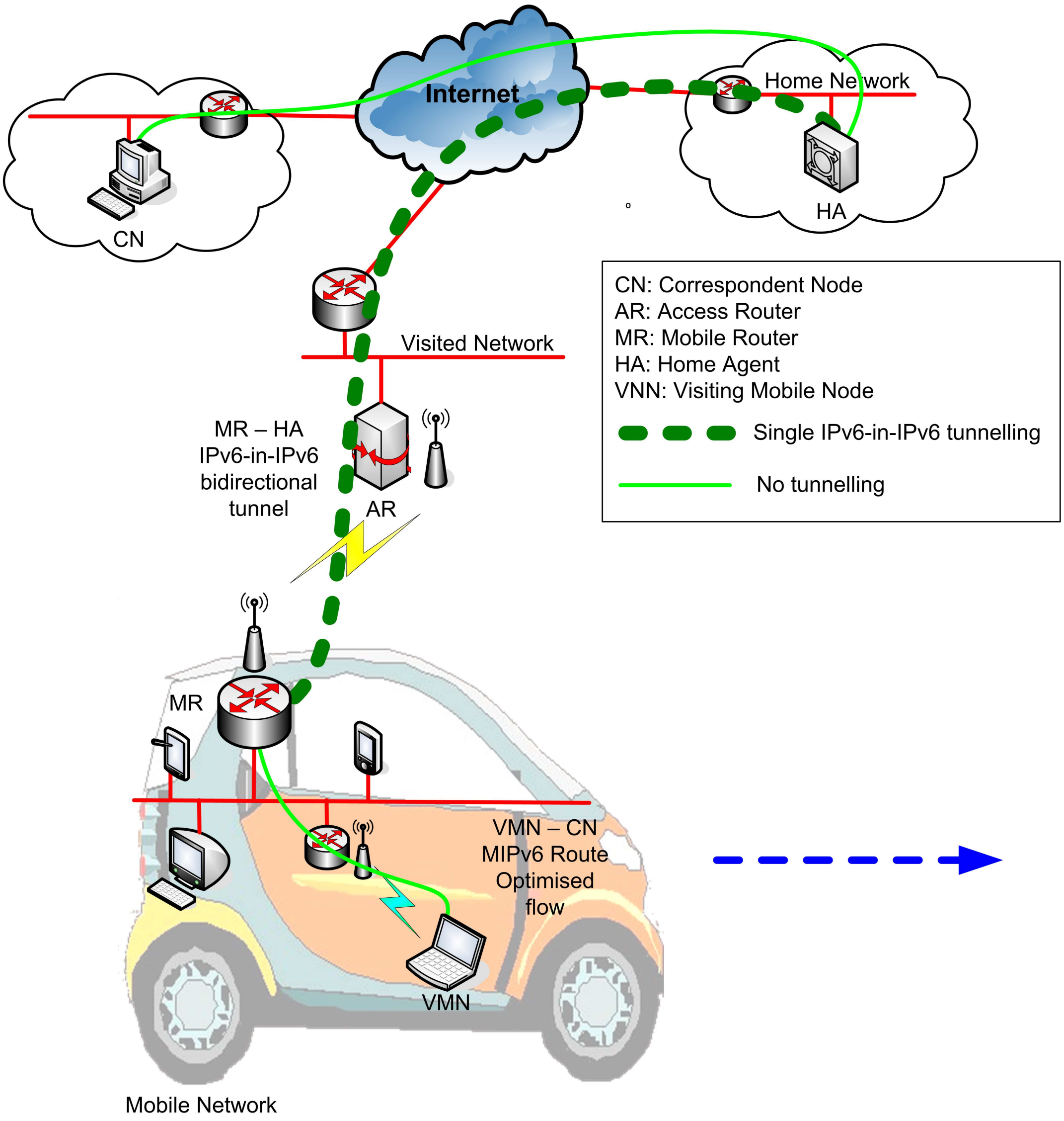


Figure 2.3: Mobile IPv6 enabled host (performing Mobile IPv6 Route Optimisation with a Correspondent Node) inside a mobile network.

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].

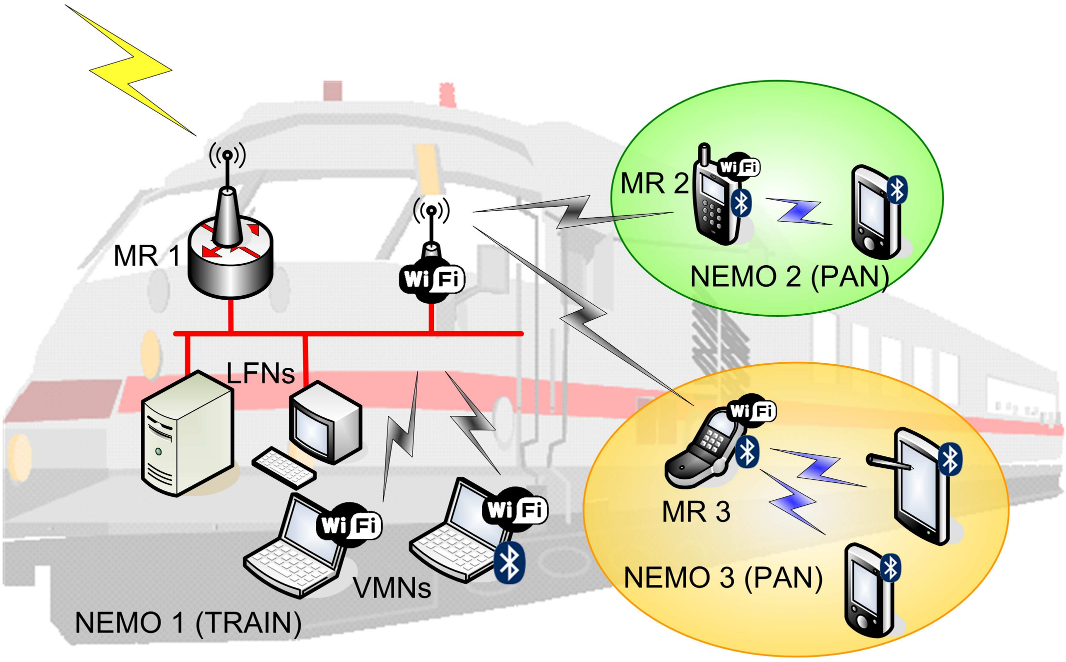


Figure 2.4: Example of intra-nested NEMO scenario: train.

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 encaminamiento 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.

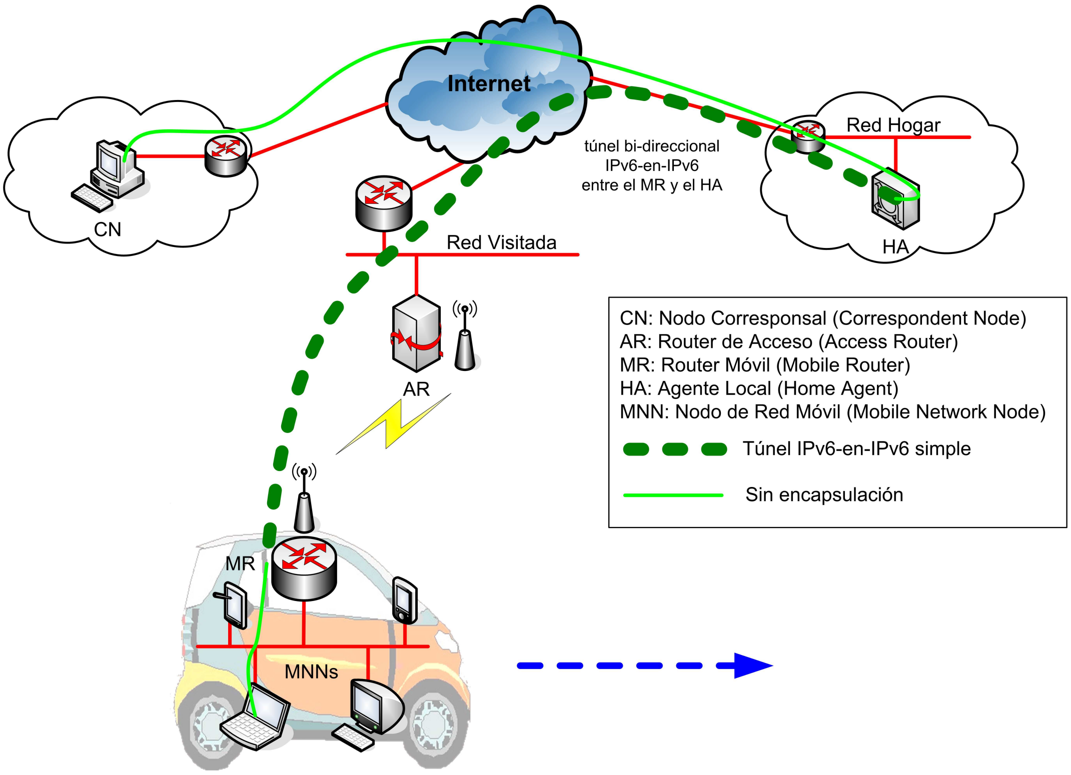

Internet
CN
túnel bi-direccional
IPv6-en-IPv6
entre el MR y el HA
Red Hogar
HA
Red Visitada
AR
MR
MNNs
CN: Nodo Corresponsal (Correspondent Node)
AR: Router de Acceso (Access Router)
MR: Router Móvil (Mobile Router)
HA: Agente Local (Home Agent)
MNN: Nodo de Red Móvil (Mobile Network Node)
Túnel IPv6-en-IPv6 simple
Sin encapsulación

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.

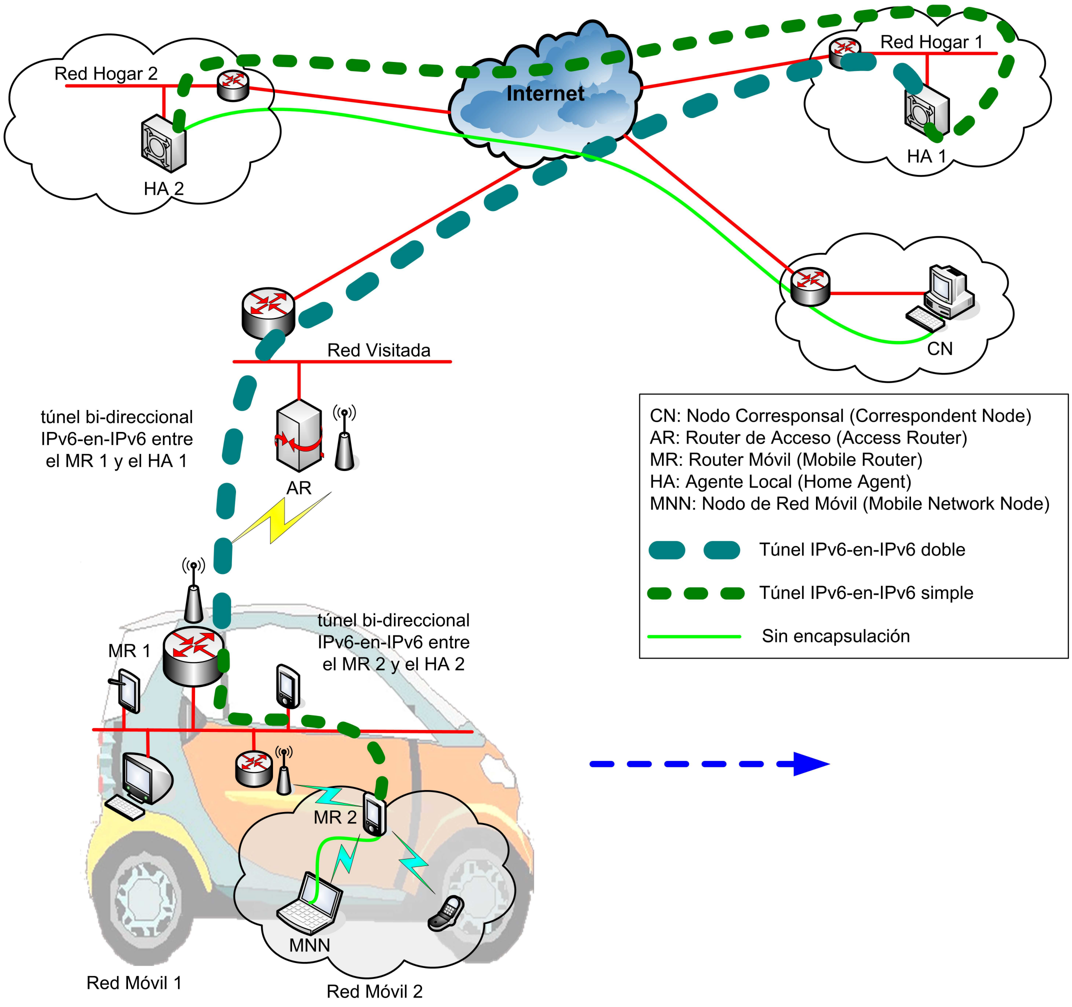

Red Hogar 2
HA 2
Internet
Red Hogar 1
HA 1
CN
Red Visitada
AR
túnel bi-direccional IPv6-en-IPv6 entre el MR 1 y el HA 1
túnel bi-direccional IPv6-en-IPv6 entre el MR 2 y el HA 2
MR 1
MR 2
MNN
Red Móvil 1
Red Móvil 2
CN: Nodo Corresponsal (Correspondent Node)
AR: Router de Acceso (Access Router)
MR: Router Móvil (Mobile Router)
HA: Agente Local (Home Agent)
MNN: Nodo de Red Móvil (Mobile Network Node)
Túnel IPv6-en-IPv6 doble
Túnel IPv6-en-IPv6 simple
Sin encapsulación

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.

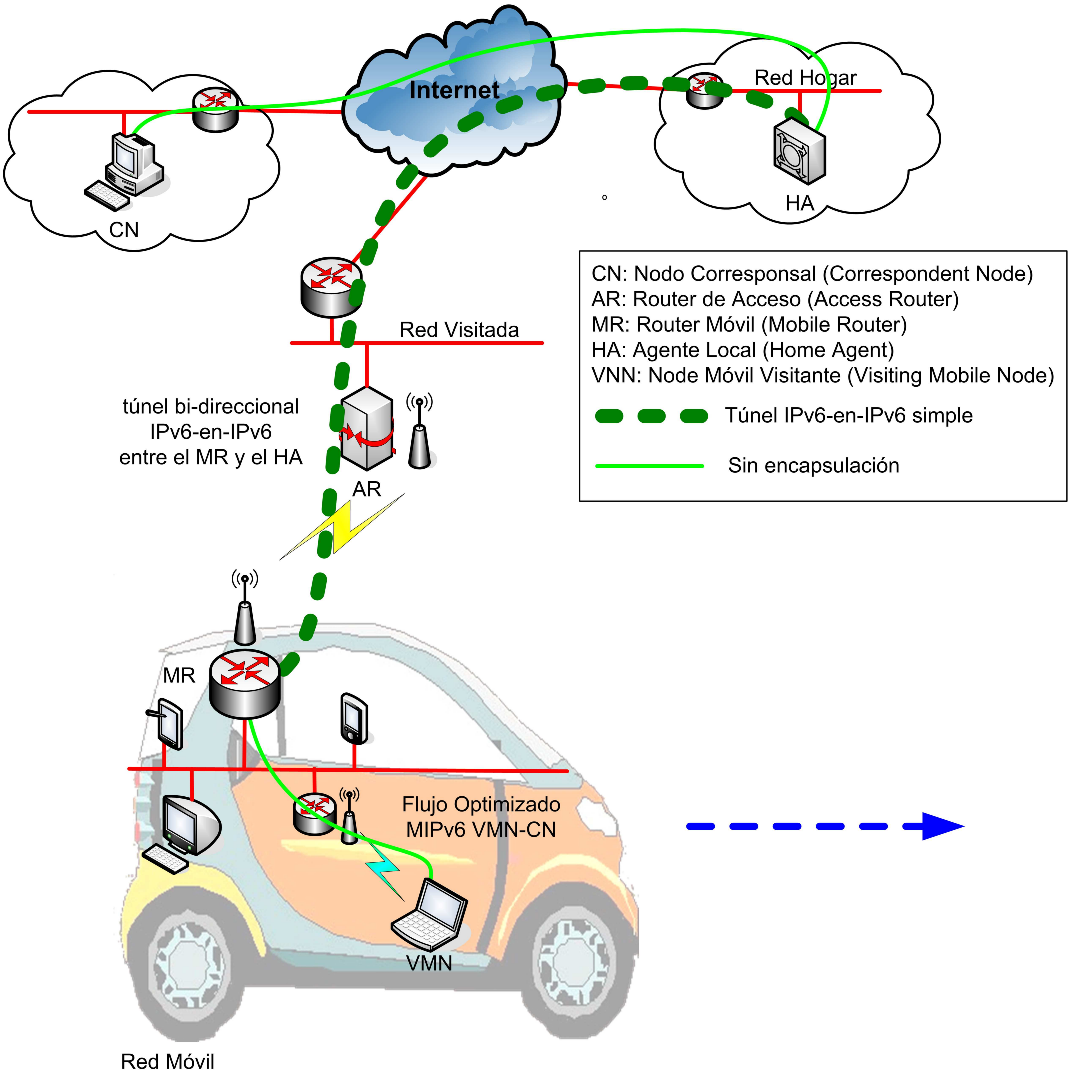

Internet
Red Hogar
CN
HA
Red Visitada
túnel bi-direccional
IPv6-en-IPv6
entre el MR y el HA
AR
MR
Flujo Optimizado
MIPv6 VMN-CN
VMN
Red Móvil
CN: Nodo Corresponsal (Correspondent Node)
AR: Router de Acceso (Access Router)
MR: Router Móvil (Mobile Router)
HA: Agente Local (Home Agent)
VNN: Node Móvil Visitante (Visiting Mobile Node)
Túnel IPv6-en-IPv6 simple
Sin encapsulación

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-

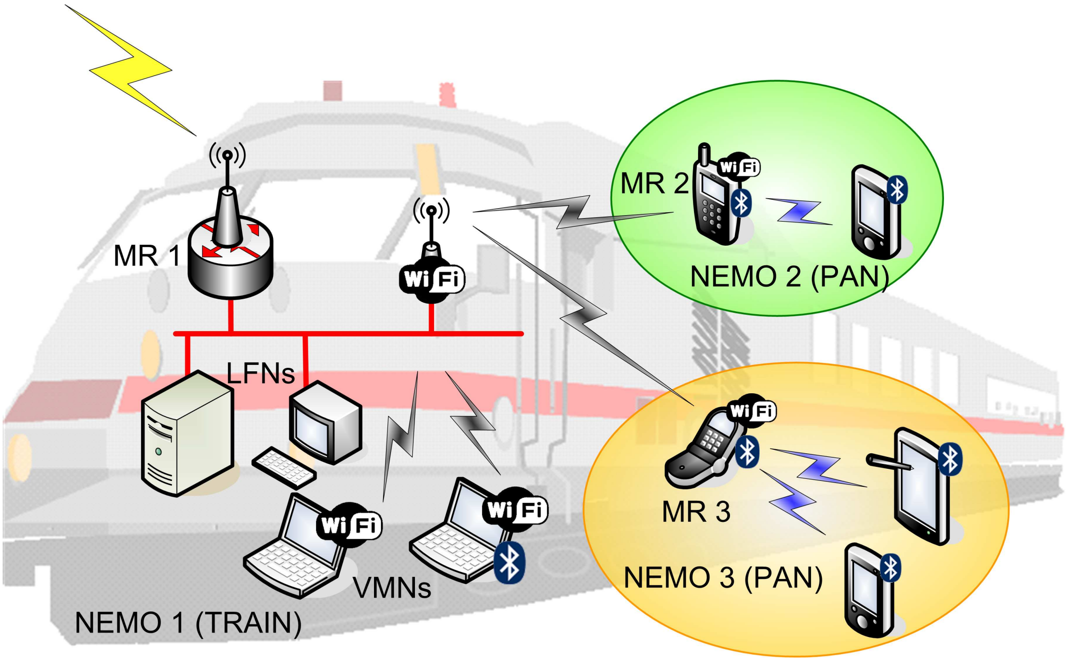


Figura 2.4: Ejemplo de escenario de comunicaciones intra-NEMO: un tren.

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

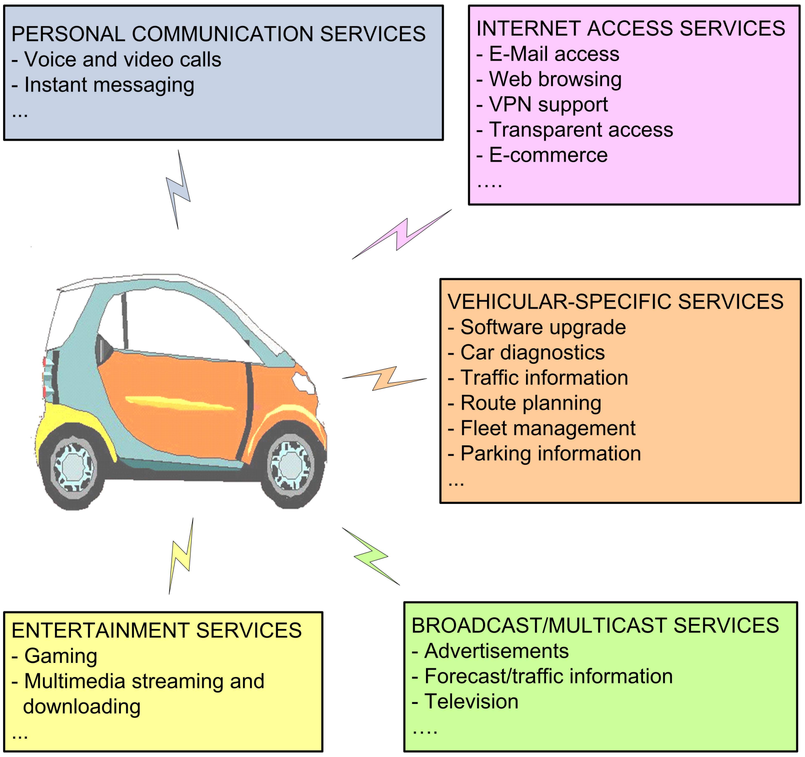


Figure 3.1: Some examples of applications and services in a vehicular scenario.

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/

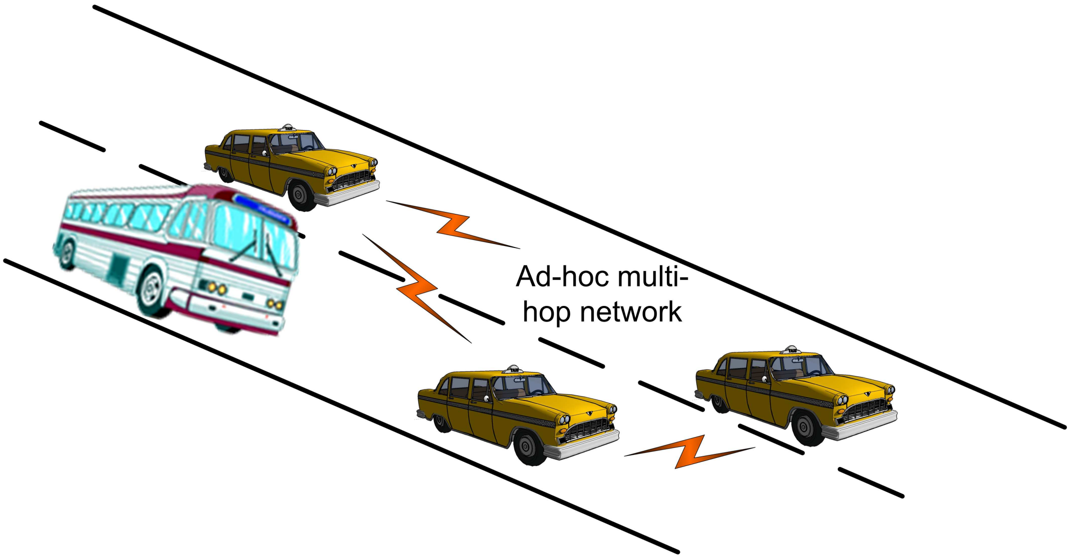


Figure 3.2: Vehicular Ad-hoc Network.

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

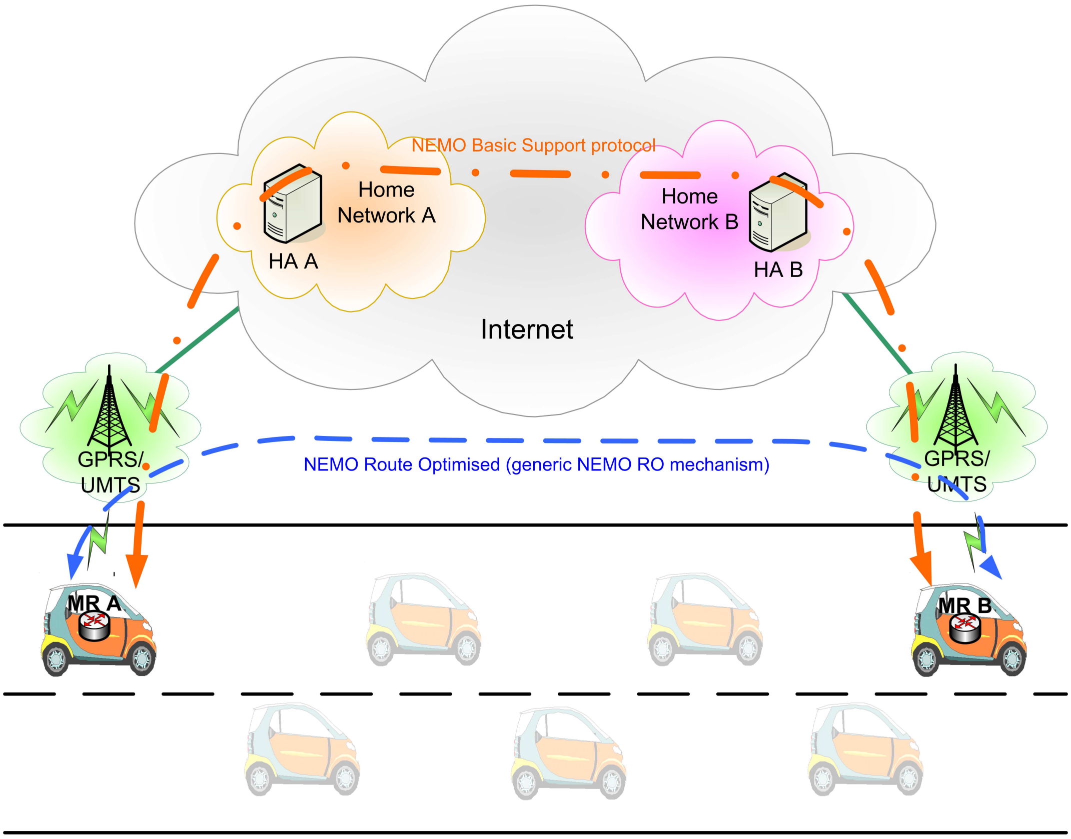

NEMO Basic Support protocol
Home Network A
HA A
Home Network B
HA B
Internet
GPRS/ UMTS
NEMO Route Optimised (generic NEMO RO mechanism)
GPRS/ UMTS
MR A
MR B

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.

Capítulo 3

Optimización de las comunicaciones entre redes móviles vehiculares

En el capítulo anterior se han presentando algunos escenarios que podrían beneficiarse de utilizar un enfoque basado en una solución de movilidad de redes. Claramente, parece que la provisión de acceso a Internet desde plataformas móviles (como trenes, aviones o autobuses) parece el escenario más relevante. Además, el escenario de comunicaciones vehiculares está recibiendo gran cantidad de atención por parte de la investigación académica e industrial.

El escenario particular de las comunicaciones vehiculares es cada vez más popular debido a que existe un gran número de aplicaciones potenciales que podrían beneficiarse de disponer de la capacidad de comunicarse a través de Internet. Principalmente, existen 2 problemas a tratar: el acceso a Internet desde coches (el denominado *car-to-Internet scenario*) y las comunicaciones entre vehículos (*car-to-car scenario*). Dada la naturaleza de las comunicaciones vehiculares y su relevancia, resulta necesario estudiar la aplicabilidad de una aproximación basada en movilidad de redes.

Este capítulo introduce primero el escenario vehicular, presentando los retos particulares derivados del mismo y analizando los diferentes enfoques que están siendo propuestos para soportar dicho escenario.

3.1. Introducción

En la sociedad moderna actual, mucha gente pasa una gran cantidad de tiempo en sus coches. En el pasado, las posibilidades de comunicación pasaban mayoritariamente por las redes celulares. Posibilitar las comunicaciones de banda ancha en coches [KBS$^+$01] es una contribución muy importante en la tendencia global hacia las comunicaciones ubicuas. Los coches deben proporcionar acceso a Internet y deben ser capaces de establecer comunicaciones entre ellos, soportando nuevos servicios y aplicaciones.

Hay una gran cantidad de aplicaciones y servicios potenciales que son de gran interés para los usuarios de automóviles. En la Figura 3.1, se muestran algunos ejemplos representativos, clasificados en cinco categorías diferentes, pero con cierto solapamiento entre ellas:

- **Servicios de comunicaciones personales.** Las aplicaciones clásicas de telecomuni-

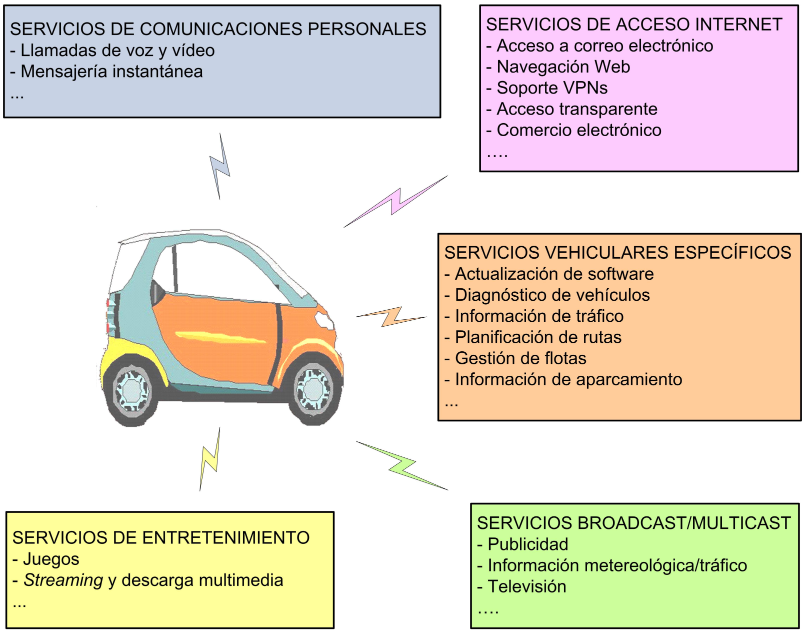

SERVICIOS DE COMUNICACIONES PERSONALES
- Llamadas de voz y vídeo
- Mensajería instantánea
...
SERVICIOS DE ACCESO INTERNET
- Acceso a correo electrónico
- Navegación Web
- Soporte VPNs
- Acceso transparente
- Comercio electrónico
....
SERVICIOS VEHICULARES ESPECÍFICOS
- Actualización de software
- Diagnóstico de vehículos
- Información de tráfico
- Planificación de rutas
- Gestión de flotas
- Información de aparcamiento
...
SERVICIOS DE ENTRETENIMIENTO
- Juegos
- *Streaming* y descarga multimedia
...
SERVICIOS BROADCAST/MULTICAST
- Publicidad
- Información metereológica/tráfico
- Televisión
....

Figura 3.1: Algunos ejemplos de aplicaciones y servicios en un escenario vehicular.

caciones, tales como las comunicaciones de voz, tienen que ser integradas para su uso en los coches. De hecho, algunas de ellas están disponibles en los coches actuales (p.e., comunicaciones manos-libres utilizando un sistema celular integrado). Sin embargo, se espera que en el futuro aplicaciones más complejas estén disponibles en los coches, aprovechando las mayores capacidades que se espera que tengan los vehículos – comparada con las de los terminales de comunicaciones portátiles actuales.

- **Servicios de acceso a Internet.** Los vehículos, especialmente los servicios de transporte público, como trenes y autobuses, deben facilitar el uso a bordo de las aplicaciones típicas de trabajo (p.e., correo electrónico, software de VPN, etc.), mediante la provisión de acceso transparente a Internet, ya sea usando dispositivos embebidos en el vehículo o los terminales de los propios pasajeros.

- **Servicios vehiculares específicos.** Existen algunas aplicaciones que son específicas del escenario vehicular, como por ejemplo la descarga de información relativa al tráfico, la monitorización y diagnóstico de vehículos, y el control y la actualización del software instalado en los vehículos. En general, la seguridad es un aspecto crítico en este tipo de aplicaciones (p.e., en la diagnosis o la actualización de software).

- **Servicios de entretenimiento.** Los juegos multi-jugador y el *streaming* multimedia son aplicaciones ampliamente extendidas hoy en día, que muy probablemente serán de gran importancia en escenarios vehiculares (p.e., niños en los asientos traseros del coche, o personas yendo a su lugar de trabajo, jugando mientras que se desplazan). Además, estos servicios pueden beneficiarse de información de localización.

- **Servicios broadcast/multicast.** El envío de contenidos a grupos de receptores es un servicio de interés en el entorno vehicular. Esta clase de servicio será probablemente proporcionado empleando tecnologías de acceso específicas, como DVB, por lo que tendrán que tenerse en cuanta además consideraciones adicionales.

Por todo lo anterior, parece que los coches dejarán de ser sistemas aislados dentro de poco [KBS$^+$01], surgirán nuevos servicios y aplicaciones cuando los coches tengan la capacidad de conectarse a Internet y de comunicarse entre ellos [Ern06]. Estos nuevos escenarios supondrán nuevos retos que tendrán que ser resueltos, principalmente relacionados con la gestión de la movilidad, pero también con la provisión de calidad de servicio y la seguridad. Algunos de estos problemas están siendo estudiados por proyectos e iniciativas de investigación conjuntos, como los siguientes:

- El proyecto europeo DRiVE[1] (1999) y su continuación OverDriVE[2] (2001), que se centraron en facilitar la entrega de servicios multimedia a vehículos y el desarrollo de un router vehicular que proporcionara acceso, mediante múltiples tecnologías de radio, a una red intra-vehicular (intra-vehicular network, IVAN) móvil [LJP03], [LN03], [WS03].

- El proyecto InternetCAR[3] (1996), investigó cómo podría facilitarse la conexión transparente de vehículos a Internet. En algunas fases del proyecto se llevaron a cabo experimentos reales (con un número de vehículos que alcanzaba hasta 1640). Algunos resultados de estos experimentos pueden encontrarse en [EMU03], [EU02], [USM03], [WYT$^+$05] y [KLE05].

- El proyecto *Red sobre Ruedas*, “Network On Wheels” (NOW[4]) (2004) se centra en IPv6 y la tecnología IEEE 802.11 para desarrollar comunicaciones entre vehículos basadas en conceptos de redes ad-hoc. Esencialmente, este proyecto está explorando maneras de que vehículos en movimiento puedan establecer dinámicamente enlaces con otros coches, motos y camiones en la vecindad, para compartir información de tráfico.

- El proyecto FleetNet (”Internet en la carretera[5]”) (2000) fue formado por un consorcio de seis compañías y tres universidades con objeto de promover el desarrollo de sistemas de comunicaciones entre vehículos.

- El proyecto Daidalos[6] (2002) es un Proyecto Integrado del Sexto Programa Marco de la Unión Europea, actualmente en su segunda fase. Uno de sus objetivos es la integración óptima de tecnologías de acceso heterogéneas para permitir a los operadores de red y proveedores de servicio ofrecer nuevos y más rentables servicios. Las redes móviles son una de las tecnologías de acceso consideradas por el proyecto. Hasta el momento, Daidalos ha trabajado en tres aspectos dentro de la movilidad de redes [BSC$^+$05b], [BSC$^+$05a]: el desarrollo de una implementación del protocolo de

[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/`

Soporte Básico de Movilidad de Redes [dlOBC05], la extensión del protocolo básico para soportar tráfico multicast [vHKBC06] y el diseño de una solución de optimización de rutas para redes móviles [BBC04].

Los proyectos anteriormente descritos son solamente algunos de los más relevantes. Existen muchos otros esfuerzos de investigación en esta línea, como el proyecto InternetITS[7] [MUM03], el consorcio Car2Car Communication[8] o el proyecto CarTALK 2000[9]. Dada la gran cantidad de esfuerzos de investigación relacionados con las comunicaciones vehiculares, queda patente que el escenario vehicular es un tema de investigación de actualidad. La mayoría de estos esfuerzos están dirigidos a proporcionar soluciones para los dos escenarios principales considerados en las comunicaciones vehiculares:

- **Comunicaciones *Car-to-Internet*.** Este es un escenario muy común ya que muchas de las aplicaciones que se espera se necesiten en un vehículo, implican comunicaciones entre un nodo dentro de un coche y otro extremo en Internet (p.e., navegación web, correo electrónico, etc.). Inicialmente sólo se empleaban las comunicaciones celulares en este tipo de escenarios [AVN00]. Recientemente, con el éxito de la tecnología inalámbrica IEEE 802.11, otras tecnologías están siendo consideradas. Se está investigando como solventar las limitaciones (p.e., costes, bajos anchos de banda, altos retardos, etc.) de las tecnologías celulares existentes hoy en día, mediante el uso de WLAN 802.11 ([LG04] presenta un estudio sobre la posibilidad o no de utilizar WLAN 802.11 para conectar trenes a Internet) y WiMAX.

- **Comunicaciones *car-to-car*.** Existen diversas aplicaciones vehiculares, como los juegos en red, la mensajería instantánea, la información de tráfico o los servicios de emergencia, que pueden implicar comunicaciones entre vehículos que se encuentran relativamente cercanos entre sí, y que incluso pueden moverse juntos (p.e., convoys militares). Además, hay algunas aplicaciones emergentes que son exclusivas del entorno vehicular. Por ejemplo, los servicios de información al conductor podrían informar de forma inteligente acerca de atascos, negocios y servicios que se encuentren en las cercanías del vehículo, u otro tipo de noticias. Estos servicios emergentes no están bien soportados en la actualidad. Numerosos retos tecnológicos han de ser solventados antes de que las comunicaciones inter-vehiculares puedan llegar a ser ampliamente desplegadas. Estos escenarios están siendo investigados mayoritariamente por la comunidad ad-hoc, debido a que los protocolos de encaminamiento ad-hoc resultan muy apropiados para este tipo de problema (es decir, topologías que cambian rápidamente a medida que los coches se desplazan, carencia de infraestructura previa, etc.).

La conectividad puede proporcionarse en ambos escenarios empleando una solución genérica de movilidad de redes (p.e., el protocolo de Soporte Básico de Movilidad de Redes [DWPT05]). Sin embargo, tal y como se describirá más tarde, el caso vehicular presenta

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

algunas particularidades que hacen que el rendimiento cuando se emplean soluciones genéricas de movilidad de redes y de optimización de rutas sea muy bajo, requiriendo por lo tanto el estudio de nuevos tipos de soluciones.

3.2. Haciendo posibles las comunicaciones vehiculares

En esta sección se presenta una visión panorámica del estado del arte en comunicaciones vehiculares, clasificando las propuestas existentes en tres categorías diferentes.

3.2.1. Soluciones basadas principalmente en ad-hoc

Hay una gran cantidad de trabajo de investigación en el campo de las redes ad-hoc. Algunos de los mecanismos desarrollados por la comunidad ad-hoc parecen ser apropiados para el escenario vehicular, al menos como punto de partida. Por lo tanto, en los últimos años se han propuesto muchas soluciones para permitir las comunicaciones vehiculares basadas en el concepto de redes ad-hoc vehiculares (Vehicular Ad-hoc Networks, VANETs). Dentro de esta categoría, a la que llamamos *soluciones basadas principalmente en ad-hoc,* incluimos a todos aquellos mecanismos que afrontan el problema de las comunicaciones vehiculares utilizando soluciones ad-hoc exclusivamente, sin emplear IP móvil.

3.2.1.1. Redes ad-hoc vehiculares

Las redes ad-hoc surgen como alternativa a las redes basadas en infraestructura, debido a las demandas de movilidad y al reto que supone desplegar redes de acceso inalámbricas sin zonas *muertas* (sin cobertura). En particular, una red ad-hoc móvil (Mobile Ad-hoc Network, MANET [CM99]) es un grupo de dispositivos móviles inalámbricos que cooperan para formar una red IP. Esta red no necesita ningún tipo de infraestructura para trabajar, ya que los dispositivos de los usuarios de una red MANET son la propia red, por lo que un nodo no sólo se comunica directamente con los dispositivos que tiene dentro de su radio de alcance, sino también con otros utilizando rutas multi-salto a través de otros nodos de la MANET.

Una red ad-hoc vehicular (Vehicular Ad-hoc Network, VANET) es un tipo particular de red ad-hoc en la que los nodos se encuentran en vehículos [FTMT+05]. Mediante la configuración de una VANET, los vehículos pueden comunicarse localmente sin necesitar ninguna infraestructura (ver Figura 3.2).

El escenario vehicular tiene características que lo diferencian de otros escenarios de comunicaciones en red. Por ejemplo, por un lado tiene similitudes con los escenarios clásicos ad-hoc, debido a que presenta una topología que cambia rápidamente a medida que los coches se mueven. Sin embargo, por otro lado, las limitaciones y optimizaciones son diferentes. Primero, la eficiencia energética no es tan importante en las comunicaciones intervehiculares como lo es en las redes ad-hoc tradicionales, debido a que los vehículos disponen de una potente fuente de energía recargable. Segundo, los vehículos en general se mueven en carreteras (y dentro de un mismo carril la mayoría del tiempo).

De cara a hacer que el escenario de la Figura 3.2 funcione correctamente, hay algunos aspectos que deben resolverse:

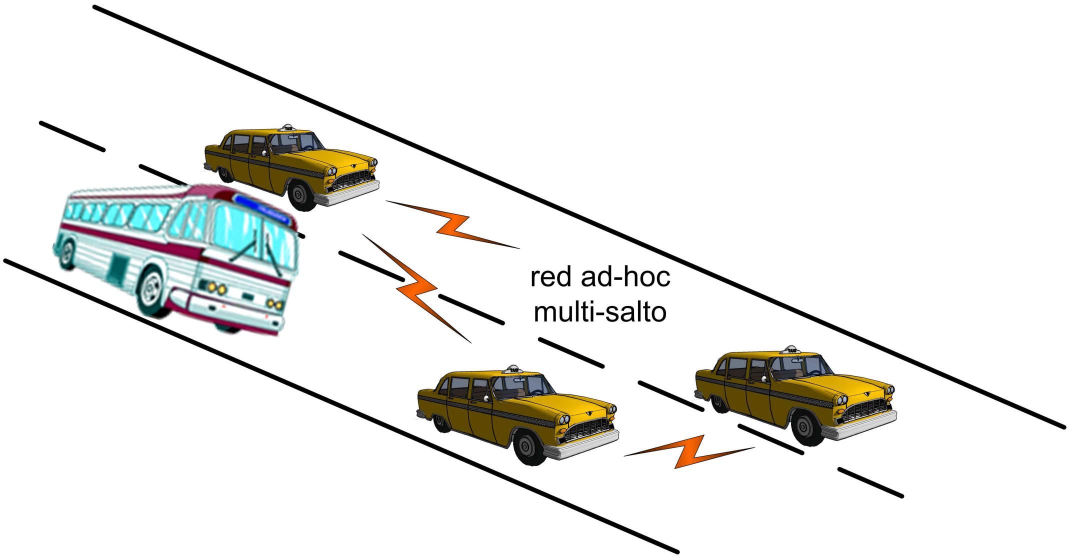


Figura 3.2: Red ad-hoc vehicular (VANET).

- *Encaminamiento.* En una red ad-hoc, no hay ninguna infraestructura de encaminamiento pre-establecida, por lo que los nodos tienen que colaborar en la configuración y mantenimiento de rutas multi-salto. Por lo tanto, se necesitan protocolos de encaminamiento específicos para escenarios ad-hoc.

- *Seguridad.* Debido a la falta de gestión que caracteriza a las redes ad-hoc, la seguridad es un aspecto crítico. Los protocolos dirigidos a trabajar en redes ad-hoc deben diseñarse prestando una especial atención a sus posibles debilidades de seguridad.

- *Autoconfiguración de direcciones IP.* Los protocolos existentes para la autoconfiguración de direcciones IP (en redes con infraestructura) no funcionan en las redes ad-hoc, por lo que tienen que definirse nuevos mecanismos que soporten la autoconfiguración IP de los nodos ad-hoc.

Si, además de las comunicaciones entre vehículos (car-to-car communications), se quiere proporcionar conectividad a Internet a los nodos de una VANET (car-to-Internet scenario), entonces debe resolverse también el siguiente aspecto:

- *Descubrimiento de una pasarela a Internet.* Se necesita un nodo especial, llamado *Internet Gateway* (pasarela a Internet), que conecta la red ad-hoc con la infraestructura. Permitir que los nodos ad-hoc descubran de forma eficiente las pasarelas a Internet supone ciertas dificultades, debido a la naturaleza de las redes MANET.

A continuación analizamos brevemente cada uno de los aspectos enumerados anteriormente.

3.2.1.2. Encaminamiento ad-hoc

Las redes ad-hoc han recibido una gran atención en los últimos años [CCL03], [AWW05], [FJL00]. Debido a su naturaleza inalámbrica, multi-salto y a su alta movilidad, los protocolos de encaminamiento tradicionales (utilizados en redes cableadas) no funcionan correctamente, y por lo tanto no pueden ser empleados, en redes MANET. Una gran cantidad de protocolos de encaminamiento han sido propuestos, la mayoría de ellos dentro del IETF. Algunos de ellos reciben el nombre de *reactivos*, porque se lanza el proceso de encontrar y establecer una ruta hacia un destino sólo cuando hay paquetes que tienen que ser enviados hacia dicho destino (como por ejemplo Ad-hoc On-Demand Distance Vector – AODV [PBRD03] – y Dynamic Source Routing – DSR [JMH04], [JMB01]).

Existen también protocolos conocidos como *proactivos*, porque los nodos proactivamente mantienen una entrada en su tabla de encaminamiento para todos los destinos alcanzables (como Optimized Link State Routing – OLSR [CJ03]), reduciendo de esta forma el tiempo que se necesita para establecer una ruta hacia un destino, aunque ello incrementa la complejidad del protocolo. Más información sobre protocolos de encaminamiento ad-hoc puede encontrarse en [AWD04], [RT99] y [CCL03].

El rendimiento de las redes ad-hoc depende en gran medida del protocolo de encaminamiento empleado y de la tecnología de radio empleada. La mayoría de los trabajos de investigación realizados hasta el momento en temáticas ad-hoc han sido realizados mediante simulación [KCC05], aunque también existen algunos trabajos experimentales, que estudian el rendimiento real de prototipos de redes ad-hoc [MBJ01]. Algunos de estos trabajos se centran en escenarios vehiculares [SBSC02], [SBS$^+$05], demostrando que es factible desplegar redes ad-hoc utilizando equipamiento IEEE 802.11b. Por otro lado, algunos autores afirman que es muy complicado conseguir que una red ad-hoc funcione con más de 10 nodos y 3 saltos intermedios [TLN03]. Se necesitan más trabajos de investigación que analicen el rendimiento de redes ad-hoc reales. Además, la disponibilidad de nuevas tecnologías DSRC (Dedicated Short Range Communication) [ZR03] impulsarán aún más las redes ad-hoc.

3.2.1.3. Seguridad

La seguridad es un aspecto crítico en las redes ad-hoc. Dada la naturaleza inalámbrica, el dinamismo de las redes MANET, y la falta de una infraestructura pre-establecida y de mecanismos de control, proporcionar a esta clase de redes un nivel de seguridad similar al de la Internet clásica (basada en infraestructura) es realmente complejo. Todos las funcionalidades enumeradas anteriormente (encaminamiento, autoconfiguración IP y descubrimiento de pasarelas de Internet) comparten este problema. Existen muchas publicaciones al respecto de la seguridad en ad-hoc, algunos de ellos analizando las amenazas, como [ZH99] y [SA99], y otros proponiendo soluciones a problemas específicos.

Aunque existen otros aspectos de seguridad que han sido tratados, tal y como el estimulo de la cooperación entre nodos, el problema del descarte de paquetes por parte de nodos maliciosos [SBR03], o la provisión de una autoridad de certificación fiable y segura en redes ad-hoc [HBC01], [CBH03], el problema del encaminamiento seguro es el que ha recibido más atención.

Algunos de los protocolos de encaminamiento propuestos actualmente, como AODV [PBRD03], DSDV [PB94] y DSR [JMH04], tienen vulnerabilidades de seguridad que permiten realizar ataques fácilmente. Debido a las importantes diferencias entre las redes IP basadas en infraestructura y las redes ad-hoc, es necesario desarrollar nuevos mecanismos de seguridad

Existen varios tipos de ataques de seguridad que pueden realizarse contra los protocolos de encaminamiento ad-hoc [SDL$^+$02]. A continuación resumimos los más relevantes:

- *Ataques de modificación.* Un nodo malicioso puede causar la redirección de tráfico de datos o ataques de denegación de servicio (Denial-of-Service, DoS) introduciendo cambios en los paquetes de control de encaminamiento o reenviando mensajes de encaminamiento con valores falsos.

- *Ataques de suplantación.* Un nodo malicioso puede suplantar la dirección IP de un nodo legítimo y, por lo tanto *robarle* su identidad y realizar este tipo de ataque combinado con un ataque de modificación. El mayor problema de este tipo de ataques es que es difícil trazar quién es el nodo malicioso.

- *Ataques de fabricación.* Un nodo malicioso puede crear y enviar mensajes de encaminamiento falsos. Este tipo de ataque es difícil de detectar, ya que no es sencillo verificar que un mensaje de encaminamiento en particular es inválido, especialmente cuando indica que un vecinos no puede ser alcanzado.

Los autores de [SDL$^+$02], [SLD$^+$05] proporcionan los siguientes requisitos como aquellos que debe cumplir un protocolo de encaminamiento ad-hoc seguro:

1. La señalización de encaminamiento no puede ser suplantada.

2. No pueden inyectarse mensajes de encaminamiento fabricados en la red.

3. Los mensajes de encaminamiento no pueden ser alterados en tránsito (salvo acorde al funcionamiento normal del protocolo de encaminamiento).

4. No pueden formarse bucles en el encaminamiento como resultado de una acción maliciosa.

5. Las rutas más cortas no pueden ser sustituidas por otras como resultado de una acción maliciosa.

La comunidad investigadora ha tratado los anteriores problemas de seguridad en los protocolos de encaminamiento ad-hoc, intentando proponer mecanismos que cumplan algunos, si no todos, de los requisitos mencionados anteriormente. Un gran número de soluciones ha sido propuesto. A continuación describimos brevemente algunas soluciones representativas:

Ref. [HPJ05] propone una versión segura de DSR (llamada ARIADNE), utilizando claves simétricamente pre-distribuidas o criptografía simétrica pre-desplegada para la autenticación.

SEAD [HJP02] es un protocolo de encaminamiento proactivo seguro, basado en DSDV [PB94], que utiliza cadenas de funciones hash (*hash-chains*).

SAODV [ZA02] es una propuesta para proporcionar seguridad a AODV [PBRD03]. Se utilizan dos mecanismos para asegurar AODV: firmas digitales para autenticar la información no mutable de los mensajes y *hash chains* para asegurar la información mutable (es decir, el número de saltos). Para la información no mutable, la autenticación se realiza extremo a extremo. Sin embargo, la misma técnica no puede aplicarse a la información que puede cambiar en tránsito, porque sería posible que un nodo intermedio suplantara la identidad de un nodo legítimo y modificara el campo que indica el número de saltos en un paquete de petición de ruta (*route request*). Para evitar esto, se utilizan cadenas de hash para proteger la información mutable.

En SRP [PH02], se asume que existe una asociación de seguridad para cada par origen-destino, para poder crear una ruta multi-salto. Este protocolo es vulnerable a algunos ataques, como la fabricación de mensajes de error en una ruta.

Una propuesta muy interesante es ARAN [SDL$^+$02], [SLD$^+$05]. Esta solución utiliza mecanismos de criptografía de clave pública para evitar todos los ataques enumerados con anterioridad. Sin embargo, presenta la desventaja de requerir certificados emitidos por una tercera parte. Este requisito puede afectar al despliegue de la solución, especialmente en entornos vehiculares.

En resumen, podemos concluir que cualquier mecanismo dirigido a trabajar en un escenario ad-hoc debe tener muy en cuenta aspectos de seguridad, si bien muchos protocolos actuales de MANET no lo hacen.

3.2.1.4. Autoconfiguración de direcciones IP

De cara a permitir que las redes MANET puedan soportar servicios IP, todos los nodos de la red deben configurar al menos una dirección IP. Sin embargo, no hay ningún mecanismo estándar que proporcione información de configuración IP a nodos de una red MANET, por lo que es necesario configurar los nodos a priori, lo que evita la formación espontánea de redes ad-hoc.

Los protocolos de configuración IP existentes [TN98] para redes tradicionales con infraestructura asumen la existencia de un único enlace con capacidad de transmisión multipunto para la señalización. Tal enlace no existe en las redes multi-salto sin infraestructura, por lo que es necesario diseñar nuevos mecanismos que permitan la autoconfiguración de direcciones IP en una red MANET [SKP$^+$06], [RRGS05].

De cara a tratar del tema de la autoconfiguración IPv6 en redes MANET, se creó un nuevo grupo de trabajo dentro del IETF, denominado AUTOCONF. Este grupo ha identificado dos posibles escenarios principales [RSCS06] dónde es necesaria la autoconfiguración de direcciones IP para redes MANET:

- Red ad-hoc *aislada* (Stand-alone): una red ad-hoc que no está conectada a ninguna red externa, como por ejemplo las redes en conferencias, las redes en campos de batalla, las redes de vigilancia, etc. Lo más probable es que en estos casos no exista ningún tipo de entidad para la delegación de direcciones o prefijos preestablecida en la red. En este escenario, las direcciones IPv6 no tienen porqué ser globales.

- Redes ad-hoc *híbridas* (en el extremo de una red con infraestructura): una red aislada conectada a Internet. Los nodos de una red híbrida deben obtener direcciones IPv6 globales, para que puedan comunicarse con cualquier otro nodo de la Internet. Esto típicamente requiere descubrir el prefijo IPv6 disponible en la red MANET y configurar una dirección única (no utilizada) a partir de este prefijo [BC06].

Aunque el grupo de trabajo AUTOCONF está aún trabajando en la definición del protocolo, ya existen muchas soluciones en la actualidad. Una clasificación de las más relevantes puede encontrarse en [BC05].

3.2.1.5. Descubrimiento de una pasarela a Internet

Para proporcionar conectividad a una red MANET híbrida [RRGS05], además de un direccionamiento IPv6 global, se necesita de un tipo de nodo especial en la red ad-hoc. La pasarela a Internet (Internet Gateway, IGW) es un nodo que tiene conexión tanto a una red de acceso con infraestructura como a la red ad-hoc, y que proporciona conectividad a los nodos conectados a esta última. Un IGW puede ser móvil o fijo y es de vital importancia para proporcionar conectividad a los nodos que están del lado MANET. Debido a las características de las redes MANET, es deseable que se desplieguen múltiples IGWs (por ejemplo, para mitigar problemas relativos a congestión).

Actualmente, una propuesta muy común para proporcionar conectividad a Internet en los vehículos consiste en desplegar IGWs a los lados de las carreteras, de forma que los vehículos que pasen puedan usarlos para acceder a Internet. Uno de los retos que supone esta arquitectura es cómo descubrir eficientemente los IGWs disponibles [BWSF03], ya que uno de los componentes clave que afectan al rendimiento global es el algoritmo empleado par descubrir y seleccionar IWGs [RGS04].

Desplegar una infraestructura de red consistente en varios IGWs en las carreteras y confiar en el encaminamiento multi-salto en las redes ad-hoc vehiculares formadas no es suficiente. Podrían existir ”agujeros” en la conectividad, que podrían evitar que los vehículos se comunicaran (no sólo entre sí, sino también con Internet). Además, los IGWs podrían no pertenecer todos al mismo proveedor y por lo tanto, no sería posible que un vehículo pudiera mantener la misma dirección IPv6 al moverse de un IGW a otro. Aunque existen soluciones que mitigan el efecto de la conectividad intermitente, como la descrita en [OK04] para una red no ad-hoc (basada en pasarelas de aplicación y proxies), debería permitirse la posibilidad de conmutar a otra interfaz de red (p.e., celular, como GPRS o UMTS) manteniendo de forma transparente las sesiones existentes (es decir, soporte de movilidad transparente real).

Las soluciones basadas principalmente en ad-hoc presentan algunos inconvenientes. Por ejemplo, hay algunos aspectos de seguridad que no están resueltos aún y no proporcionan un soporte de movilidad global. Por lo tanto, este tipo de solución no es válido para satisfacer todos los requisitos del escenario vehicular.

3.2.2. Soluciones basadas en movilidad de terminal

Una forma diferente de soportar comunicaciones vehiculares consiste en considerar cada coche como un terminal individual y emplear técnicas que utilizan IP móvil par soportar la movilidad del terminal. A este tipo de soluciones es a las que denominamos *soluciones basadas en movilidad de terminal*.

Este tipo de soluciones están basadas en aprovechar los protocolos inalámbricos y de movilidad existentes, haciendo los cambios necesarios para incrementar el rendimiento en entornos vehiculares. Un ejemplo muy sencillo consiste en utilizar soluciones basadas en redes celulares 2.5G/3G [AVN00].

Otro ejemplo es la arquitectura definida en el proyecto Drive-thru [OK04]. Está basada en proporcionar algunos servicios de Internet útiles en entornos con conectividad intermitente. Los coches obtienen esta conectividad intermitente conectándose a puntos de acceso WLAN desplegados en la carretera.

En algunos escenarios resulta interesante combinar un mecanismos de IP móvil con soluciones ad-hoc, de cara a soportar el movimiento de los vehículos entre redes ad-hoc y redes con infraestructura. Esto requiere permitir la *movilidad global* entre diferentes tipos de redes de acceso (ad-hoc o con infraestructura) para preservar de forma transparente la conectividad de los vehículos. La mayoría de las propuestas para la gestión global de la movilidad en redes ad-hoc están basadas en adaptar los mecanismos de IP móvil existentes para ser utilizados con protocolos de encaminamiento ad-hoc particulares.

Una de las propuestas más conocidas es MIPMANET [JAL+00], que básicamente propone una solución basada en IPv4 Móvil y AODV. Para combinar la naturaleza reactiva de AODV con la proactiva de IPv4 Móvil, los Agentes Foráneos (Foreign Agents, FAs) se anuncian periódicamente en la red ad-hoc. Los Agentes Foráneos son utilizados como pasarelas a Internet (IGWs), de cara a mantener información sobre en qué red ad-hoc se encuentra localizado un nodo y para encaminar los paquetes hacia el borde de dicha red ad-hoc. Se utiliza AODV para entregar los paquetes entre el FA y el nodo móvil. Se emplea un enfoque en capas y túneles para el tráfico saliente de la red ad-hoc, de forma tal que se separa la funcionalidad de IPv4 Móvil del protocolo de encaminamiento ad-hoc. Se propone un mecanismo similar en MEWLANA [EP02], pero adecuado para el protocolo de encaminamiento Destination-Sequenced Distance Vector (DSDV) [PB94]. En [RK03], se combinan técnicas tales como limitar la inundación de los anuncios de los Agentes Foráneos a un vecindario de n-saltos de radio – utilizando para ello un campo de tiempo de vida (TTL) en los mensajes de anuncio –, y espiar y cachear mensajes de agentes, para mejorar el rendimiento. De manera similar, un mecanismo que integra IPv4 Móvil y OLSR se propone en [BMA+04].

En relación al soporte de IPv6, [PMW+02] describe cómo proporcionar conectividad a Internet con soporte de IPv6 Móvil a redes ad-hoc. IPv6 Móvil utiliza el protocolo de *Neighbour Discovery* como parte de su mecanismo de detección de movimiento, con la adquisición de una dirección IP globalmente encaminable. Este mecanismo de detección de movimiento es modificado en las redes ad-hoc, en las que el IGW juega el papel de router local y los *Router Advertisements* son reemplazados por *Gateway Advertisements*. La dirección IPv6 configurada del prefijo de la red MANET que se incluye en los anuncios emitidos por el IGW es utilizada como la CoA del MN. Esta manera de realizar la detección de movimiento tiene el inconveniente de que requiere más tiempo que descubrir el movimiento entre dos puntos de conexión a la Internet fija, debido a que los Gateway Advertisements no son enviados con tanta periodicidad como los Router Advertisements (para evitar consumir recursos radio en exceso). Otros mecanismos propuestos para el soporte de movilidad global IPv6 en redes ad-hoc son [HSFN04] – que adopta una arquitectura jerárquica (basada en HMIPv6) para permitir que los nodos ad-hoc se registren en más de un AR/IGW simultáneamente – y [HLWC05] – que propone un protocolo que automáticamente organiza la red ad-hoc en una arquitectura en árbol para facilitar el direccionamiento y encaminamiento dentro de la red MANET.

También existen algunas soluciones propuestas que tratan específicamente con el escenario *car-to-car*. Un ejemplo es [BW05], que es similar a MIPMANET [JAL$^+$00], en el sentido de que reutiliza el concepto de Agente Foráneo de IPv4 Móvil – colocado en el IGW – para gestionar la movilidad global de nodos ad-hoc. Se sigue empleando comunicación IPv4 entre el HA y el FA (utilizando túneles IPv6-en-IPv4), ya que la solución asume una Internet basada en IPv4 (los autores también proponen el uso de una arquitectura basada en proxies para soportar que vehículos que soporten sólo IPv6 puedan comunicarse con CNs IPv4 en la Internet). Tal y como se hace en [RK03], los FAs anuncian activamente su servicio, pero limitado a áreas locales, para evitar inundar toda la red vehicular.

Las soluciones basadas en movilidad de terminal tienen un inconveniente principal, consistente en que no tienen en cuenta que un vehículo muy probablemente contendrá más de un dispositivo que podría beneficiarse de disponer de acceso a Internet. Las soluciones basadas en movilidad de terminal requieren que todos los dispositivos gestionen su propia conectividad y movilidad (aunque se muevan todos juntos a la vez) y por lo tanto evita que nodos sin soporte de movilidad puedan ser desplegados en coches.

3.2.3. Soluciones basadas en movilidad de redes

Debido a que el escenario vehicular involucra a un grupo de dispositivos que se mueven juntos, tanto el caso de comunicaciones *car-to-Internet*, como el caso *car-to-car*, pueden ser abordados asumiendo que hay un router móvil desplegado en cada vehículo, encargado de gestionar la movilidad del grupo de dispositivos que se encuentra dentro del vehículo (a este tipo de soluciones, las denominamos *soluciones basadas en movilidad de redes*). Sin embargo, cabe destacar que después de estudiar la literatura relacionada, hemos encontrado muy pocas propuestas que consideran enfoques de movilidad de redes para escenarios vehiculares, puesto que la mayoría de los mecanismos consideran los coches como terminales individuales.

El escenario particular de comunicaciones *car-to-Internet* encaja muy bien en el paradigma de la Movilidad de Redes. Por lo tanto, la aplicación de un conjunto de soluciones genérico de movilidad de redes debe ser estudiada para el caso de comunicaciones ente vehículos e Internet. De hecho, es un buen ejemplo de escenario dónde se necesitan soluciones de optimización de rutas para movilidad de redes.

El escenario *car-to-car* también puede ser abordado utilizando una solución genérica NEMO. Sin embargo, ese tipo de solución no ofrece un rendimiento demasiado bueno en una comunicación entre vehículos, incluso aún cuando se utiliza alguna solución genérica de optimización de rutas para NEMO. Las razones para este subóptimo rendimiento son las siguientes:

- Las Redes Hogar de dos coches que se están comunicando pueden no ser la misma o estar localizadas lejos una de la otra. Esto hace muy necesaria la implantación de una solución de optimización de rutas, para evitar un incremento en el retardo debido a la utilización del protocolo de Soporte Básico de NEMO.

- Los coches muy probablemente obtendrán conectividad a Internet mediante una red celular 2.5/3G. Esta clase de redes típicamente presenta unos retardos muy elevados y

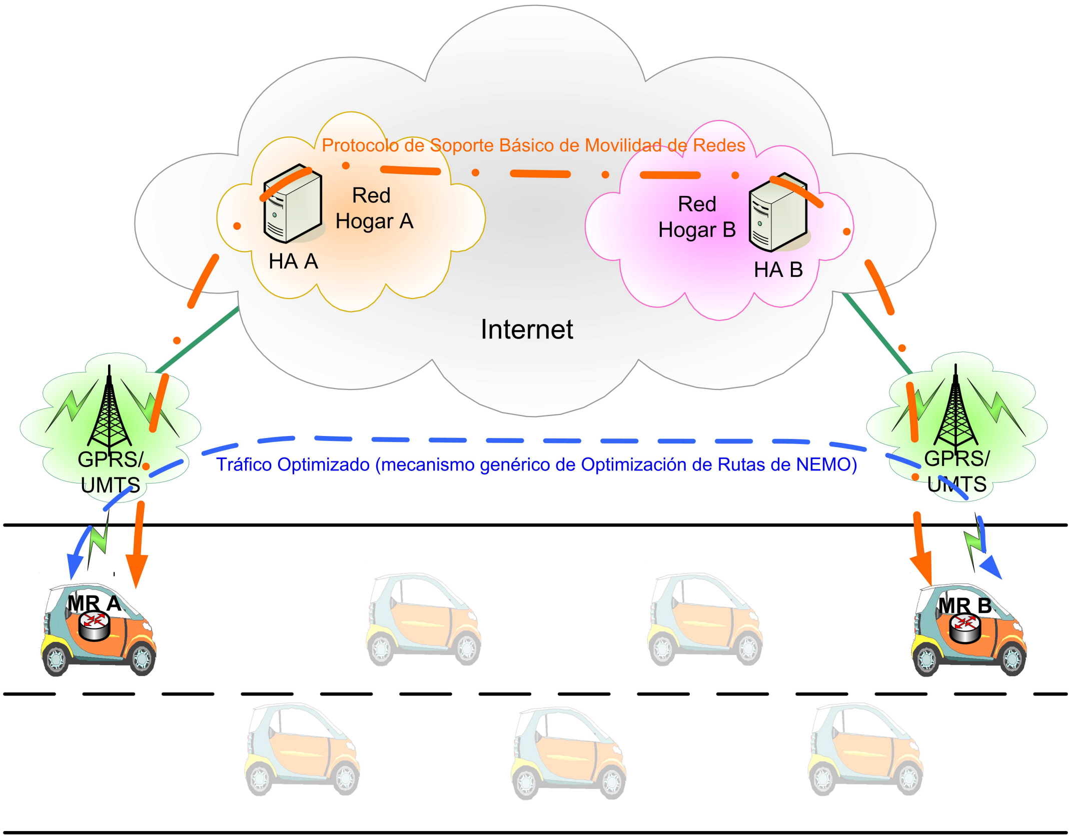

Protocolo de Soporte Básico de Movilidad de Redes
Red Hogar A
HA A
Red Hogar B
HA B
Internet
GPRS/ UMTS
Tráfico Optimizado (mecanismo genérico de Optimización de Rutas de NEMO)
GPRS/ UMTS
MR A
MR B

Figura 3.3: Funcionamiento de una solución genérica de Movilidad de Redes en el escenario *car-to-car*.

> unos anchos de banda reducidos [VBM+05], [VBS+06]. Esto tiene un gran impacto en las comunicaciones inter-vehiculares cuando se usa una solución NEMO genérica. Un ejemplo de escenario *car-to-car* se muestra en la Figura 3.3. Si se utiliza el protocolo de Soporte Básico de Movilidad de Redes [DWPT05], el tráfico de datos fluye desde el Router Móvil de un coche (MR A) hacia su Red Hogar (Red Hogar A), dónde los paquetes son reenviados hacia la Red Hogar del otro coche (Red Hogar B) y finalmente entregados al Router Móvil B (MR B). Ésta es claramente una ruta subóptima. Si se utiliza una solución genérica de optimización de rutas, los paquetes no atraviesan las diferentes Redes Hogar de las redes móviles involucradas, pero siguen teniendo que pasar por la infraestructura para ser enviadas de un coche a otro. Esto puede significar un elevado retardo (las redes GPRS presentan retardos de unos 500 ms sólo en un sentido [VBM+05], [VBS+06], mientras que las redes UMTS tienen unos 150 ms [MdlOS+06], [OMV+06]) y un ancho de banda reducido. Por lo tanto, deben explorarse diferentes esquemas de optimización de rutas.

Aunque los coches pueden comunicarse entre sí a través de la infraestructura – empleando el protocolo de Soporte Básico de NEMO –, una conclusión que se puede obtener de la anterior discusión, es que los esquemas clásicos de optimización de rutas NEMO no ofrecen un buen rendimiento en las comunicaciones inter-vehiculares. Sin embargo, hay una oportunidad de optimización que está siendo actualmente estudiada en el campo de las comunicaciones inter-vehiculares (inter-vehicular communications, IVC). Esta optimización está basada en la utilización de redes ad-hoc vehiculares (VANET), para explotar la conectividad entre coches vecinos, y el establecimiento una ruta multi-salto para soportar los servicios inter-vehiculares. La aplicación de este enfoque a una solución vehicular basada en NEMO es uno de los objetivos de esta Tesis Doctoral. En ella exploramos como diseñar un mecanismo basado en movilidad de redes que optimiza las comunicaciones inter-vehiculares, aprovechando que los MRs pueden establecer redes ad-hoc para comunicarse directamente (evitando pasar por la infraestructura).

De acuerdo a nuestro conocimiento, sólo hay una propuesta combinando los enfoques de NEMO y ad-hoc [WOKN05], [WMK+05], [WMK+04], [OWUM04]. La solución (definida en [WOKN05], [WMK+05], [WMK+04]) básicamente considera redes MANET que se mueven juntas (por ejemplo, dentro de un coche) e integra MANET y NEMO, colocando las funcionalidades del IGW y el MR en lo que denominan *Pasarela Móvil* (Mobile Gateway, MG). El protocolo de Soporte Básico de Movilidad de Redes [DWPT05] es responsable de proporcionar conectividad a Internet a la MANET móvil (por lo tanto, no es necesario que los nodos de dicha MANET soporten el protocolo IPv6 Móvil), mientras que un protocolo de encaminamiento ad-hoc adicional es ejecutado ente las Pasarelas Móviles, creando una red MANET superpuesta para comunicaciones entre diferentes redes móviles. Este esquema permite la comunicación directa entre nodos de MANETs móviles que pertenecen a la misma MANET superpuesta (usando la denominada *ruta directa*), mientras que el protocolo de Soporte Básico de Movilidad de Redes se utiliza para el resto de los casos (*ruta nemo*). Además, el mecanismo permite que un MG pueda tomar prestada la conectividad a Internet de un MG adyacente (*ruta detour*). Se propone utilizar un protocolo de encaminamiento ad-hoc proactivo para la MANET superpuesta, en particular, OLSR es considerado en [OWUM04].

La solución descrita anteriormente es una primera aproximación para combinar de manera óptima NEMO y ad-hoc para soportar comunicaciones vehiculares. Los autores han dejado como trabajo futuro el análisis de seguridad, por lo que en la arquitectura que ellos proponen, por ejemplo, nada previene a nodos malintencionados robar tráfico o realizar un ataque de inundación a la Red Hogar (Return-to-Home Flooding [NAA+05] attack). Esta falta de seguridad es un aspecto crítico, especialmente en entornos inter-vehiculares.

El diseño de un mecanismo basado en una solución de movilidad de redes combinado con soporte ad-hoc, de una forma *segura*, para permitir comunicaciones vehiculares óptimas es uno de los objetivos clave de esta Tesis Doctoral.

Part II

Route Optimisation for Mobile Networks in IPv6 Heterogeneous Environments

Optimización de Rutas para Redes Móviles en Entornos IPv6 Heterogéneos

Chapter 4

Goals and Design considerations

4.1. Introduction

This chapter enumerates the main goals of this PhD thesis and provides some design considerations that have been followed in the fulfilment of these goals.

4.2. Goals

The main goal of this PhD thesis is to design a set of solutions providing Route Optimisation support for Network Mobility, in such a way that the solutions are secure and easily deployable. A second objective of this PhD thesis is to develop a Route Optimisation solution for vehicular environments, by combining in a secure way Network Mobility and Ad-hoc concepts. Next, we elaborate more on the specific goals and requirements that the designed solutions solution should meet.

There are many possible scenarios where Network Mobility will play a key role, some of them related to the provision of Internet access from mobile platforms, such as cars or buses. We believe that there is a severe drawback in the existing standardised solution supporting Network Mobility [DWPT05], [dlOBC06], that is the sub-optimal packet routing that this solution forces in order to preserve mobility transparency. This sub-optimality can lead even to prevent communications from taking place, and therefore should be tackled if it is desired to deploy moving networks in practice.

A general overview of the existing proposals on Route Optimisation for NEMO[1] has been provided in Section 2.4, highlighting their problems and those issues that are still unsolved. Taking this into account, a brief summary of the requirements that we consider that a generic Route Optimisation (RO) for NEMO solution should fulfil (in order to be rapidly deployed in current scenarios) is provided next:

- The NEMO Route Optimisation solution should provide **support for legacy nodes**. In order to facilitate the practical deployment of the solution today, it should not require changes on the operation of any node but the Mobile Router and maybe the

[1] The interested reader may refer to [NZWT06], [PSS04b] and [LLKC05] for published surveys on existing Route Optimisation solutions for NEMO.

Home Agent of the mobile network. Therefore, Correspondent Nodes, Local Fixed Nodes and Mobile IPv6 hosts connected to a Mobile Network should not require any modification to be compatible with the NEMO RO mechanism. This does not necessarily imply that the mechanism should be able to optimise the traffic of any node in any scenario, but that at least the use of the RO mechanism on a network should not prevent any node from being able to communicate through the mobile network.

- The NEMO Route Optimisation solution should support the optimisation of communications of **Local Fixed Nodes** attached to a NEMO, that is, the mechanism should enable direct path routing between a CN and an LFN, by providing Angular Route Optimisation. Local Fixed Nodes will represent a large number of the nodes attached to a NEMO, for example in a moving vehicle, such a car, where it is likely to expect that many of the nodes that will require Internet connectivity, such as sensors, on-board computer, infotainment devices, etc, will have no mobility support at all. Therefore, providing them with NEMO RO is critical to exploit the benefits of a network mobility solution. To achieve that, mobility transparency (i.e. LFNs not being aware of the mobility of the NEMO) should be preserved.

- The NEMO Route Optimisation solution should support the optimisation of communications of **Visiting Mobile Nodes** attached to a NEMO. This means that the mechanisms should enable direct path communication between a VMN and its HA – when the VMN is operating in Bidirectional Tunnel (BT) mode – or between a VMN and a CN – when the VMN is operating in Route Optimisation (RO) mode.

- The NEMO Route Optimisation solution should support the optimisation of communications involving **nested configurations of Mobile Routers**, that is the number of tunnels traversed by packets belonging to a communication between a MNN attached to a sub-MR and a CN should be eliminated (or at least minimised), by providing Multi-angular Route Optimisation. At least, 3 levels of nesting should be supported, since nowadays, a higher number of nesting levels is not foreseen.

- The NEMO Route Optimisation solution should be **secure**, at least as secure as current NEMO Basic Support protocol and Mobile IPv6 are. Therefore, the solution should provide a similar level of security than the Route Optimisation solution of Mobile IPv6 [JPA04], [NAA$^+$05].

- If the specific mechanism designed to provide Angular Route Optimisation differs from those used to cope with the different configurations of Multi-angular Route Optimisation, they should be **interoperable** in such a way that an optimal route results from the combined operation of both.

- The NEMO Route Optimisation solution should be **scalable**, so that in case of large mobile networks in terms of number of attached nodes, the designed RO solution should allow many sessions to be optimised, minimising the additional resources needed in any node of the network, compared to the resources required by plain NEMO Basic Support protocol.

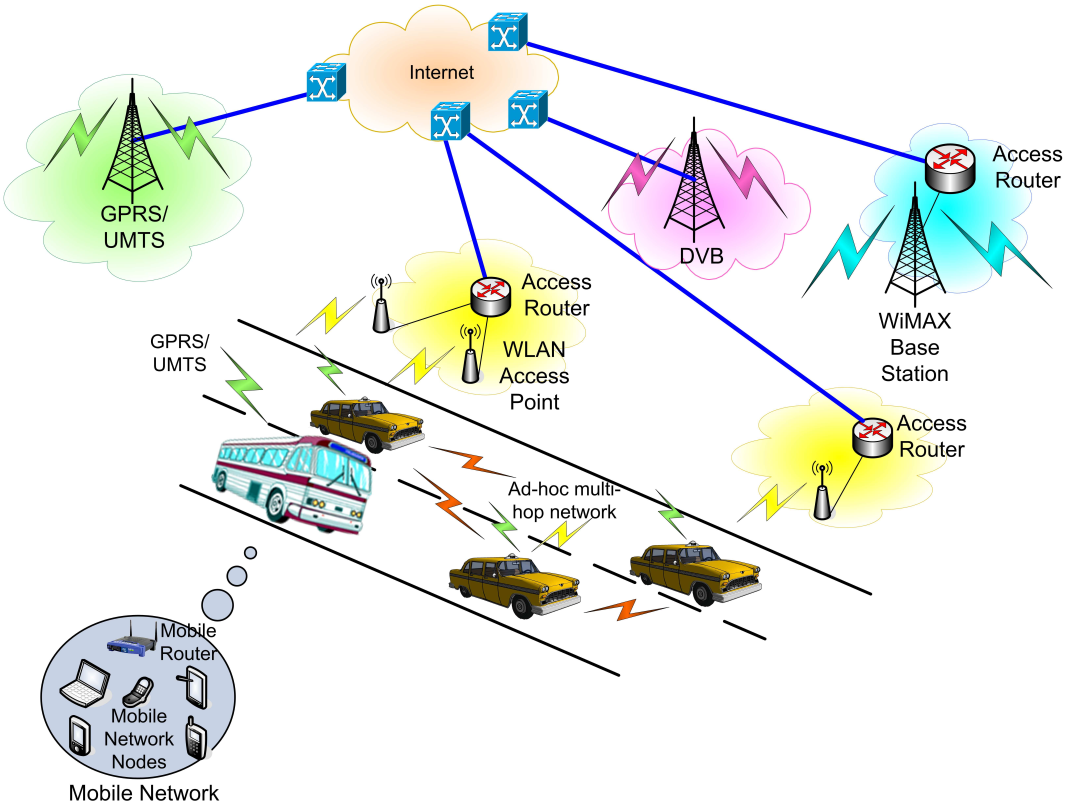


Figure 4.1: Vehicular communications scenario.

- The NEMO Route Optimisation solution should **minimise additional protocol complexity, processing load and signalling overhead** in order to facilitate the deployment of the solution in real scenarios.

- The NEMO Route Optimisation solution should **minimise the effect of increased handover delay** that it may have, when compared to the plain NEMO Basic Support protocol handover.

These are very **strong requirements** that, according to our analysis of the current state of the art (summarised in Chapter 2), are not fulfilled by any existing solution. This PhD thesis proposes a generic Route Optimisation for NEMO solution (described in detail in Chapter 5) that take these requirements as the basic design criteria.

Chapter 3 introduced the issue of vehicular communications. Vehicular scenarios (an example is shown in Figure 4.1) are becoming very important nowadays, since there exists a number of new services and applications that will likely be deployed in cars when they are provided with communication capabilities. Because of the importance of this particular scenario, it is needed to provide the tools and mechanisms that enable the optimisation of vehicular communications.

An objective of this PhD thesis is the study of an existing opportunity for **optimisation** of local communications in vehicular environments by using an **ad-hoc network** formed by the vehicles involved in the communication and perhaps other vehicles in their surroundings. The design of a solution that optimally combines a Network Mobility approach with multi-hop ad-hoc communications in a secure way, and the evaluation of its performance in car-to-car communications, is the second main goal of this PhD work.

4.3. Design considerations

In this section we briefly summarise the considerations that we have adopted for the design of the mechanisms proposed in this PhD thesis. The rationale behind these considerations is provided in the PhD thesis when the specific mechanisms are described.

Since we aim at designing a generic Route Optimisation solution for NEMO and a mechanism that addresses the specific issue of vehicular communications, being both suitable for existing legacy nodes and not requiring changes on the operation of any node but the Mobile Router, there are several design aspects that should be addressed:

- *Layer of the protocol stack.* It seems clear that if it is required to avoid changes on the nodes, IP it is the only possible choice, since IP already has some mobility support, provided by the Mobile IPv6 [JPA04] protocol. It may be argued that the mobility can also be handled at other layers, but as it was briefly discussed in Section 2.1 (when talking about how Network Mobility could be provided), making it at the application [HLZ06] or transport [CAI06] layers requires the modification of all the applications or transport protocols to support mobility, which is redundant. On the other hand, making it at the link layer is not feasible if mobility across different technologies is required. Therefore, the option chosen is to **implement the designed mechanisms at the IP layer, using/modifying the Mobile IPv6 protocol.**

- *Entities involved on the optimisation.* Since one of our requirements is not to change any node but the MR (and maybe also the HA), it is clear that neither VMNs, not LFNs nor CNs can be changed. However, there would be the possibility of involving some nodes on the routing infrastructure in the optimisation, such as proposed in [WKUM03] and [WW04]. Nevertheless, as the deployment and scalability of the solution are also very important design considerations, the requirement of involving external nodes to perform the optimisation is not feasible. Therefore, the option chosen is to **put all the specific new functionalities required to perform the Route Optimisation on the Mobile Router only.** This does not mean that the designed mechanisms cannot make use of available mobility capabilities that certain Mobile Network Nodes (e.g., VMNs) may have.

Capítulo 4

Objetivos y Consideraciones de Diseño

4.1. Introducción

Este capítulo enumera los principales objetivos de esta Tesis Doctoral y proporciona algunas consideraciones de diseño que han sido seguidas para el cumplimiento de los objetivos perseguidos.

4.2. Objetivos

El objetivo principal de esta Tesis Doctoral es el diseño de un conjunto de soluciones que proporcionen soporte de optimización de rutas para redes móviles, de tal forma que las soluciones propuestas sean seguras y fácilmente desplegables. Un segundo objetivo de esta Tesis es el desarrollo de una solución de optimización de rutas para entornos vehiculares, mediante la combinación de forma segura de los conceptos de movilidad de redes y ad-hoc. A continuación se desarrollan un poco más las metas específicas y los requisitos que las soluciones diseñadas deben cumplir.

Existen muchos posibles escenarios donde la movilidad de redes jugará un papel clave, algunos de ellos relacionados con la provisión de acceso a Internet en plataformas móviles, como coches o autobuses. Creemos que hay un severo problema en la solución estandarizada existente para el soporte de la movilidad de redes [DWPT05], [dlOBC06], consistente en el encaminamiento subóptimo de paquetes que fuerza dicha solución de cara a preservar la transparencia de la movilidad. Este efecto subóptimo puede llegar incluso a impedir que las comunicaciones lleguen a efectuarse, y por lo tanto debe ser resuelto si se desea que las redes móviles puedan llegar a desplegarse en la práctica.

Una panorámica general de las propuestas existentes en relación a la optimización de rutas en redes móviles[1], ha sido proporcionada en la Sección 2.4, resaltando sus problemas y aquellos puntos que están todavía sin resolver. Teniendo esto en cuenta, a continuación se incluye un breve resumen de los requisitos que consideramos que una solución genérica

[1] El lector interesado puede acudir a [NZWT06], [PSS04b] y [LLKC05], para encontrar publicaciones que clasifican soluciones existentes de optimización de rutas para redes móviles.

de optimización de rutas para redes móviles debe cumplir (de cara a facilitar un rápido despliegue de la solución en los escenarios existentes):

- La solución de optimización de rutas para redes móviles debe proporcionar **soporte para nodos legados**. De cara a facilitar un rápido despliegue de la solución, ésta no debe requerir cambios en el funcionamiento de ningún nodo salvo el Router Móvil y quizás el Agente Local de la red móvil. Por lo tanto, ni los Nodos Corresponsales, ni los Nodos Locales Fijos ni los Nodos Móviles (que implementen IPv6 Móvil) conectados a una red móvil deben precisar cambios para ser compatibles con el mecanismo de optimización de rutas. Esto no implica necesariamente que el mecanismo deba ser capaz de optimizar el tráfico de todos los nodos en cualquier escenario, pero sí que al menos, la utilización de un mecanismo de optimización de rutas en una red no impida que ningún nodo sea capaz de comunicarse a través de la red móvil.

- La solución de optimización de rutas para redes móviles debe soportar la optimización de comunicaciones de **Nodos Locales Fijos** conectados a la red móvil, es decir, el mecanismo debe habilitar la comunicación directa entre un CN y un LFN, proporcionando optimización de rutas angular. Los Nodos Locales Fijos representarán un gran porcentaje de los nodos conectados a una red móvil, por ejemplo en un vehículo, como un coche, dónde es probable esperar que muchos de los nodos que requieran conectividad a Internet, como sensores, ordenadores de abordo, dispositivos de entretenimiento, etc., no tendrán soporte de movilidad alguno. Por lo tanto, es vital proporcionar a esta clase de nodos soporte de optimización de rutas, de cara a explotar los beneficios que brinda una solución de movilidad de redes. Para conseguir esto, la transparencia de la movilidad (los LFNs no deben ser conscientes de la movilidad de la red a la que están conectados) debe preservarse.

- La solución de optimización de rutas para redes móviles debe soportar la optimización de comunicaciones de **Nodos Móviles Visitantes** conectados a una red móvil. Esto significa que los mecanismos deben habilitar la comunicación directa entre un VMN y su HA – cuando el VMN está operando en modo de Túnel Bidireccional – o entre un VMN y un CN – cuando el VMN está operando en modo de Optimización de Rutas.

- La solución de optimización de rutas para redes móviles debe soportar la optimización de comunicaciones que involucren **configuraciones anidadas de routers móviles**, es decir, debe eliminarse el número de túneles atravesados por un paquete perteneciente a una comunicación entre un MNN conectado a un sub-MR y un CN (o al menos minimizar dicho número), proporcionando optimización de rutas multi-angular. Al menos deben soportarse 3 niveles de anidamiento, ya que actualmente no se prevé un número mayor de niveles de anidamiento.

- La solución de optimización de rutas para redes móviles debe ser **segura**, al menos tan segura como el protocolo de Soporte Básico de Movilidad de Redes e IPv6 Móvil. Por lo tanto, la solución debe proporcionar un nivel de seguridad similar al que presenta la solución de optimización de rutas de IPv6 Móvil [JPA04], [NAA$^+$05].

- Si el mecanismo específico diseñado para proporcionar optimización de rutas angular es diferente de aquel utilizado para soportar las diferentes configuraciones de optimi-

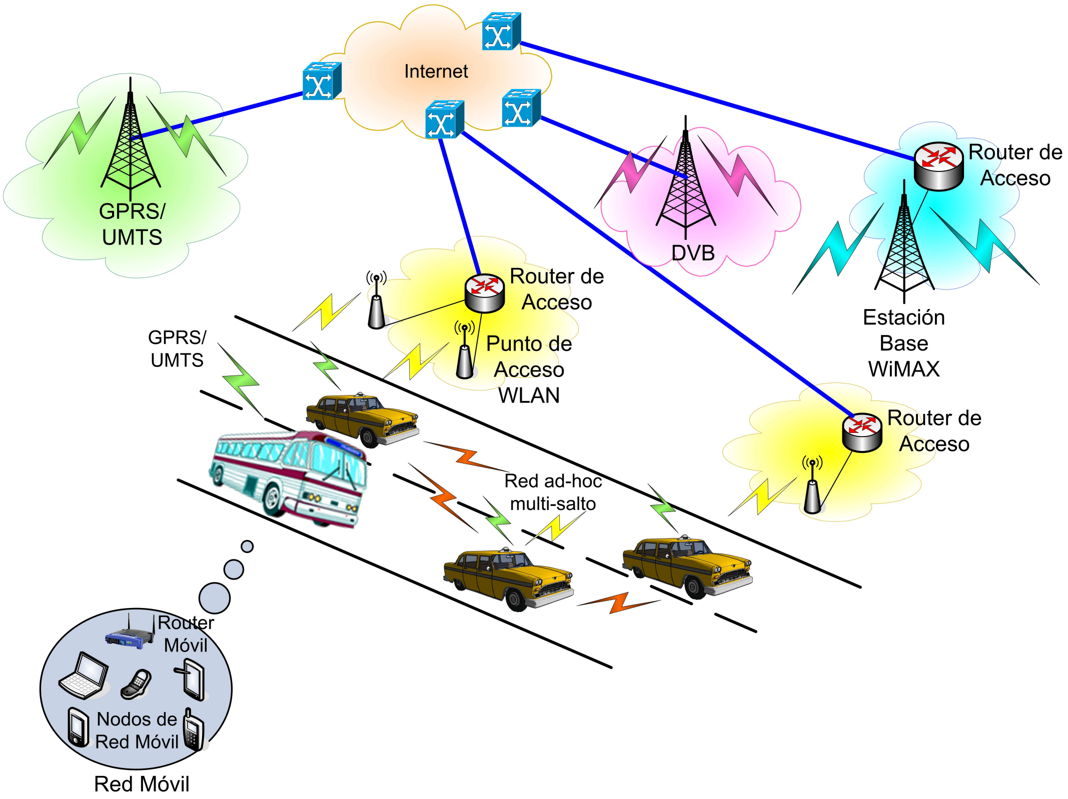


Figura 4.1: Escenario de comunicaciones vehiculares.

zación de rutas multi-angular, los dos mecanismos deben ser **interoperables**, de una forma tal que resulte una ruta óptima del funcionamiento combinado de ambos.

- La solución de optimización de rutas para redes móviles debe ser **escalable**, de forma tal que la solución diseñada permita optimizar un gran número de comunicaciones en caso de redes móviles muy grandes, minimizando los recursos adicionales requeridos en cualquier nodo de la red, comparado con los recursos que requiere el protocolo de Soporte Básico de Movilidad de Redes.

- La solución de optimización de rutas para redes móviles debe **minimizar la complejidad adicional del protocolo, la carga de procesamiento y la sobrecarga de señalización**, de cara a facilitar el despliegue de la solución en escenarios reales.

- La solución de optimización de rutas para redes móviles debe **minimizar el efecto de incremento en el retardo del traspaso**, que pudiera tener, comparado con el retardo de un traspaso utilizando el protocolo de Soporte Básico de Movilidad de Redes.

Los anteriores, son **requisitos muy fuertes** que, de acuerdo a nuestro análisis del estado del arte actual (resumido en el Capítulo 2), ninguna solución existente cumple. Esta Tesis Doctoral propone una solución genérica de optimización de rutas para redes móviles (descrita en detalle en el Capítulo 5) que adopta los requisitos anteriores como criterio básico.

El Capítulo 5 introdujo la problemática de las comunicaciones entre vehículos. Los escenarios vehiculares (un ejemplo se muestra en la Figura 4.1) están adquiriendo gran importancia actualmente, dado que existe un número de nuevos servicios y aplicaciones que muy probablemente serán desplegados en los coches cuando éstos dispongan de capacidades de comunicación en red. Debido a la importancia de este escenario particular, es necesario proporcionar las herramientas y mecanismos que faciliten la optimización de las comunicaciones vehiculares.

Un objetivo de la presente Tesis Doctoral es el estudio de la oportunidad de **optimización** que existe en comunicaciones locales entre vehículos, por medio de una **red ad-hoc** formada por los vehículos involucrados en la comunicación y quizás otros vehículos cercanos. El diseño de una solución que combine de forma segura el enfoque de movilidad de redes con el de las redes ad-hoc multi-salto, y la evaluación de su rendimiento en comunicaciones inter-vehiculares, es el segundo objetivo principal de esta Tesis.

4.3. Consideraciones de Diseño

En esta sección resumimos brevemente las consideraciones que hemos adoptado en el diseño de los mecanismos propuestos en esta Tesis Doctoral. El razonamiento subyacente se proporciona en la Tesis cuando los mecanismos específicos son descritos.

Dado que queremos diseñar una solución genérica de optimización de rutas para redes móviles y un mecanismo dirigido a la problemática específica de las comunicaciones vehiculares, siendo ambos aptos para su utilización con nodos legados y sin que se precisen cambios en el funcionamiento de ningún nodo, salvo el router móvil, hay algunos aspectos de diseño que deben ser considerados:

- *Capa de la pila de protocolos.* Parece claro que si se quiere evitar cambiar el funcionamiento de los nodos, IP es la única posibilidad, dado que IP ya cuenta con cierto soporte de movilidad, proporcionado por el protocolo IPv6 móvil [JPA04]. Podría argumentarse que la movilidad se puede gestionar en otras capas de la pila de protocolos, pero como ya fue brevemente discutido en la Sección 2.1 (cuando se hablaba sobre cómo se podía proporcionar soporte de movilidad de redes); hacerlo en las capas de aplicación [HLZ06] o transporte [CAI06] requeriría la modificación de todas las aplicaciones o protocolos de transporte para soportar la movilidad, lo cual es redundante. Por otro lado, no es posible hacerlo en el nivel de enlace si se quiere soportar movilidad entre diferentes tecnologías. Por lo tanto, la opción escogida es **implementar los mecanismos diseñados en la capa IP, usando/modificando el protocolo IPv6 Móvil.**

- *Entidades involucradas en la optimización.* Dado que uno de requisitos es no cambiar ningún nodo salvo el MR (y quizás también el HA), parece claro que ni los VMNs, ni los LFNs ni los CNs pueden ser cambiados. No obstante, existiría la posibilidad de involucrar a algunos nodos de la infraestructura de encaminamiento en la optimización, como se propone en [WKUM03] y [WW04]. Sin embargo, como la desplegabilidad y escalabilidad de la solución son también consideraciones de diseño muy importantes, no parece adecuado involucrar a nodos externos en la optimización. Por lo tanto, la opción elegida es **poner todas las funcionalidades requeridas para realizar la optimización de rutas en el router móvil exclusivamente.** Esto no significa que los mecanismos desarrollados no puedan hacer uso de las capacidades de movilidad que determinados Nodos de Red Móvil (p.e., MNNs) puedan tener.

Chapter 5

Generic Route Optimisation solution for Network Mobility

5.1. Introduction

The Network Mobility (NEMO) Basic Support protocol [DWPT05] enables complete networks to roam among different access networks, without disrupting network nodes' ongoing sessions and without requiring any specific mobility capability in the hosts. Nevertheless, it has some important limitations in terms of performance (see section 2.3), due to the increased path length and the packet overhead that this solution introduces. Such limitations triggered the need for what has been called Route Optimisation (RO) for NEMO. Although there exist a number of proposed solutions that try to overcome the suboptimal routing problems that arise due to use the NEMO Basic Support protocol (see section 2.4), there is no solution that addresses the multifold problem of Route Optimisation in such a way that it solves all the main limitations of the NEMO Basic Support protocol under the most important deployment scenarios (e.g., nested and non-nested NEMOs, non-mobile and mobile capable nodes attached to the NEMO, etc). An additional requirement that current proposed mechanisms do not meet, is not to put any additional strong requisite on the operation of the nodes of the Mobile Network in order to be able to benefit from Route Optimisation.

This chapter describes a generic Route Optimisation solution for Network Mobility, designed in this PhD thesis, called Mobile IPv6 Route Optimisation for NEMO (MIRON) [BBC04], [BBCS05], [CBB+06]. MIRON is composed of two main modes:

- For those nodes of the mobile network that do not have any mobility capability, the Mobile Router (MR) performs all the Route Optimisation and mobility tasks on their behalf (what some authors [NZWT06] have called *Proxy MR*).
- For those nodes and (mobile) routers with standard Mobile IPv6 support, an address delegation mechanism, based on PANA (Protocol for Carrying Authentication for Network Access) [JLO+06] and DHCP [DBV+03], provides these nodes with topologically meaningful addresses (i.e. addresses that are directly reachable without requiring special rendezvous points, such as Home Agents, to be deployed to re-route any packet towards the actual location of the node). This enables these nodes to manage their own mobility and to perform the Route Optimisation by themselves.

These two different key modes of operation of MIRON combined give as a result a complete Route Optimisation solution for mobile networks, enabling traffic from any kind of node (with and without mobility support) and network configuration (including nesting) to be optimised. This is achieved without requiring changes on the operation of any node except Mobile Routers.

This chapter is organised as follows. An overview of the protocol is first provided in Section 5.2, before describing in detail how the proposed solution works. This description is presented next, divided into two sections, in order to deal with the Angular (Section 5.3) and Multi-angular (Section 5.4) Route Optimisation issues separately. A validation and evaluation of the protocol, taking into consideration security and scalability concerns, is provided in Section 5.5. In Section 5.6, the solution is compared with some existing RO proposals. After that, Section 5.7 explores an additional long term topic: the provision of Route Optimisation for NEMO by using secure delegation of signalling rights based approaches. Finally, some conclusions are provided in Section 5.8.

5.2. Protocol Overview

MIRON aims at improving the overall performance of communications involving nodes within a NEMO, by both avoiding data packets passing through the MR's HA and reducing the packet overhead due to the additional IPv6 headers introduced by the NEMO Basic Support protocol. MIRON does not introduce any change on the operation of the Correspondent Nodes and the Mobile Network Nodes, but only of the Mobile Routers.

Figure 5.1 shows a possible Route Optimisation target scenario for MIRON. It considers a mobile network deployed in a train, consisting of different types of MNNs:

- *Fixed nodes* in the train without mobility support (i.e. LFNs), such as internal servers or passengers' laptops.

- *Mobile devices* (i.e. VMNs), such as passengers' laptops, running Mobile IPv6, that keep using their Home IPv6 Addresses.

- Nested mobile networks, such as Personal Area Networks (PANs), e.g., a passenger's laptop, acts as a MR of his devices and is connected to the train's MR.

All of these devices access the Internet through the train's MR. This scenario includes almost every possible mobile network communication, involving LFNs, VMNs and nested NEMOs. Figure 5.1 also shows the different components every entity is composed of. Both the components and the way they work together to construct a complete Route Optimisation solution will be described in detail later in this chapter.

MIRON addresses two different Route Optimisation aspects:

- *Angular routing*. 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. MIRON addresses this problem in two different ways, depending on whether the MNN that is communicating with a CN has mobility support or not. If the MNN has no Mobile

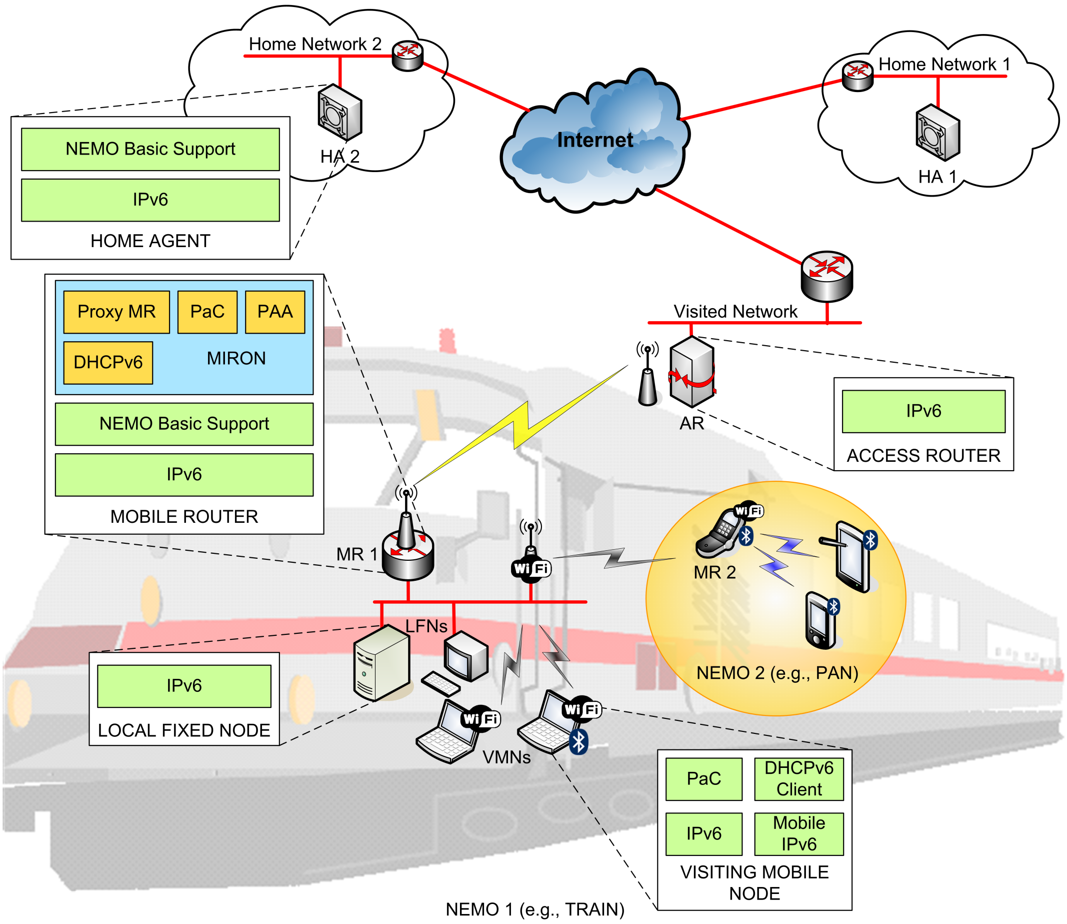


Figure 5.1: Overview of the MIRON architecture in a practical scenario.

IPv6 capabilities (i.e. an LFN), the approach followed by MIRON consists in delegating the Route Optimisation functionality to the MR, that performs all the RO signalling and packet handling on behalf of the LFNs. Therefore, the MR is a kind-of “Proxy MR” [NZWT06] for the LFNs of the NEMO. On the other hand, if the MNN is a Mobile IPv6 MN (i.e. a VMN) that is visiting the mobile network, MIRON takes advantage of the already available mobility support that the MN has. In this case, by using PANA and DHCPv6, the MR provides a topologically meaningful IPv6 address (that is, an address belonging to the network that the MR is visiting) to every VMN attached to the NEMO and updates it every time the NEMO moves. This, in addition to a routing mechanism that enables these addresses to be routed inside the NEMO, allows the VMN to make use of its own Mobile IPv6 Route Optimisation functionality, therefore avoiding traversing the MR’s HA and reducing the packet overhead.

- *Multi-angular routing*. Multi-angular routing is caused in nested NEMOs by the chain of nested MRHA bidirectional tunnels that packets should traverse. MIRON addresses this problem by using PANA and DHCPv6 to provide topologically meaningful IPv6 addresses to every MR in the nested NEMO hierarchy. In this way, every MR has an

IPv6 address belonging to the network that the root-MR (that is, the MR of the NEMO at the top of the hierarchy) is visiting. This, in addition to a routing mechanism that enables these addresses to be reachable, makes it possible to avoid traversing any HA.

The set of mechanisms of MIRON enables direct path communication between a MNN (LFN or VMN) and a CN, avoiding the suboptimal MR-HA path. The recursive tunnelling due to nesting is also eliminated, therefore optimising the traffic in every possible configuration of a mobile network. MIRON only introduces changes in the MR (see Figure 5.1), while MNNs, HAs and CNs remain unchanged, thus facilitating the deployment of the solution. The next two sections provide a detailed protocol walk-through of MIRON.

5.3. Angular Route Optimisation

If no Route Optimisation mechanism is used, all the traffic sent/directed to a MNN goes through the bidirectional tunnel set up between the MR and its HA. MIRON enables direct communication – without traversing the MR's HA – by following one of the next approaches, depending on the type of MNN:

- Local Fixed Node (LFN). LFNs do not have mobility support, so any mechanism that attempts to optimise their traffic should be implemented without requiring support from the LFN itself. The MIRON mechanism for LFNs is basically a proxy-MR approach, in which the MR performs the Mobile IPv6 Route Optimisation [JPA04] on behalf of the LFN.

- Visiting Mobile Node (VMN). VMNs are Mobile Nodes that are visiting the mobile network, managing their own mobility. By default, the Care-of Address obtained and used by a VMN attached to a NEMO belongs to the Mobile Network Prefix of that NEMO, so although these mobile nodes may be performing Route Optimisation with the CNs they are communicating to, there still exists a tunnel – between the NEMO's MR and the MR's HA – introduced by the NEMO Basic Support protocol. In this case, our proxy-MR approach is not feasible, therefore a different mechanism is used. MIRON takes advantage of the mobility support that VMNs already have. Basically, we propose a mechanism, using PANA and DHCPv6, that enables the VMNs to configure topologically valid IPv6 addresses (i.e. those addresses that belong to the address space of the foreign network the NEMO is visiting) as CoAs, and letting the VMNs manage their mobility and perform their Route Optimisation tasks.

5.3.1. Detection of the type of node

In order to apply the appropriate Route Optimisation mechanism, the MR should first be able to determine which kind of node (LFN or VMN) every node that is communicating is. The MR performs such a task by looking for Binding Update messages received at its ingress interfaces, since an MN right after gaining connectivity to a foreign network and configuring a new CoA (from the MNP), has to send a Binding Update to its HA to inform it about its new location (i.e. MN's CoA).

5.3.2. Route Optimisation mechanism for LFNs

Local Fixed Nodes are nodes without any mobility support running, therefore a mechanism that optimises their traffic cannot relay on any mobility function implemented by them. MIRON puts this LFN mobility support into the MR, that performs all the required mobility and Route Optimisation tasks on behalf of the LFNs attached to it.

The mechanism basically consists in enabling a MR to behave as a proxy for the LFN, performing the Mobile IPv6 Route Optimisation signalling and packet handling [JPA04] on behalf of the LFN. In order to do that, the MR first tracks the different communications that LFNs have established and decides which of those will be optimised, since optimising a traffic flow involves a cost – in terms of signalling and computation resources at the MR – that may not be worth for some kinds of flows (e.g., DNS queries). This decision (that is, whether to perform Route Optimisation for each flow or not) is out of the scope of this PhD thesis.

For those LFN-CN pairs whose traffic is to be optimised, the MR starts to send the RO signalling described for standard Mobile IPv6 in [JPA04]:

- The BU is sent by the MR.
- The BU contains the LFN's address as the Home Address (HoA) and the MR's CoA as the CoA (since the MR's CoA is the only topologically meaningful address available).

The Route Optimisation mechanism defined by Mobile IPv6 [JPA04] requires an additional procedure to be performed before sending the BU message, in order to mitigate possible attacks [NAA+05]. Basically, this mechanism, called Return Routability (RR), verifies that the node that is reachable at the HoA is able to respond to packets sent to a given CoA (different to the HoA of the node). This mechanism can be deceived only if the routing infrastructure is compromised or if there is an attacker between the verifier and the addresses (that is, HoA and CoA) to be verified. With these exceptions, the test is used to ensure that the MN's Home Address (HoA) and MN's Care-of Address (CoA) are collocated.

In our solution we adopt the procedure described above. For this purpose, the MR has to perform the Mobile IPv6 Return Routability procedure [JPA04] on behalf of the LFN. Such a procedure involves sending the Home Test Init (HoTI) and Care-of Test Init (CoTI) messages to the CN and processing the replies (Home Test message – HoT – and Care-of Test message – CoT). These messages are sent as specified in [JPA04], using the LFN's address as the source address in the HoTI message – which is sent encapsulated through the MR's HA –, and the MR's CoA as the source address in the CoTI message. With the information contained in the HoT and CoT messages, sent by the CN in response to the HoTI and CoTI messages respectively, the MR is able to build a BU message to be sent to the CN on behalf of the LFN. This message is sent using the MR's CoA as the packet source address and carries a Home Address destination option set to the LFN's address.

Besides performing the Route Optimisation signalling on behalf of the LFN, the MR has to process the packets sent by and directed to the LFN. Packets sent by the CN follow a direct path to the MR, not traversing the HA, as a result of the Route Optimisation. These packets carry the MR's CoA as destination address, and also carry a Type 2 Routing Header with the LFN's address as next hop. The MR processes and removes the Routing Header of the packet, checking if the next hop address belongs to one of its LFNs and, if so, delivering

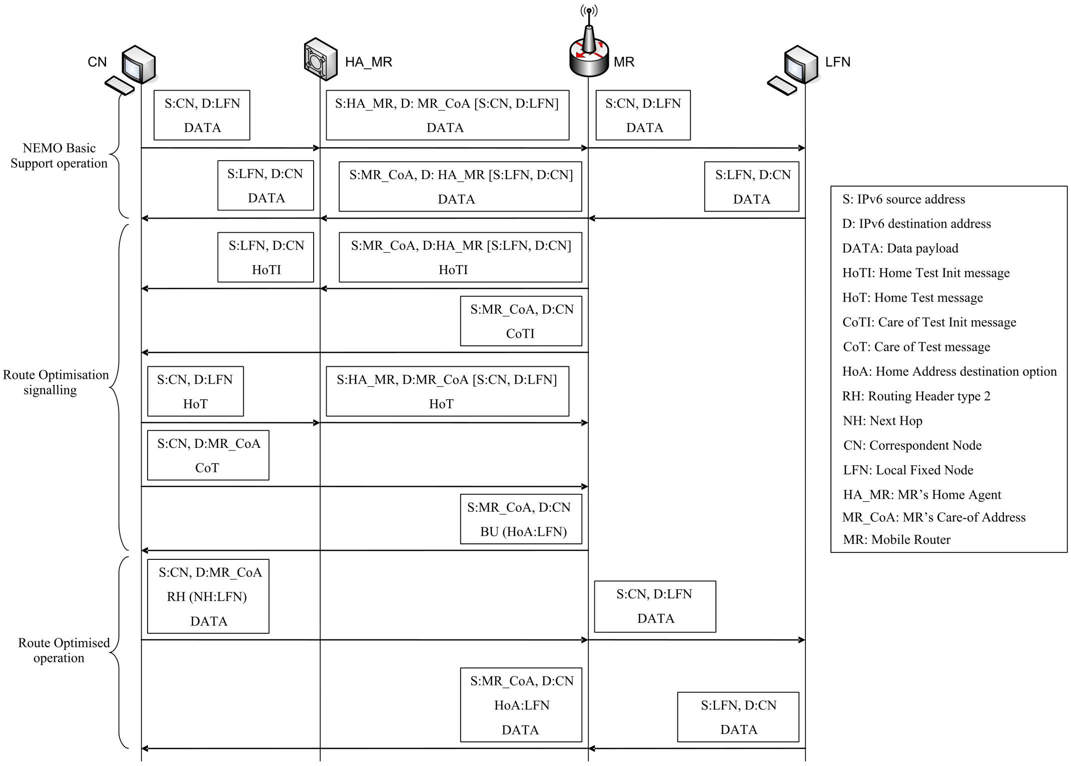

CN
HA_MR
MR
LFN
NEMO Basic Support operation
S:CN, D:LFN DATA
S:HA_MR, D: MR_CoA [S:CN, D:LFN] DATA
S:CN, D:LFN DATA
S:LFN, D:CN DATA
S:MR_CoA, D: HA_MR [S:LFN, D:CN] DATA
S:LFN, D:CN DATA
Route Optimisation signalling
S:LFN, D:CN HoTI
S:MR_CoA, D:HA_MR [S:LFN, D:CN] HoTI
S:MR_CoA, D:CN CoTI
S:CN, D:LFN HoT
S:HA_MR, D:MR_CoA [S:CN, D:LFN] HoT
S:CN, D:MR_CoA CoT
S:MR_CoA, D:CN BU (HoA:LFN)
Route Optimised operation
S:CN, D:MR_CoA RH (NH:LFN) DATA
S:CN, D:LFN DATA
S:MR_CoA, D:CN HoA:LFN DATA
S:LFN, D:CN DATA
S: IPv6 source address
D: IPv6 destination address
DATA: Data payload
HoTI: Home Test Init message
HoT: Home Test message
CoTI: Care of Test Init message
CoT: Care of Test message
HoA: Home Address destination option
RH: Routing Header type 2
NH: Next Hop
CN: Correspondent Node
LFN: Local Fixed Node
HA_MR: MR's Home Agent
MR_CoA: MR's Care-of Address
MR: Mobile Router

Figure 5.2: Route Optimisation mechanism for LFNs: Proxy-MR operation.

the packet to the LFN. Current Mobile IPv6 specification [JPA04] defines that IPv6 nodes which process a Type 2 Routing Header must verify that the address contained within is the node's own Home Address. This is done in order to prevent packets from being forwarded outside the node. In MIRON this has been changed and the MR verifies that the address contained in the Routing Header is the address of one of the LFNs that the MR is acting as Proxy-MR. In the opposite direction, the MR receives the packets sent by the LFN and performs the following actions on every packet:

- Set the MR's CoA as IPv6 source address.

- Insert an IPv6 Home Address destination option, carrying the address of the LFN.

Figure 5.2 shows the signalling and data flows of the proposed Route Optimisation mechanism for LFNs, including at the top of the figure the NEMO Basic Support protocol data flow for comparison purposes.

5.3.3. Route Optimisation mechanism for VMNs

Visiting Mobile Nodes are nodes that support mobility (that is, nodes running Mobile IPv6 [JPA04]) and are visiting a mobile network. Therefore the VMN is attached to an Access Router that is the NEMO's MR, and the address that the VMN obtains and configures as CoA belongs to the Mobile Network Prefix. In this case, our proxy-MR mechanism used for LFNs cannot be used, as the VMN itself may generate Route Optimisation signalling with its CNs. Besides, the MR cannot modify the RR and RO signalling sent by the VMN in order to make the MR's CoA the CoA that the CN uses to send the packets to the VMN, because part of the RR signalling is protected by IPsec (the HoTI message is sent through the VMN's HA protected by IPsec ESP).

In this thesis, two different approaches were explored to provide VMNs with Route Optimisation, although only one was finally adopted by MIRON. The first mechanism is based on linked Mobile IPv6 Binding Cache entries, while the second is based on the use of PANA and DHCPv6 to provide topologically meaningful IPv6 addresses to VMNs. A detailed description of these two mechanisms is included next.

5.3.3.1. Linked Mobile IPv6 Binding Cache Entries

As we have previously explained, a MR cannot modify the Route Optimisation signalling generated by an attached VMN in order to make the MR's CoA be the address that the CN uses as the VMN's CoA. However, Mobile IPv6 specification [JPA04] does not prevent from having linked Binding Cache (BC) entries (as long as a circular reference – a loop – is not created). A linked BC entry exists when the Care-of Address of an entry appears as the Home Address of a different entry.

A VMN attached to a NEMO configures a CoA that belongs to the Mobile Network Prefix of the moving network. This CoA is used by the VMN in the Home Registration to its HA, but also in the Route Optimisation signalling sent to its CNs. Therefore, a CN communicating with a VMN performing RO, would have an entry in its BC as follows:

Home Address	Care-of Address
VMN's HoA	VMN's CoA ($\in$ MNP)

A MR may help a VMN by sending Binding Updates to the CN on its behalf. This BUs would bind the VMN's CoA to the MR's CoA, so an additional entry would be added to the CN's BC:

Home Address	Care-of Address
VMN's HoA	VMN's CoA ($\in$ MNP)
VMN's CoA ($\in$ MNP)	MR's CoA

The Mobile IPv6 specification (RFC 3775 [JPA04]) does not clearly define what should be the behaviour of a CN with linked BC entries (such as the previous one) when it has to send a packet to VMN's HoA. The logical processing would be to the following:

- The CN examines its Binding Cache for an entry for the destination address (VMN's HoA) to which the packet is being sent. Since the CN has a BC entry for this address, it adds a type 2 Routing Header to route the packet to the VMN (the destination node) by way of its Care-of Address (that is, the destination address of the packet is set to the VMN's CoA).

- The CN examines again its BC for an entry for the new destination address (VMN's CoA) to which the packet is now being sent. Again, the CN has a BC entry for this

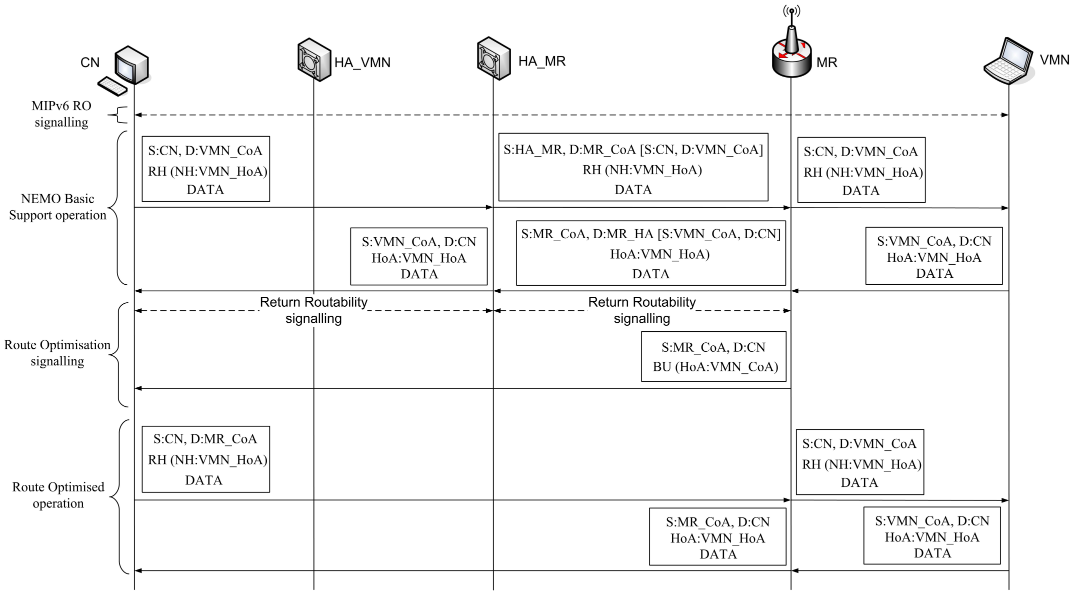

CN
HA_VMN
HA_MR
MR
VMN
MIPv6 RO signalling
NEMO Basic Support operation
S:CN, D:VMN_CoA RH (NH:VMN_HoA) DATA
S:HA_MR, D:MR_CoA [S:CN, D:VMN_CoA] RH (NH:VMN_HoA) DATA
S:CN, D:VMN_CoA RH (NH:VMN_HoA) DATA
S:VMN_CoA, D:CN HoA:VMN_HoA DATA
S:MR_CoA, D:MR_HA [S:VMN_CoA, D:CN] HoA:VMN_HoA) DATA
S:VMN_CoA, D:CN HoA:VMN_HoA DATA
Return Routability signalling
Return Routability signalling
Route Optimisation signalling
S:MR_CoA, D:CN BU (HoA:VMN_CoA)
Route Optimised operation
S:CN, D:MR_CoA RH (NH:VMN_HoA) DATA
S:CN, D:VMN_CoA RH (NH:VMN_HoA) DATA
S:MR_CoA, D:CN HoA:VMN_HoA DATA
S:VMN_CoA, D:CN HoA:VMN_HoA DATA

Figure 5.3: Route Optimisation mechanism for VMNs: Linked Mobile IPv6 Binding Cache Entries.

address, so it adds a new type 2 Routing Header to the packet, and sets the destination address to the Care-of Address of this BC entry (i.e. MR's CoA).

However, IPv6 specification (RFC 2460 [DH98]) states that a Extension Header (such a Routing Header) can occur at most once in a packet (except for the Destination Options Header, that can occur at most twice). Besides, RFC 3775 [JPA04] restricts the type 2 Routing Header to carry only one address, so the above behaviour cannot happen.

On the other hand, it is not clear what a Correspondent Node Mobile IPv6 implementation would do if it receives Binding Updates that creates linked BC entries. A Mobile Router would still benefit from sending a BU, binding the VMN's CoA to the MR's CoA, if the CN performed the following processing when sending a packet:

- The CN examines its Binding Cache for an entry for the destination address (VMN's HoA) to which the packet is being sent. Since the CN node has a BC entry for this address, it adds a type 2 Routing Header to route the packet to the VMN (the destination node) by way of its Care-of Address (that is, the destination address of the packet is set to the VMN's CoA).

- The CN examines again its BC for an entry for the new destination address (VMN's CoA) to which the packet is now being sent. The CN has a BC entry for this address, and it sets the destination address of the packet to the Care-of Address of the last BC linked entry (i.e. MR's CoA).

If a CN behaved like described above, a MR would be able to enable direct path communication between a CN and an attached VMN by performing the following operations (see Figure 5.3):

- Once the MR has detected that a VMN has attached to the NEMO, and that it is doing Route Optimisation with a CN, the MR sends a BU to the CN binding the VMN's CoA (that belongs to the NEMO's MNP) and the MR's CoA. This BU creates a linked BC entry in the CN.

- The MR processes packets sent by the CN to the VMN, since the CN – because of the linked BC entry – now is sending packets to the VMN with the MR's CoA as destination address. The MR replaces this destination IPv6 address with the VMN's CoA.

- The MR processes packets in the reverse direction as well (that is, packets sent by the VMN to the CN), replacing the source IPv6 address with the MR's CoA (the VMN originally sets it to the VMN's CoA).

Although this Route Optimisation mechanism is allowed by current Mobile IPv6 specification (RFC 3775 [JPA04]), a crucial point was to check how existing MIPv6 implementations behaved about linked BC entries. This was the next step after designing the mechanism presented above (that was actually a natural extension of the Proxy-MR operation defined for the RO support of LFN communications). In order to investigate the operation of MIPv6 CN implementations, MIPL[1] was chosen as a candidate for analysis, because it is one of the most used available MIPv6 implementation. MIPL is an open source implementation of Mobile IPv6 fully compliant with RFC 3775 [JPA04]. It was checked whether a CN running MIPL 2.0 RC2 would support our mechanism, and the result was that it was not possible without modification of MIPL (although it would be possible to easily modify it to support linked BC entries).

Based on our analysis of a representative Mobile IPv6 implementation, it seems that linked BC are not well supported by existing MIPv6 implementations, which means that a modification of CNs would be required to enable our proposed mechanism to work. Therefore, we decided to seek for a different approach to address our requirement of enabling NEMO RO for VMNs. The mechanism that we finally designed and adopted is described in the next section.

5.3.3.2. PANA-based Address Delegation

The Route Optimisation approach that MIRON defines for Visiting Mobile Nodes attached to a NEMO is based on taking advantage of the mobility support that these nodes already have, providing the means to the VMN to perform the RO. In order to allow the VMN to manage its own mobility and enable it to perform Route Optimisation with the CNs (in a way that avoids the MRHA bidirectional tunnel), we propose the following:

- Provide a topologically meaningful IPv6 address to the VMN. These addresses are those that belong to the network that the root-MR is visiting.

- Enable this address to be routable inside the NEMO, as it only has topological meaning in the visited network. The MR has to perform proxy neighbour discovery for this

[1] Mobile IPv6 for Linux `http://www,mobile-ipv6.org/`

address in the egress interface that is attached to the network to which the address belongs. Besides, the MR has to insert a host route for this address to be able to route packets destined to it.

- Perform source address routing in the MR in order to send directly (that is, avoiding the bidirectional MR-HA tunnel that still exists and is used for non-optimised traffic) packets sent by the VMN.

- Update the address of the VMN when the NEMO moves.

A mechanism that fulfils the previous goals should be able to allow VMNs, and only the VMNs – the mechanism must not affect other type of nodes –, to obtain a new IPv6 address to be used as the CoA, whenever the MR wants to, and in a secure way that does not introduce any new security threat.

The Route Optimisation mechanism for VMNs that we propose in this section uses a particular functionality that is included in the PANA protocol[2], namely, the capability of telling a node that it must change its IPv6 address and how to get a new one.

This imposes the requirement that PANA client (PaC) software must be available in VMNs for providing them Route Optimisation, and PaC and PANA agent (PAA) software must be available in MRs. The PaC software in the MRs is needed to optimise nested NEMOs as it will be described in the next section. The PAA software in MRs is needed to support the Route Optimisation for VMNs visiting the NEMO, and to support the Route Optimisation of nested NEMOs. PANA support is not required by MIRON in the access network that the root-MR is visiting (in the infrastructure access network) nor in the LFNs attached to the NEMO.

The assumption of availability of PANA software in the MRs is not a problem, because MIRON is based on modifications in the MRs software, PANA is just an additional software to have. The assumption of PANA in VMNs can be more restrictive. The idea of the solution is that MIPv6 compliant Mobile Nodes can visit the NEMO and optimise its routing just like when they visit an infrastructure access network. This will not be true if they do not have a PANA client installed.

Most of current access networks (such as hotspots deployed in airports and cafeterias) require users to authenticate to the network before gaining Internet access. As the number of hotspots continues growing in the coming years, authentication mechanisms will be more and more important in order to avoid non-authorised users using and wasting the network resources. Using a standard protocol to perform such authorisation and authentication tasks would help in the deployment of ubiquitous access "anytime anywhere" networks. Our Route Optimisation protocol, MIRON, assumes that (i) an authentication protocol will be used in public heterogeneous access networks and that (ii) PANA [YOP$^+$05], [JLO$^+$06], [FOP$^+$06] will be a standard protocol widely deployed and used, so PANA support will be available in VMNs.

We argue that assuming that VMNs will have PaC software does not limit the practical usability of MIRON for Route Optimisation in VMNs, since, on one hand, it is not realistic to assume public access networks to be open and not to require any kind of authentication. On the other hand, we assume that PANA support will be available on VMN, because it is

[2] A brief summary of PANA is provided in Appendix A.

expected that PANA will become a standard authentication protocol once its specification is concluded within the IETF, finishing with the current status of multiple possible authentication mechanisms (e.g., IEEE 802.1X, proprietary web-based systems, etc).

Even if that is not finally the case, and PANA does not turn to be the standard authentication protocol in heterogeneous networks, a different protocol that is able to provide IPv6 routable addresses to arriving VMNs and change them every time the NEMO moves, could be alternatively used. One example could be the use of the DHCPv6 *Reconfigure* mechanism [DBV$^+$03], using some authentication information between MR and VMN obtained from any other means to authorise the MR changing the IPv6 address used by the VMN.

Anyway, if neither PANA nor an alternative protocol is available in a VMN, this VMN – attached to a MIRON MR – will just not benefit from the Route Optimisation mechanism provided by MIRON, and its traffic will follow the suboptimal path provided by the NEMO Basic Support protocol.

The mechanism to provide an IPv6 address to the VMN using PANA works as follows (see Figure 5.4): when a VMN attaches to a NEMO, it initiates the PANA session (PANA discovery and handshake phases). Immediately after that, the actual authentication and authorisation phase (by executing EAP between the PAA and PaC) takes place. Then, the VMN is authorised to access the network and it has an IPv6 address. This address is obtained by using the address autoconfiguration mechanism available at the NEMO. Initially, we assume that we are using stateless address configuration for addresses of the Mobile Network Prefix, but later we will see that we can also use stateful address configuration within the NEMO. The VMN then sends a Binding Update message to its Home Agent, informing about its current location. Once this BU is received at the MR, it becomes aware that a new VMN is now attached to the NEMO. The MR discards this BU message and starts a PANA re-authentication phase.

During the PANA re-authentication phase, the PAA located in the MR tells the PaC located in the VMN that it should obtain and configure a new IPv6 address (Post-PANA address, POPA) and how to obtain it, by including available configuration methods in a Post-PANA-Address-Configuration (PPAC) AVP contained in a PANA message (PANA-Bind-Request). DHCPv6 is the only available configuration mechanism listed in the message, and upon the reception of that, the VMN requests an address using DHCPv6. There is a DHCPv6 component located at the MR that receives the DHCPv6 requests from the VMN and then obtains (using one of the available autoconfiguration mechanisms at the foreign network) an IPv6 address. The DHCPv6 component generates a DHCPv6 reply – including this address – that is delivered to the requesting VMN. This DHCPv6 component implements the client part of DHCPv6 and also some reduced functionalities of the server part (e.g., the generation of DHCPv6 responses), but it is not a DHCPv6 server (for example, the DHCPv6 component does not have a pool of available addresses, each time an address is needed, it obtains it from the foreign network), although the implementation of this DHCPv6 component can be performed very easily from the code of a normal DHCPv6 client and server implementation. Once the MR has sent the DHCPv6 reply – including the (/128) delegated address – to the VMN, the PaC in the VMN conveys this newly configured IPv6 address to the PAA in the MR by sending the PANA-Update-Request message.

The use of stateful address configuration (DHCPv6) within the NEMO (to configure addresses from the MNP) is also possible, but it requires the DHCPv6 component at the MR

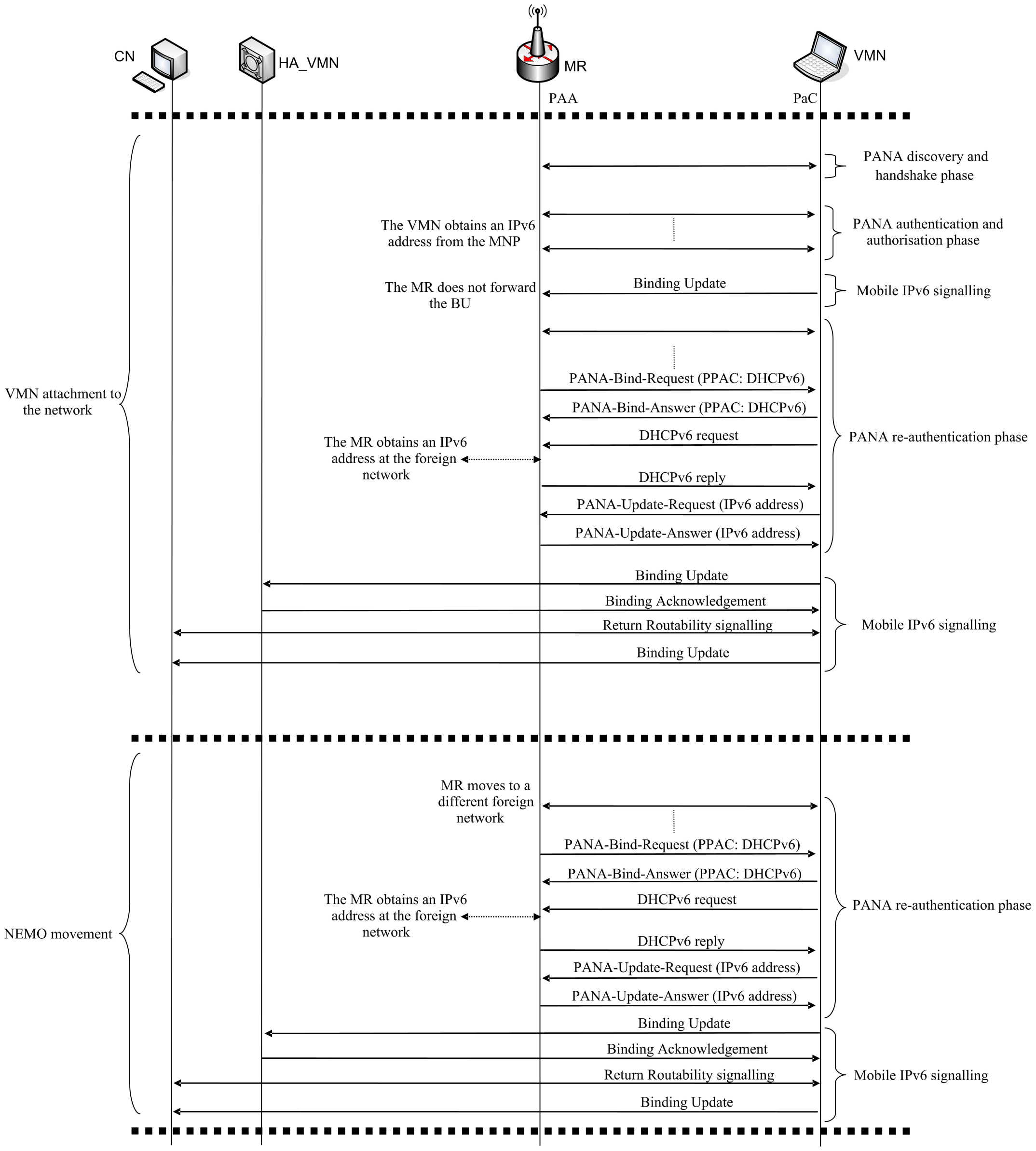

CN
HA_VMN
MR
PAA
VMN
PaC
PANA discovery and handshake phase
The VMN obtains an IPv6 address from the MNP
PANA authentication and authorisation phase
The MR does not forward the BU
Binding Update
Mobile IPv6 signalling
VMN attachment to the network
PANA-Bind-Request (PPAC: DHCPv6)
PANA-Bind-Answer (PPAC: DHCPv6)
DHCPv6 request
The MR obtains an IPv6 address at the foreign network
PANA re-authentication phase
DHCPv6 reply
PANA-Update-Request (IPv6 address)
PANA-Update-Answer (IPv6 address)
Binding Update
Binding Acknowledgement
Return Routability signalling
Mobile IPv6 signalling
Binding Update
MR moves to a different foreign network
PANA-Bind-Request (PPAC: DHCPv6)
PANA-Bind-Answer (PPAC: DHCPv6)
DHCPv6 request
The MR obtains an IPv6 address at the foreign network
PANA re-authentication phase
NEMO movement
DHCPv6 reply
PANA-Update-Request (IPv6 address)
PANA-Update-Answer (IPv6 address)
Binding Update
Binding Acknowledgement
Return Routability signalling
Mobile IPv6 signalling
Binding Update

Figure 5.4: Route Optimisation mechanism for VMNs.

to implement the complete server functionality and to check, before providing an address, whether or not the requesting node is an identified VMN, to know if this address should belong to the MNP or to the visited network address space. Nodes are identified as VMNs by the MR according to the procedure described above.

In order to enable the VMNs' addresses reachability inside the NEMO, the MR has to add a host route for each VMN's address and perform proxy neighbour discovery on its egress interface (the interface that is connected to the link where the address has topological meaning), allowing the MR to forward packets to their final destinations. Both the delegated IPv6 addresses and the host routes have a lifetime that prevents this state to remain in the network after a sub-NEMO or a node leaves a parent-NEMO (the value depends on the lifetime of the address obtained by the root-MR).

The VMN, triggered by the change of address, starts the Mobile IPv6 location update process, sending first a Binding Update (BU) message to its HA. The VMN may then update the location information in the CNs it is communicating with (if the VMN is running Route Optimisation with its CNs). This process consists of the VMN performing the Return Routability process [JPA04] and sending a BU to every CN whose traffic is to be route optimised.

When the NEMO moves to a different foreign network, the MR requests new IPv6 addresses and provides them to the VMNs attached to the NEMO by starting a new PANA re-authentication phase. The MR requests VMNs to configure a new IPv6 address using DHCPv6.

Due to the PANA and DHCPv6 signalling, MIRON takes much longer to finish its handover than the NEMO Basic Support. Similarly to the case of Mobile IPv6, micromobility solutions such as Fast Handovers for Mobile IPv6 [Koo05], may be designed/adapted to MIRON to alleviate the increase in the handover delay [BSM$^+$05].

5.4. Multi-angular Route Optimisation

The routing inefficiencies due to the MRHA bidirectional tunnel are exacerbated when NEMOs are attached to other NEMOs, forming a nested NEMO. Packets belonging to a communication between a MNN of a nested NEMO and a CN have an additional IPv6 header per nesting level and traverse the HAs of every MR of the nested NEMO.

The problem of enabling RO for nested NEMOs (i.e. MRs visiting a NEMO) is very similar to that of VMNs (i.e. MNs visiting a NEMO). Both VMNs and MRs are nodes that are mobile-capable and can manage their own mobility. Routing inefficiencies arise from the fact of not using topologically meaningful addresses (i.e. addresses belonging to the NEMO MNP) as CoAs. Section 5.3.3 describes an address delegation mechanism with a built-in routing system that is able to provide IPv6 addresses – belonging to the foreign network that the MR is visiting – to a VMN in a secure way, by using PANA facilities.

MIRON extends that solution, used for providing Angular RO for VMNs, to enable Multi-angular RO in nested NEMOs. Basically, the solution consists in providing topologically meaningful addresses – that is, those that belong to the foreign network that the root-MR is visiting – to every MR in the nested NEMO. The same PANA-with-DHCPv6-based mechanism is used to provide an IPv6 address to a MR that attaches to a NEMO (and to change it when one of the parent NEMOs moves). MRs have both a PAA and a PaC component and also a DHCPv6 component, so when a MR connects to a mobile network, they are able to get and configure a new IPv6 address.

Providing topologically meaningful addresses is not the only required step to avoid the suboptimal multi angular routing in nested networks. Another requirement that has to be met is that these addresses are globally reachable. To enable that, every MR in the nested NEMO keeps track of the address of the node requesting an IPv6 address using DHCPv6, so when the delegated address is received, it can insert a host route entry in its routing table that allows it to route packets destined to that address afterwards. This information is also used to perform source address based routing for the packets generated inside the NEMO, as every

MR should know for each packet if it has to be sent directly to the router it is connected to (in this way, avoiding the tunnel), or it has to be sent towards the HA, through the bidirectional tunnel (for traffic that is not being optimised).

This address delegation mechanism with built-in routing avoids the multi encapsulation and multi angular routing in nested networks. Besides, it enables angular MIRON route optimisations to work when applied to a NEMO located at any level of a nested NEMO.

5.5. Validation and evaluation of the proposed solution

This section provides both an experimental and analytical evaluation of MIRON. The main aim of this evaluation is to study the performance of MIRON and compare it with the NEMO Basic Support protocol. A security and scalability analysis is also provided, in order to demonstrate that the designed mechanism has no critical security or scalability issues that may have an impact on the deployment of the solution.

5.5.1. Experimental evaluation

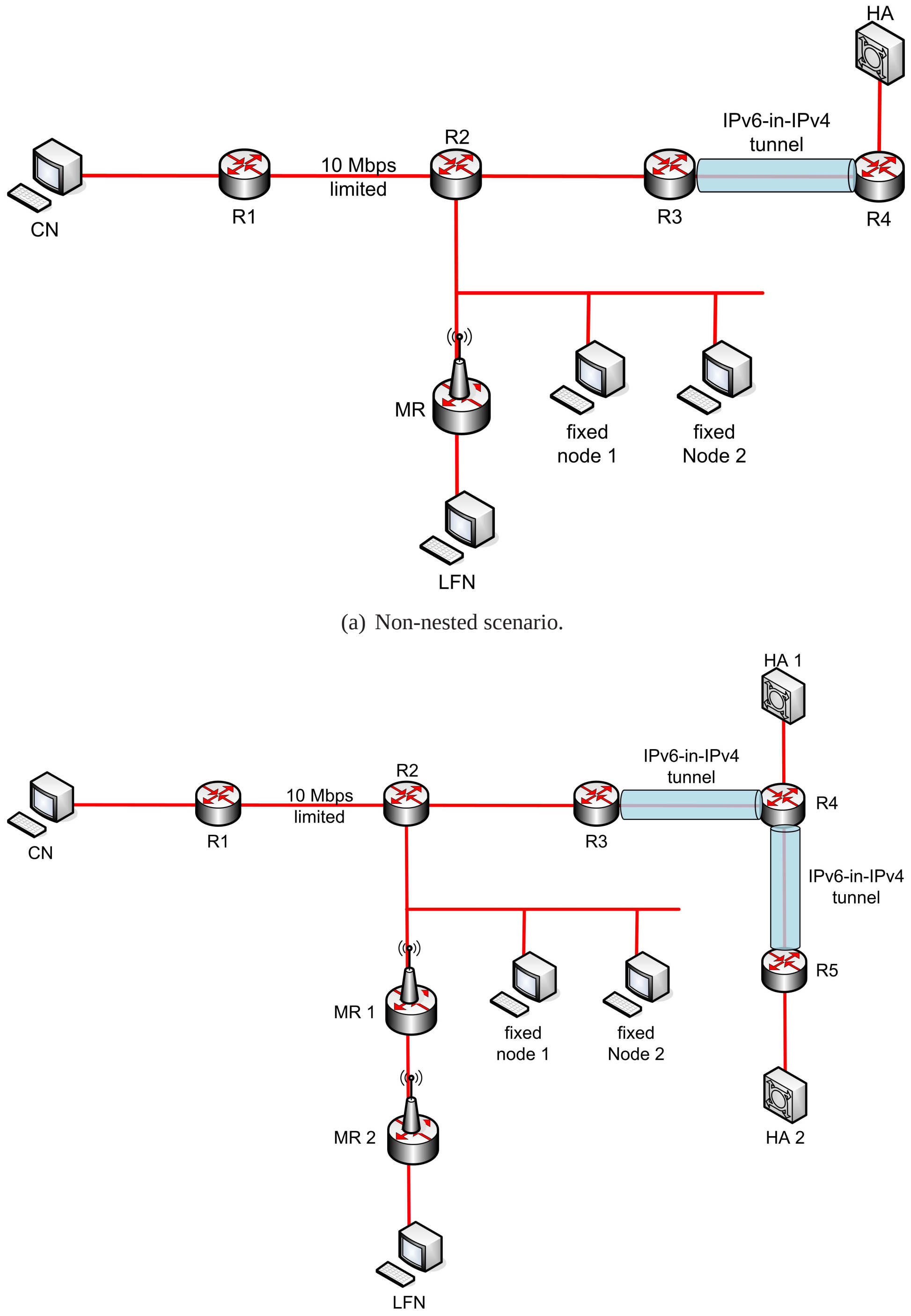
5.5.1.1. MIRON implementation

In order to be able to conduct real experiments that allowed us to evaluate the performance of the NEMO Basic Support protocol and the improvements provided by MIRON, we first implemented the NEMO Basic Support protocol [dlOBC06]. A first prototype of MIRON was also implemented, providing all the Route Optimisation mechanisms [BOC$^+$06].

Packets belonging to a communication flow optimised by MIRON must not traverse the bidirectional tunnel. Therefore, for outgoing traffic, a host route towards the CN of the flow should be inserted at the MR, to avoid the default route through the tunnel interface. Besides, there may be simultaneously communications in a NEMO – from different MNNs – with the same destination CN that are not all being optimised, thus source address based routing is necessary.

The required additional protocols and procedures (such as the Return Routability and DHCPv6) were completely implemented, with the exception of PANA, that is currently being implemented and integrated. The fact that PANA is not implemented does not have an impact on the results obtained in the tests, as we have focused on the TCP throughput, and the PANA signalling is generated during handovers (and also periodically to renew the lifetime). In this PhD thesis, we have not been concerned about the performance of our solution during handovers as we address the problem of Route Optimisation, just in the same way that the Route Optimisation solution for Mobile IPv6 does. Improvements in the handover latency (like the ones designed for Mobile IPv6 [Koo05], [SCMB05], [BSM$^+$05]) requires further study and will be addressed in future works.

The NEMO Basic Support protocol [dlOBC06] and MIRON were mostly implemented in user space, because in this way the development was easier and quicker than doing that in the kernel. The main software characteristics are: a Linux machine with kernel linux-2.6.x (tested with linux-2.6.8.1) with support for IPv6-in-IPv6 tunnels (used for the MRHA bidirectional tunnel) and Netlink sockets, and the *pcap* library (used for the capture and processing of the mobility related signalling).



(a) Non-nested scenario.

(b) Nested scenario.

Figure 5.5: Network mobility testbed employed during the experimental evaluation.

5.5.1.2. Studied scenarios

Two different scenarios (Figure 5.5) were deployed to allow us to experimentally test the performance of MIRON and compare it with the NEMO Basic Support solution. The first one (Figure 5.5(a)) was used to evaluate the performance in a non-nested case, whereas the second (Figure 5.5(b)) is an extension of the former to include nesting.

Next, we describe the second scenario, as it is an extension of the first one. This scenario (Figure 5.5(b)) consists of thirteen Mandrake 10.0 Linux machines (all with linux-2.6.8.1 kernels, except 3 routers that run linux-2.4.22). Five of them act as *fixed* (i.e. non-mobile) routers (R1 to R5), two as Home Agents (HA1 and HA2), two as Mobile Routers (MR1 and MR2), one as Correspondent Node (CN), one as Local Fixed Node (LFN) and two as *fixed* nodes (Fixed nodes 1 and 2). This is part of the IST Daidalos[3] project testbed at the Universidad Carlos III de Madrid.

All mobility-aware nodes run network mobility software, that is, the NEMO Basic Support protocol (at the HA and MR) and MIRON (at the MR only) developed by us. The CN runs MIPL 2.0 RC2, with the support of Route Optimisation enabled.

We need to be able to modify the delay in the path followed by packets of a communication between a CN and a MNN (that is, the path between the CN and the MNN's HA and/or the path between the MNN's HA and the foreign network the MR is currently attached to). This allows us evaluate how the performance of a particular network mobility solution is affected by network characteristics, such as the particular location of mobile networks, home networks and correspondent nodes. For this purpose, we used the NIST Net emulator[4]. NIST Net allows a single Linux PC, set up as a router, to emulate a wide variety of network conditions (e.g., latency, jitter, packet loss, . . .).

We were interested in studying how the delay (and also the packet overhead) introduced by the MRHA bidirectional tunnel affects the performance of applications. TCP performance is heavily dependent on the round trip time (RTT) between the communication peers. Taking this into consideration and the fact that 85% of the traffic in the Internet is generated by TCP connections [MC00b], the TCP study case becomes very interesting to be performed and analysed. Therefore, we set up an scenario that allowed us to modify the delay in the CN-HA-MR path.

Other network characteristics, besides the delay, that do not have an special effect in the TCP performance and that are also present in non-mobile networks, were not modified.

NIST Net software runs only in IPv4 and with linux-2.4.x kernels (at the moment we performed these tests). Therefore, in order to use it in our testbed, we had to set up an IPv6-in-IPv4 tunnel – between R3 and R4 and between R3 and R5 – using it in our IPv6 scenario. In the first scenario, the non-nested one (Figure 5.5(a)), every packet in the CN-HA-MR path traverses the IPv6-in-IPv4 tunnel, which allows us to modify the network behaviour by changing the parameters of the NIST Net emulator running in R3 and R4. In the rest of the path followed by packets, native IPv6 is used, so the tunnel inclusion does not affect the overall test performance except for the small added delay due to IPv6-in-IPv4 tunnelling and the reduction of the PMTU (the situation is not different from having a change of the transport link technology in the path and it is transparent to the IPv6 behaviour). Actually, the IPv4 tunnel clearly shows the current status of IPv6 networks in the Internet, with lot of IPv4 clouds connecting IPv6 native networks. In the nested scenario, a second IPv6-in-IPv4 tunnel was set up – between R4 and R5 – to allow us to modify the network delay between the two different home networks (i.e. between HA1 and HA2).

[3] `http://www.ist-daidalos.org/`

[4] `http://www-x.antd.nist.gov/nistnet/`

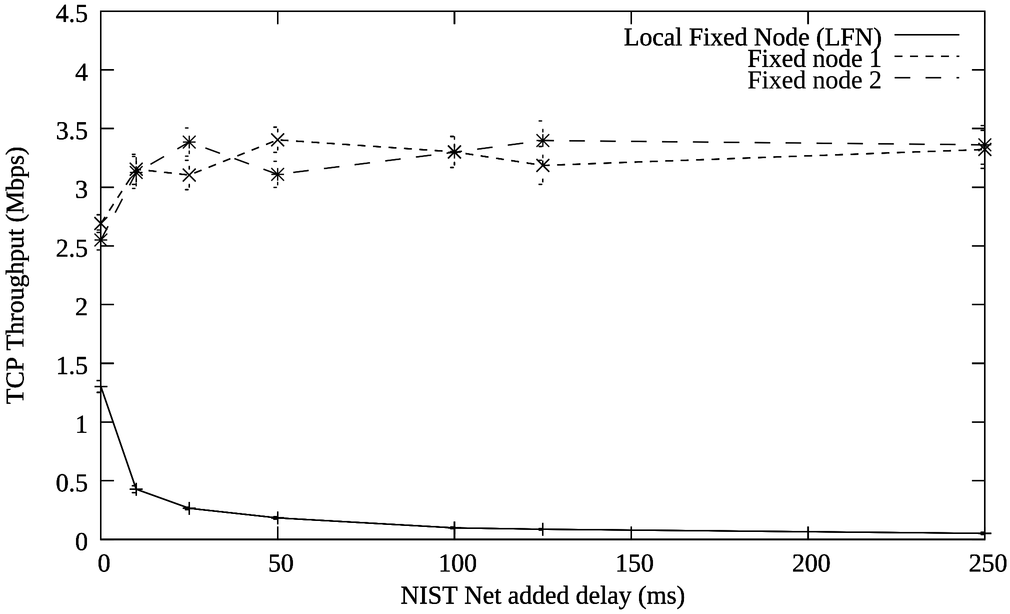


Figure 5.6: Impact of NEMO Basic Support protocol on the TCP throughput.

To avoid the influence of the wireless media characteristics and interferences from other neighbouring wireless networks, the performance tests were conducted using wired mobile routers, although experiments using wireless mobile networks were also performed to check the correctness of our solution.

5.5.1.3. Impact of network mobility on the TCP performance

The suboptimal routing introduced by the NEMO Basic Support protocol [DWPT05] makes packets not follow the direct CN-MR-MNN path, but the usually longer CN-HA-MR-MNN path. This adds a delay in the packet delivery that can significantly reduce the performance of certain applications. Furthermore, packets are encapsulated between the HA and the MR, thus reducing the PMTU. Both effects, increased delay and reduced PMTU, have an impact in the performance of applications.

The test consists in measuring the average TCP throughput of an MNN (an LFN in the tests) downloading a file from a CN, while two other non-mobile network hosts (Fixed nodes 1 and 2), attached to the same network the NEMO is visiting, simultaneously download the same file, both in a non-nested and in a nested scenario (see Figures 5.5(a) and 5.5(b)). The available bandwidth between the CN and the network that the mobile network is visiting was limited to 10 Mbps, by setting the R1-R2 link to 10 Mbps Half-Duplex. The tool used for the download was *scp* (secure copy) and the size of the file was 50 MBytes.

Each average TCP throughput sample was calculated over a 20 seconds independent interval of download and at least 30 samples were obtained for each test (to guarantee the statistical validity of the measurements).

For the non-nested scenario, the unidirectional NIST Net added delay of the link R3-R4 – *delay1* – was varied between 0ms (i.e. home network, visited network and CN locate very

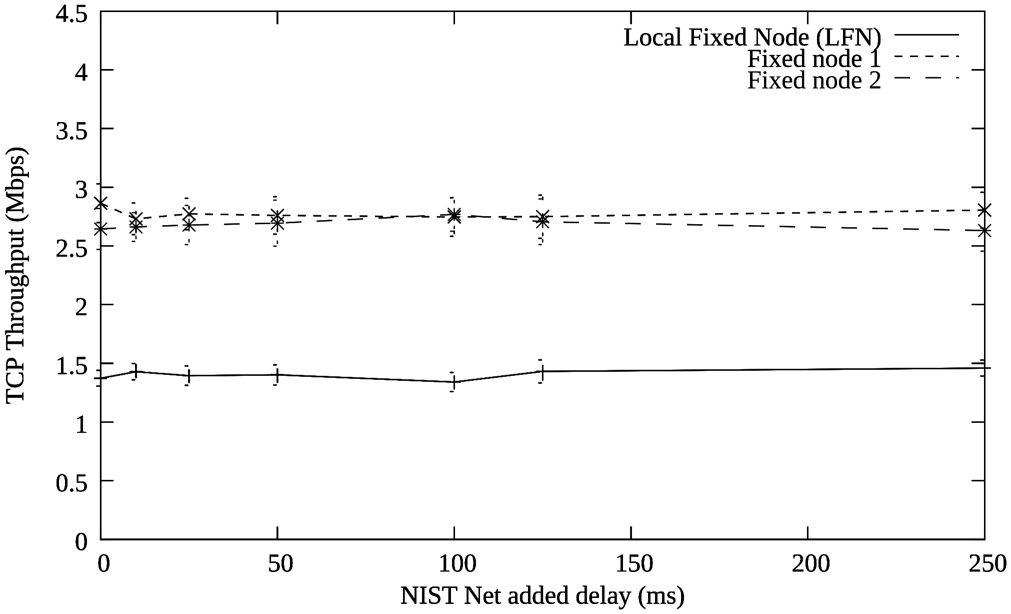


Figure 5.7: Impact of MIRON on the TCP throughput.

close each other) and 250ms (this value represents a high, but still common RTT value of 500ms in the Internet nowadays). *Delay1* is part of the CN-HA and HA-MR delays, thus affects the overall delay in the CN-HA-MR-LFN path followed by packets of the CN-LFN communication. Results for the case of using the NEMO Basic Support protocol are shown in Figure 5.6. Results for the case of using MIRON are shown in Figure 5.7. Confidence limits (95%) are also shown in both figures.

When the NEMO Basic Support protocol is used, the effect of a higher value of *delay1* in the performance of TCP application is clear: the effective throughput decreases as the delay increases (Fig 5.6). The LFN would obtain a much higher effective throughput if it was connected directly to the foreign network instead of the NEMO. This difference in the throughput increases with the delay in the CN-HA-MR-LFN path. Therefore, nodes of a mobile network located way from its home network and/or from the CN they are communicating with, would obtain extremely low TCP throughput when competing with other TCP flows, because of the suboptimal path introduced by the NEMO Basic Support protocol. Even for a value of *delay1* equal to 0ms the throughput obtained by the MNN is almost a half of the one obtained by the non-mobile nodes. Although *delay1* is 0ms, the RTT between CN and MNN is bigger than the RTT between CN and fixed nodes, because the path is not direct and there are more hops, and this difference, even though small, has an important effect on the TCP fairness. Moreover, there exists a difference in the PMTU because of the overhead that also has an influence in the TCP performance.

If MIRON is used, the performance improvement is substantial (see Figure 5.7). The TCP throughput remains constant despite the value of *delay1*. This result is as expected, because with MIRON data packets do not follow the CN-HA-MR-LFN sub-optimal path, but the direct CN-MR-LFN path. Part of the difference in the TCP throughput of the fixed nodes and the LFN is due to the packet overhead (MIRON introduces a 24-byte per packet

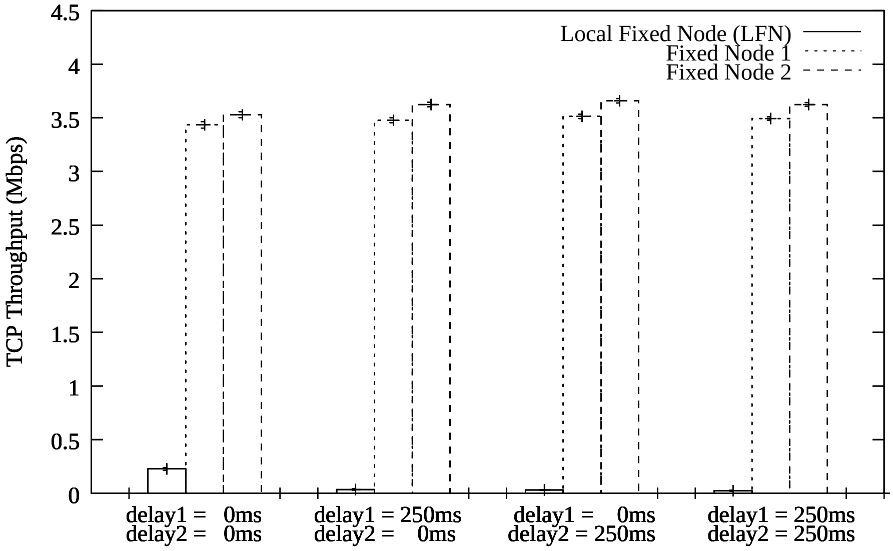


Figure 5.8: Impact of NEMO Basic Support protocol on the TCP throughput in a 2-level nested Mobile Network.

overhead, because of the Routing Header type 2 and the Home Address destination option). The performance of the MIRON prototype used during the tests (completely implemented in user space) may also have something to do with the obtained difference, although this difference could be reduced by improving the implementation (e.g., by implementing it in kernel space, or at least those tasks that have an strong impact in the overall performance).

For the nested scenario (Figure 5.5(b)), besides evaluating the effect of the varying *delay1*, that is, the delay of the path CN-HA-MR-LFN, a second adjustable delay – *delay2* – was introduced between R4 and R5, allowing us to evaluate also the effect of the distance between the home networks of two different mobile networks that are nested. Figure 5.8 shows the obtained throughput results for the NEMO Basic Support protocol and Figure 5.9 for MIRON.

As in the non-nested test (see Figure5.9), the improvement achieved by MIRON is clear. The NEMO Basic Support protocol performs worse than in the non-nested scenario, even for the null added delay case. This is because the actual RTT is bigger for the LFN than for the fixed nodes due to the longer path that packets have to traverse (CN-HA2-HA1-MR1-MR2-LFN) and the reduced PMTU. On the other hand, the performance obtained with MIRON is the same as in the non-nested scenario, as packets follow the optimal direct path and the overhead remains the same, no matter what number of nesting levels the mobile network has. As in the non-nested scenario, the TCP throughput of the LFN is lower than the one achieved by the fixed nodes because of higher RTT (packets go through more intermediate hops – MR1 and MR2) and the impact of implementing MIRON completely in user space.

5.5.2. Analytical evaluation

We have analysed how the added delay due to the suboptimal CN-HA-MR-MNN path introduced by the use of the NEMO Basic Support protocol affects the performance of TCP

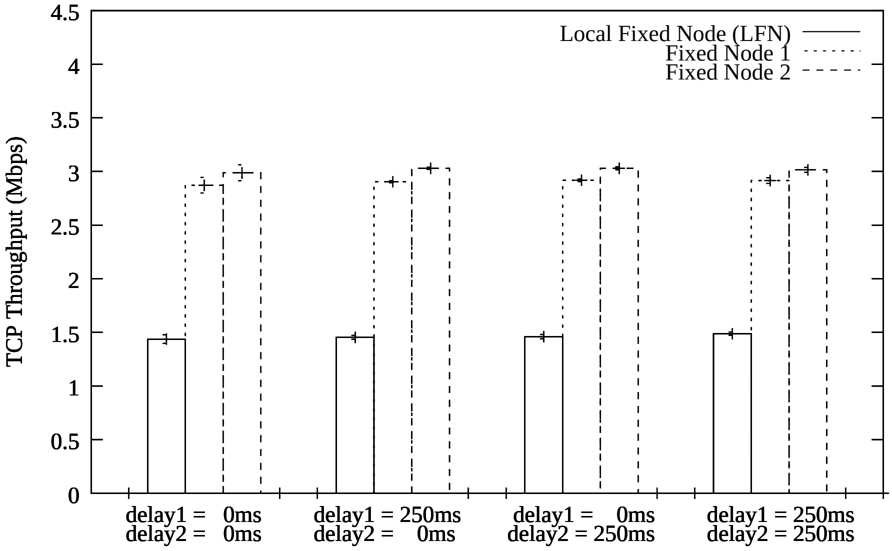


Figure 5.9: Impact of MIRON on the TCP throughput in a 2-level nested Mobile Network.

applications. In addition to the severe effect that the RTT has in the TCP performance, and the obvious effect that the delay itself has on real time applications[5], there is another effect that impacts performance: the packet overhead (and the associated PMTU reduction).

A 40-byte IPv6 header is added to every packet in the MR-HA bidirectional path due to the NEMO Basic Support protocol. Moreover, an IPv6 additional header is added per nesting level. The effect of this overhead can be negligible for non real time applications, but it can be very important for real time ones, such as VoIP applications. In order to quantitatively evaluate this effect, we analyse next the effects of the NEMO Basic Support protocol and MIRON, comparing it with plain IPv4 and IPv6, in a VoIP communication using the widely utilised Skype[6] 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. The codec is designed for narrow band speech and results in a payload bit rate of 13.33 kbps with an encoding frame length of 30 ms and 15.20 kbps with an encoding length of 20 ms.

Table 5.1 shows the packet overhead and the bandwidth consumed by a VoIP communication using UDP/RTP and the iLBC codec, for plain IPv4, plain IPv6, the NEMO Basic Support protocol and MIRON. The overhead of MIRON is less than the one introduced by the NEMO Basic Support protocol and remains constant though the number of nesting levels. The reader should notice that a nested mobile network connected to the Internet through a 64 kbps connection would not be able to support this kind of VoIP traffic (VoIP applications are expected to be very important in forthcoming 4G networks). In [dlOBC06] an additional analysis of the packet overhead in network mobility environments is presented.

[5] There are analytical studies [KT01] that state that the maximum tolerable delay in a voice communication is about 50 ms.

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

Protocol	Bitrate (kbps)	Packet Overhead (%)
IPv4	31.2	51.28
IPv6	39.2	61.22
NEMO (without nesting)	55.2	72.46
NEMO (2 nesting levels)	71.2	78.65
NEMO (3 nesting levels)	87.2	82.57
MIRON (without nesting)	48.8	68.85
MIRON (2 nesting levels)	48.8	68.85
MIRON (3 nesting levels)	48.8	68.85

Table 5.1: iLBC bitrates and packet overhead (20ms encoding length).

5.5.3. Security considerations

From the security point of view, allowing the MR to perform some operations on behalf of the LFNs attached to it (i.e. Proxy-MR operation) does not introduce any threat, because LFNs trust their MR for the routing of all their traffic. From the architectural point of view, the solution is also natural, as the Route Optimisation support defined by Mobile IPv6 [JPA04] conceptually could be implemented in multiple boxes. MIRON just applies this mechanism, by dividing the functionalities among two different physical boxes, but actually the conceptual basis of the solution is the same as the one defined in RFC 3775 [JPA04].

It may be argued that an attacker may induce the MR to initiate the Route Optimisation procedure with a large number of CNs at the same time, by sending to an LFN of the NEMO a spoofed IP packet (e.g., ping or TCP SYN packet) that appears to come from a new CN. MIRON shares this and others vulnerabilities of Mobile IPv6 [NAA$^+$05], but the solutions proposed to mitigate these attacks in [NAA$^+$05] are also applicable to MIRON. For example, to avoid bringing down the MR by making it send unnecessary Binding Updates (after performing the complete Return Routability procedure), the Mobile Router should apply some local policies [NAA$^+$05], such as:

- Setting a limit on the amount of resources (i.e. processing time, memory, and communications bandwidth) that it uses for the *Proxy-MR* functionality. In this way, when the limit is exceeded, the MR may decide to stop initiating the RO procedure for new CN-LFN communications, following the plain NEMO Basic Support protocol operation for these ones.
- The MR may also recognise addresses with which an LFN had meaningful communication in the past and only start the RO procedure for those addresses.

[NAA$^+$05] proposes additional mechanisms for a Mobile Node to avoid attacks regarding to Route Optimisation. Most of them may also be considered by a Mobile Router implementation that provides MIRON capabilities.

5.5.4. Scalability considerations

MIRON requires some additional operations to be performed in the MR. This section briefly analyses the scalability of MIRON and provides some implementation considerations to ensure a scalable deployment.

Basically, there are three different aspects that may affect to the scalability of MIRON:

- *Signalling load.* In order to optimise a CN-LFN flow, the MR has to perform the MIPv6 RO signalling with the CN on behalf of the LFN. This signalling grows linearly with the number of CN-LFN pairs being optimised. Similarly, to optimise the traffic of a VMN or a nested NEMO, the PANA and DHCPv6 signalling also grow linearly with the number of VMNs/MRs. This linearity is important, since it makes the required resources in a MR proportional to the size of the NEMO and it seems natural to expect MRs of large mobile networks (such the ones deployed in trains) to be powerful enough and not be resource-constrained. On the other hand, resource-limited devices, such as cellular phones and PDAs are not expected to be the MR of networks with more than a few attached nodes.

- *Memory consumption at the MR.* MIRON needs some additional information to be stored at the MR, such as host routes, extended Binding Cache entries (since state information regarding each LFN-CN optimised pair is required), and information about delegated addresses. The required memory to store a host route, a binding entry or the information about a delegated address is relatively small and grows linearly with the number of mobile nodes (i.e. VMNs and MRs) being optimised and LFN-CN route optimised pairs.

- *Processing load at the MR.* MIRON requires the MR to perform some additional operations: inspection of every packet, special handling (that is, removal of the Routing Header in the CN to LFN direction and addition of the Home Address Destination Option in the LFN to CN direction) of route optimised packets and source routing. Regarding packet inspection, MIRON just needs to look at the source and destination addresses of every packet to track LFN-CN flows and also to certain IPv6 headers to detect new arrived VMNs/MRs attached to the NEMO, so this inspection is quite similar to the normal inspection that a router does. Even if some local policies are implemented at the MR to enable smarter decisions about whether a certain flow should be optimised or not, requiring the MR to look also at other fields in a packet (such as transport headers), this inspection is not much different than the inspection than typical firewall software does in an border (access) router. Besides, the amount of traffic being processed by a MR is in general related to the size of the NEMO, so the same reasoning about the size of the NEMO and the resources of its MR also applies here.

  The special packet handling is performed by MIRON only to packets that belong to an LFN-CN communication that is being route optimised. Therefore, neither the optimised packets from VMNs or MRs, nor the packets of communications that are not being optimised, require such special packet handling. This special packet handling adds some delay in the packet processing time that depends on the MR capabilities and how this processing is implemented.

  Finally, source routing at the MR is needed to avoid route optimised packets to be forwarded through the MRHA bidirectional tunnel (instead of following the optimised direct path). Therefore, MIRON requires a different routing table per LFN that has traffic being optimised. Each of these routing tables has an entry per each CN the LFN is communicating with. Therefore, the amount of routing entries grows linearly with the number of different LFN-CN pairs being route optimised and it is independent of the nesting level.

We can conclude that MIRON required resources grow linearly with the number of optimisations being performed, independently of the nesting level. This allows practical deployments, since it is natural to expect that the capabilities and resources of a MR to be proportional to the size of the managed NEMO. Besides, a limit on the amount of resources (memory, processing power, etc) used by MIRON can always be set, so the MR may stop starting new RO operations when that limit is exceeded.

5.6. Comparison with previous work

This section compares two of the most well-known Route Optimisation for NEMO proposals with MIRON, in terms of performance, signalling load and complexity.

As we described in section 2.4.1.1, authors of [LJP03] propose to allow the Mobile Router directly to inform the CN about the location of the MNP (using the Prefix Scope Binding Update, PSBU) [EMU03]. We will next compare this proposal (hereafter BU for Network Prefixes) with MIRON. In particular, we will consider the benefits and the costs associated with each one of them. With respect to the costs, the main difference concerns the deployment effort associated with the different proposals. MIRON, as we have already mentioned, uses the existent MIPv6 protocol unchanged. This means that the deployment of MIRON only implies modifications to the MRs. CNs do not need any upgrade since they do not require any MIRON-specific mechanism. On the other hand, BU for Network Prefixes requires not only upgrading the MRs but also upgrading all the potential correspondent nodes, i.e. all the nodes in the Internet. This is a huge deployment cost, which may not be worth depending on the resulting benefits, which will be considered next.

The benefit resulting from the adoption of any of the proposals is the optimised path through which packets are routed between the MR and the CN. However, the approach based on BU for Network Prefixes requires less signalling than MIRON. We will next quantify the difference in order to evaluate if this overhead reduction can justify the deployment cost previously identified. Consider a moving network with N MNNs. Suppose that each MNN communicates simultaneously with M CNs in average. This means that with MIRON, $N \times M$ Binding Updates messages will be required to optimise these communications. On the other hand, if the approach based on BU for network prefixes is used, the number of BU required depends only of the number of different CNs that are communicating with at least one MNN. This is so, because the BU message refers to the whole MNP, implying that if two or more MNNs are communicating with the same CN, only one BU message is needed. The net benefit resulting from the adoption of BU for Network Prefixes with respect to MIRON is a reduction in the amount of BU messages required proportional to the number of MNNs that are simultaneously communicating with a common CN. It should be noted that this only applies for those CNs that do not belong to the Home Network, since those nodes residing in the Home Network already benefit from a direct routing with the mobile network thanks to NEMO Basic Support protocol. So, the benefits provided by an approach based on BU for Network Prefixes heavily depend on the expected number of MNNs that will communicate with a common CN outside the Home Network. The costs, on the other hand, are objective and account for the upgrading of all the nodes of the Internet to support the new option. MIRON, on the other hand, is compatible with standard Mobile IPv6 CNs.

The NEMO Basic Support protocol when applied to the case of nested mobile networks is quite inefficient as was mentioned in section 2.4.2. The Reverse Routing Header (RRH) mechanism [TM04a] proposes a solution to alleviate these inefficiencies. The proposal requires modifications in MRs and HAs, but not in LFNs, VMNs, or CNs. Besides, this proposal requires the use of Tree Discovery [TM04b] to allow the MRs to find out the level of hierarchy in the nesting.

RRH introduces an overhead (see section 2.4.2.1 for details of the mechanism operation) that can be quantified in one IPv6 header plus one routing header plus one IPv6 address per level of nesting of the Mobile Network, i.e. $(40 + 8 + n \times 16)$ bytes $= (48 + n \times 16)$ bytes, where n is the number of levels in the nesting (at least 2). This overhead is required in all the packets that go to and from the mobile network. It could be eliminated from some packets in the way out of the mobile network only at some cost in functionality (ability to detect changes in the nesting) and security. Notice that the solution of MIRON for nested mobile networks only requires the 40 bytes of the tunnelling and even that is avoided when an end-to-end optimisation of the path between the mobile network and the CN is used.

The additional need for using Tree Discovery [TM04b] implies changes in MRs and routers included in the nesting, because Router Advertisements must support the functionality of Tree Discovery. This also implies an overhead in signalling because Router Advertisements in the nesting must have a minimum of 32 bytes more than normal Router Advertisements. This must be compared with the signalling load required to distribute topological valid addresses to MRs in MIRON.

Based on the previous analysis, we can conclude that MIRON provides better Route Optimisation support than the two chosen proposals for comparison: PSBU and RRH. Besides, MIRON does not require to change any node but the MR, and in most cases requires less signalling load to optimise traffic.

5.7. A long term approach: secure delegation-based RO mechanisms

MIRON is a Route Optimisation solution for NEMO that has been designed with a very strong requirement in mind: not to impose any change on the operation of any node of the Internet (i.e. CNs) or any node attached to the Mobile Network (that is, MNNs). This is so in order to enable an easy deployment of the solution. However, it may be argued that there are certain scenarios that could benefit from different NEMO RO mechanisms (e.g., those scenarios that require stronger security guarantees or need to limit even more the signalling load required by the solution). Because of that, in this section a brief discussion about other alternative approaches is provided, based on the secure delegation of the signalling rights [NA03] to the Mobile Router.

There are several good reasons to let the Mobile Router in a NEMO send the signalling on behalf of the MNNs belonging to that NEMO (that is, whenever it is needed to optimise a MNN-CN communication flow, the MR sends a Binding Update to the CN, binding the

MNN’s HoA to the MR’s CoA). One of these reasons is the reduction of the signalling overhead within the NEMO, since it is the MR the one that manages the Route Optimisation and therefore MNNs no longer send any signalling regarding NEMO RO.

Although MIRON partially follows this kind of approach, there are several scenarios in which a different mechanism may be needed. For instance, it is known that in different contexts there have been doubts about the goodness of the MIPv6 Return Routability mechanism[7], and therefore it may be necessary to think of different approaches to the NEMO RO problem (compared to the MIRON solution). Future Route Optimisation mechanisms may take advantage from introducing changes on the operation of Correspondent Nodes and/or Mobile Network Nodes. For instance, this may enable the use of strong cryptography mechanisms to provide Route Optimisation support for NEMO.

A strong cryptography approach to protect Binding Updates must be based on a security association between the two nodes participating in the communication (i.e. MNN and CN). When signalling messages (e.g., Binding Updates) are sent, the problem is then how to efficiently create a security association between these nodes. Some solutions have already been proposed to solve that in Mobile IPv6 for host mobility scenarios. We consider the following important solutions: solutions based on the availability of a Public Key Infrastructure (PKI), solutions based on the use of Cryptographically Generated Addresses (CGAs) [Aur05], [Aur03], [AVH06] and solutions based on Crypto Based Host Identifiers (CBHIs) [vB04].

Letting the MR send the location update signalling on behalf of the MNNs has some advantages (such as a reduction of the signalling overhead). In MIRON, the MR behaves as a Proxy-MR for the RO signalling of the LFNs. However, in order to enable the MR to send also the signalling on behalf of LMNs and VMNs, a delegation of the signalling rights to the MR is needed. That is, some procedure must be carried out to allow the MR to send signalling messages on behalf of MNNs, in a way that enables the CN to verify that the MR is actually allowed to send this signalling.

Next, different approaches to the secure delegation of the signalling rights are explored.

5.7.1. Delegation based on PKI certificates

As a first approach, the delegation may be expressed in the form of certificates generated by a PKI. This general concept can be easily adapted to be used in NEMO. Basically, the PKI assigns prefix certificates to MRs, binding a MR public key to a NEMO Mobile Network Prefix.

$$CERT = [MNP, K_{MR}+]_{K_{CA-}}$$

Basically, the certificate states that the MR owning the public key K_{MR+} is authorised to bind a CoA to a HoA with network prefix MNP. This certificate is signed by a Certification Authority (CA).

[7] Many mobile operators seem to be reluctant to use a solution based on Return Routability as compared to ”strong cryptography” to protect the location information updates (i.e. Binding Updates sent to Correspondent Nodes) in their Mobile IPv6 deployments. Essentially RR is considered a ”weak security mechanism” and it is accused of introducing a non-negligible burden of signalling in the network, which is a relevant handicap in links where resources are scarce (i.e. the wireless access link from a NEMO to the infrastructure).

5.7.1.1. Procedure of operation

- The MR obtains a certificate from the PKI, containing the Mobile Network Prefixes associated to the MR.
- Each Binding Update sent by the MR to a CN on behalf of a MNN is signed with the MR's private key. The message also contains the MR's prefix certificate.
- The Correspondent Node, when receiving a Binding Update, obtains the prefix certificate associated with the HoA contained in the BU, and verifies it. If the Binding Update is valid, the CN adds an entry in its Binding Cache.

5.7.1.2. Analysis of the solution

In this approach, a high protection against identity attacks is provided, but the major drawback of this solution is the requirement of a global key infrastructure, which is an unrealistic requirement for the whole Internet nowadays (although it is a solution feasible in more restricted environments).

Using prefix certificates introduces the non-trivial issue of the Prefix Ownership and this problem is much more complex than the basic Address Ownership issue that arises with Mobile IP.

5.7.2. Delegation based on self-signed certificates

In this case, the MNN is assumed to have a Cryptographically Generated Address (CGA) as its HoA. As described in [Aur05], a CGA[8] is an IPv6 address, which contains a set of bits generated by hashing the IPv6 address owner's public key. This property allows the user to provide a ”proof of ownership” of its IPv6 address. On the other hand the MR (i.e. delegate) has a certificate as follows:

$$CERT = [CGA, K_{MR+}]_{K_{MNN-}}$$

Basically, the certificate states that the MR owning the public key K_{MR+} is authorised to bind a CoA to the CGA (MNN's HoA) included in the certificate. In other words, the MNN, identified by the CGA, delegates the right to send Binding Updates (location update messages) to a trusted node, the delegate, identified by K_{MR+}. This certificate is signed with the MNN's private key associated to the CGA (K_{MNN-}).

5.7.2.1. Procedure of operation

In this scenario, whenever a MNN-CN RO is needed, the MR performs it on behalf of the MNN and sends to the CN a location update message (BU) linking the MNN's HoA to a CoA. The process is the following: the Binding Update is signed with the MR's private key and it includes the certificate. When the CN receives this location update message, it first verifies the certificate using the MNN's public key associated to the CGA (HoA of the BU) and then it verifies the received message using the MR's public key (K_{MR+}), included in the certificate.

[8] A more elaborated description of CGAs is provided in Section 6.3.2.1.

5.7.2.2. Analysis of the solution

The main advantages of this approach are the following:

- It does not require the deployment of a PKI infrastructure. This is a crucial point because assuming the availability of a global PKI infrastructure is not very realistic in large networks (e.g., Internet), at least nowadays.
- On the other hand, it would be potentially compatible with SEND [AKZN05].

Also, some drawbacks can be pointed out:

- The solution is not transparent for the CN, since any CN must understand the address format and the procedures involved, which requires changes on the software of the CN.

5.7.3. Implicit Delegation

In this approach to the delegation of signalling rights, there is not explicit delegation from the Mobile Network Node to the Mobile Router. Instead, the MNN gives to the MR the right to send signalling on its behalf by accepting the use of an address with a particular structure (the address format is proposed in [vB04]).

5.7.3.1. Address format

This address (an IPv6 address) is composed of the network prefix (64 bits) and the Interface Identifier (64 bits). The network prefix is simply the Mobile Network Prefix. The Interface Identifier (IID) is called a Crypto Based Host Identifier [vB04] and is created in the following way:

$$IID = [4\, control\ bits,\ 48\, bit\ site\ identifier,\ 12\, host\ bits]$$

The format for this IID is proposed and described in [vB04]. The 4 control bits are: one reserved, one to distinguish between 80 bit identifiers and 64 bit identifiers (in this application we are only interested in 64 bit identifiers), and the usual universal/local bit and group bit. To ensure EUI-64 compatibility, [vB04] proposes to set the u/l bit to ”universal” and the group bit to indicate a group address. Because we have 12 host bits, we will be able to address $2^{12} = 4096$ hosts, which seems to be large enough for a NEMO.

The site identifier contains cryptographic information that allows Correspondent Nodes to verify that the address is used legitimately. The site identifier must contain the following information (this is different from what is proposed in [vB04] because of the reasons explained in next section):

$$NEMO\ Site\ identifier = Hash(MNP, K_{MR+})$$

5.7.3.2. Procedure of operation

A MR willing to serve a NEMO by sending the signalling on behalf of its MNNs, must generate a pair of keys: public/private. Then, it generates and provides addresses (Home Addresses or HoAs) to the MNNs. The addresses have the format explained in the previous section.

If the MR wants to send a Binding Update on behalf of a MNN of its NEMO to a Correspondent Node, the MR signs the BU with its own private key. The MR also informs the Correspondent Node of its public key and Mobile Network Prefix (that must match the one of the HoA included in the BU).

The CN can verify the address by re-calculating the Site Identifier (it has the MR public key and the NEMO Mobile Network Prefix) and checking that it matches that of the HoA. Using the MR public key, the CN can also verify the authenticity of the BU.

An attacker cannot generate a fake BU that binds a certain HoA to a CoA. To be able to do that, the attacker would need to authenticate the BU with a private key that corresponds to the public key used to create the Site Identifier of the HoA.

An attacker can also try to generate pairs of public/private keys and create a dictionary of 2^{48} different Site Identifiers. Then, if the attacker detects a particular HoA that she wants to attack, she only has to look up the public/private key corresponding to the Site Identifier of the HoA in the dictionary. Using the Mobile Network Prefix in the calculation of the Site Identifier makes this attack much more difficult, because the dictionary must include not only Site Identifiers but also network prefixes: $2^{48} \times 2^{64}$ entries.

Notice that in this section we focused on the conceptual ideas of this mechanism, a practical solution would use some improvements, for example a symmetric key could be generated from the public/private key for doing authentications less computationally costly. Also, the particular hash algorithm or public key cipher method are not analysed.

5.7.3.3. Analysis of the solution

The main advantage of this delegation solution is that is very simple. Nevertheless some disadvantages can be pointed out:

1. It is incompatible with stateless address autoconfiguration and other solutions that work with the IID as CGAs (what can have a negative effect in SEND for example).

2. The solution is not transparent for the CN, i.e. any CN must understand the address format and the procedures involved, which requires changes to the software of the CN.

3. It imposes a limit of 2^{12} to the number of hosts in a NEMO. This does not seem to be a great problem for a NEMO. A solution for this limitation would be to use more than one prefix in the NEMO (this, of course, uses address space).

5.7.4. Secure-delegation of signalling rights: summary and final remarks

In this section, we have analysed the need of a delegation of the signalling rights in those environments in which a Route Optimisation for NEMO using strong cryptography is required.

The delegation of signalling rights can be done in an explicit way, by means of authorisation certificates, or, as it has been devised here, in an implicit way, accepting the use of an address with some particular characteristics.

Likely, the simplest solution, implicit delegation, has also several limitations (as incompatibilities with other mechanisms like SEND or stateless address auto-configuration). The most flexible solution, the one based on PKI certificates, requires an important infrastructure. The solution based on CGAs can be a good compromise between complexity and flexibility.

5.8. Conclusions

The NEMO Basic Support protocol [DWPT05] enables whole networks to move and change their point of attachment, transparently to the nodes of the network. This solution introduces some limitations and problems in terms of performance (increased delay in packet delivery and packet overhead, decrease in available PMTU, the HA becoming a bottleneck, etc). To overcome these limitations we have designed and implemented a Route Optimisation solution: MIRON, that enables direct path communication between a node of the mobile network – supporting any kind of node, with and without mobility capabilities – and a Correspondent Node.

MIRON has two modes of operation: the MR performing all the Route Optimisation tasks on behalf of those nodes that are not mobility capable – thus working as *Proxy MR* [NZWT06] – 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 Routers) that actually have mobility and Route Optimisation capabilities to manage their own Route Optimisation.

To validate the design of the solution and evaluate the actual performance of it, a prototype of MIRON was implemented in Linux. The NEMO Basic Support was also implemented so we could compare the results obtained with MIRON with the basic solution for network mobility. Tests involving TCP applications showed that the increased RTT perceived by the nodes of a NEMO (due to the suboptimal path followed by packets) has a severe impact on the performance (in terms of effective throughput, when sharing some link with traffic from other active non-mobile TCP nodes). This effect is exacerbated when NEMOs are nested. On the other hand, the same tests conducted with MIRON showed a better performance, by obtaining much higher effective TCP throughput than in the case of the NEMO Basic Support, also in the case of nested networks.

The effect of packet overhead was described by means of a quantitative analytical study of the overhead that several protocols add to packets belonging to a VoIP application, such as Skype. These results show that the packet overhead introduced by the NEMO Basic Support protocol is significant for this kind of application, specially when there is nesting.

We could also think about a long term NEMO Route Optimisation solutions that could be developed without the constraints of keeping CNs (i.e. any potential peer that a node in the mobile network may have) unmodified. An interesting approach along this line is the secure delegation of the signalling rights to the Mobile Router. Three different solutions based on this scheme have been proposed. We think that there is the need of working in the design of NEMO RO solutions that, by taking advantage of introducing some changes on Correspondent Nodes and/or Mobile Network Nodes, could be more efficient than MIRON.

But both types of solutions will coexist, because a large installed base of legacy nodes will require a solution like MIRON.

In conclusion, this chapter proposes a Route Optimisation for NEMO solution (MIRON), that provides significant performance improvements over the NEMO Basic Support protocol and that is implemented only modifying the software in the MRs. LFNs, VMNs, or CNs do not need to be modified for MIRON to work, which facilitates the deployment of the solution. The validity of the solution has been proven by making experiments and tests with an implementation for Linux.

We want to highlight that MIRON is cited in a document of the IETF NEMO Working Group that analyses the NEMO Route Optimisation solution space [NZWT06], considering MIRON as one of the reference solutions.

Chapter 6

Route Optimisation for Mobile Networks in the car-to-car scenario

6.1. Introduction

There exist several vehicular applications (see Section 3.1), such as multi-player gaming, instant messaging, traffic information or emergency services, that might involve communications among vehicles that are relatively close each other (i.e. car-to-car communications) and may even move together (e.g., military convoys). These applications are currently not well supported in vehicular scenarios.

Although automobiles can communicate with other vehicles through the infrastructure (the Internet) by means of the NEMO Basic Support protocol, they could benefit from better bandwidth, delay and, most probably, cheaper communication, by forming vehicular ad-hoc networks (VANETs) and making use of the resulting multi-hop network to directly communicate with each other. The challenge is to achieve this direct communication through the VANET with a security level equivalent to the one provided by today's IPv4 fixed Internet.

As described in Section 3.2.3, to the best of our knowledge, there is only one proposal, described in [WMK$^+$05], that combines Network Mobility and ad-hoc approaches. This solution assumes that each vehicle is a moving network and the performance of inter-vehicular communications is improved by creating and using a VANET. This mechanism is a first attempt to optimally combine Network Mobility and ad-hoc concepts to support vehicular communications. However, the security analysis of this proposal was omitted by the authors. Their proposed solution has several security vulnerabilities, that would enable malicious nodes to perform several types of attacks [NAA$^+$05], such as stealing traffic or flooding a particular node. The design of a solution that provides a combination of NEMO and VANET to optimise vehicular communications in a secure way is one of the main objectives of this PhD thesis.

This chapter presents a Route Optimisation solution called Vehicular Ad-hoc Route Optimisation for NEMO (VARON). VARON allows local car-to-car communications to be optimised, by enabling – in a secure way – the use of a Vehicular Ad-hoc Network (VANET) for local communications among cars. The rest of the chapter is organised as follows. An analysis of the security challenges posed by a generic vehicular solution that combines a Network Mobility approach (e.g., based on [DWPT05]) for general car-to-Internet communications, with ad-hoc mechanisms aimed at improving local car-to-car communications, is provided in Section 6.2. After that, VARON protocol operation is described in detail in Section 6.3. A security analysis, and a validation and evaluation of the proposed mechanism – based on simulation – are provided in Section 6.4. Finally, Section 6.5 is devoted to the conclusions.

6.2. Exploits against vehicular ad-hoc car-to-car optimisations

By using a Vehicular Ad-hoc Network to route packets of local car-to-car communications, the performance of the communications in such a kind of scenario may be greatly improved – in terms of bandwidth and delay – when compared to data traversing an infrastructured network through a cellular radio network (e.g., UMTS). However, this kind of optimisation enables many different types of attacks. In this section, we briefly describe some relevant examples of attacks that would be possible if no additional mechanisms were used to secure this optimisation. This would help us to introduce all the relevant security problems that our proposal – VARON (described in Section 6.3) – avoids.

There are several types of attacks that may be performed against a vehicular ad-hoc car-to-car optimisation. Next, we describe the most relevant ones:

- **Prefix ownership attacks.** Devices within a vehicle form a mobile network, sharing a prefix (the Mobile Network Prefix), which is managed by the Mobile Router of the vehicle. It is necessary to provide Mobile Routers with a mechanism that enables them to mutually verify that a Mobile Router actually manages the Mobile Network Prefix it claims to (i.e. it is authorised to forward/receive packets addressed from/to that MNP). Otherwise, a malicious node would be allowed to spoof ("steal") a certain prefix and get all the traffic addressed to this prefix from other MRs connected to the ad-hoc network.

  Figure 6.1 illustrates an example of this attack. Alice is accessing her Internet bank account from her PDA that is connected to the Internet through the mobile network deployed in the car where she is travelling. The car is accessing the Internet through a UMTS interface. A malicious node (MR M) claims that it owns the IPv6 prefix `prefixBank::/64`. Since MR M is reachable through the VANET and Alice's bank server address belongs to `prefixBank::/64`, MR A decides to optimise this traffic by forwarding it to MR M, using the shorter route through the VANET. This is a clear example of how dangerous a Route Optimisation mechanism can be if not properly secured.

- **Ad-hoc routing attacks.** The creation and maintenance of the ad-hoc routes to locally exchange traffic between MRs connected to the VANET, is a critical issue from the security point of view. This task is performed by ad-hoc routing protocols, which still suffer from many vulnerabilities, mainly due to the unmanaged and non centralised nature of ad-hoc networks. Typical exploits against existing ad-hoc routing protocols may be classified into the following categories [SLD$^+$05]:

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

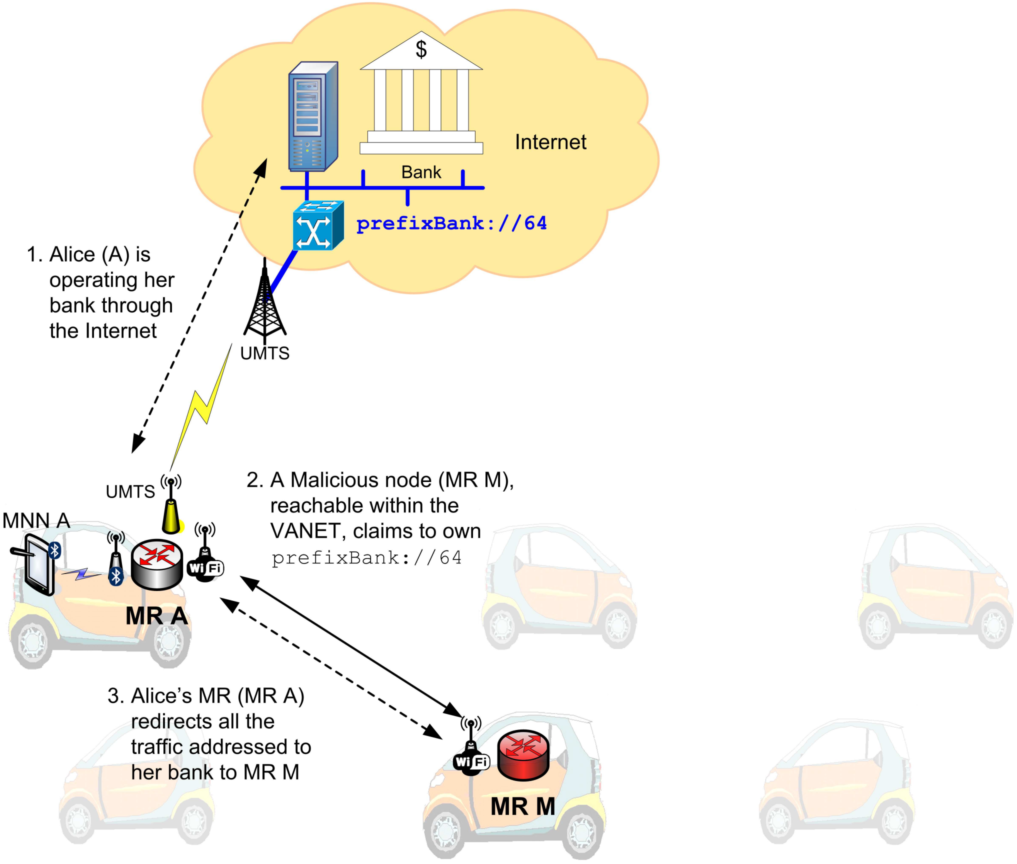

$
Internet
Bank
prefixBank://64
1. Alice (A) is operating her bank through the Internet
UMTS
UMTS
2. A Malicious node (MR M), reachable within the VANET, claims to own prefixBank://64
MNN A
MR A
3. Alice's MR (MR A) redirects all the traffic addressed to her bank to MR M
MR M

Figure 6.1: An example of prefix ownership attack.

this attack (see Figure 6.2), a malicious node MR M could prevent a legitimate node MR B from receiving traffic from a node MR A by consistently advertising to an intermediate node (MR 2) a shorter route to MR B than the one that the true next hop towards B (MR 3) advertises.

- *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 claims that a neighbour cannot be reached.

  An example of fabrication and impersonation combined attack could be the following. Suppose that in the example of Figure 6.2, MR A has a route to MR B established via MR 1, MR 2, MR 3 and MR 4. A malicious node MR M could keep traffic from reaching MR B (i.e. Denial-of-Service attack against MR B) by continuously sending route error messages to MR A, spoofing MR 2 identity, indicating a broken link between MR 2 and MR B. If this is done by MR M every

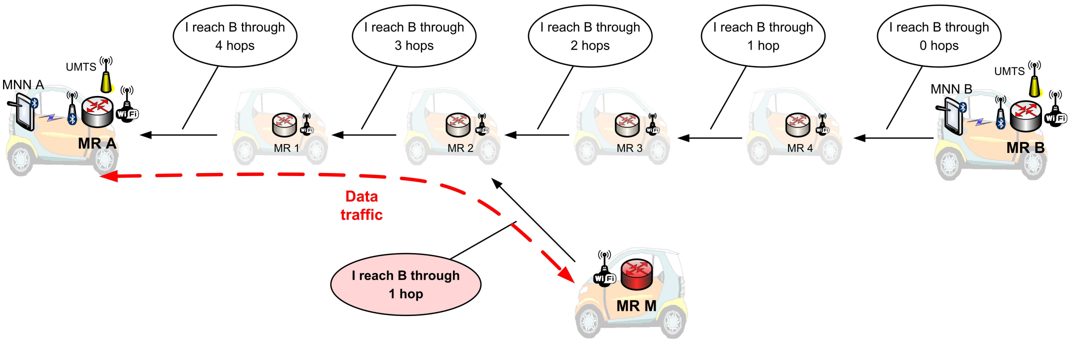


Figure 6.2: An example of ad-hoc modification attack.

time MR A manages to set-up a route to MR B, the communication between MR A and MR B through the VANET is prevented from taking place.

Some ad-hoc secure protocols make impossible to perform most of these exploits (such as ARAN [SLD$^+$05]). However, there is no mechanism that combines in a secure way a Network Mobility approach (to provide vehicles with global connectivity), and a Vehicular Ad-hoc Network (to optimise local car-to-car communications). By security, we mean a mechanism that is not exploitable in the previously described ways. However, we do not deal with the issue of avoiding DoS attacks based on noncooperation and packet dropping, which are really difficult to mitigate in ad-hoc networks.

6.3. Vehicular ad-hoc Route Optimisation solution for NEMO

In this section, we present a novel solution that provides Route Optimisation for NEMO in vehicular environments, where a Vehicular Ad-hoc Network (VANET) may be created and securely used to optimise local communications among vehicles.

It is assumed that the Mobile Router (MR) deployed in each vehicle will have at least three network interfaces: one *ingress* interface to communicate with the nodes inside the vehicle that belong to the NEMO (e.g., WLAN, Bluetooth), one or more *egress* interfaces to connect to the Internet (e.g., UMTS, WiMAX, even WLAN in some cases), and an additional ad-hoc interface (e.g., WLAN) to communicate with neighbouring cars and set-up multi-hop networks (see Figure 4.1). Compared to a normal Mobile Router (without any ad-hoc optimisation), only one (ad-hoc) additional interface is required. It is important to notice that Mobile Routers deployed in vehicles will not be much concerned about energy constraints, as opposed to personal mobile devices or other ad-hoc scenarios (such as sensor networks).

It is also assumed that vehicle's devices will be always able to communicate with other vehicle's devices through the Internet, by using the NEMO Basic Support protocol. On the other hand, there may exist the possibility of enabling these devices to directly communicate if a multi-hop vehicular ad-hoc network could be set-up by the involved vehicles and other neighbouring cars. VARON aims at making possible to benefit from this optimisation opportunity in a secure way.

In our proposal, VARON, the MR is the node in charge of performing the optimisation of the communications. The steps for carrying out this procedure are the following:

1. *Discovery of reachable MNPs.* The MR needs to find out which other MRs are available within the VANET, that is, which Mobile Network Prefixes are reachable through its ad-hoc interface.

2. *Creation of a secure ad-hoc route* between the MRs of the mobile networks that want to optimise the route they are using to exchange traffic. The ad-hoc routing protocol used to create this route should provide certain security guarantees making impossible to perform any of the exploits described in Section 6.2. The mechanism used by VARON to set-up and maintain a secure ad-hoc route is based on ARAN (Authenticated Routing for Ad-Hoc Networks) [SLD$^+$05], modified and extended to fulfil the requirements of our Network Mobility based vehicular scenario.

Next, we describe in detail each of these two steps.

6.3.1. Discovery of reachable MNPs

Every MR announces its Mobile Network Prefix (MNP) by periodically broadcasting – through the ad-hoc interface – a message, called *Home Address Advertisement* (HoAA)[1], that contains its Home Address and an associated lifetime, to allow this information to expire. These messages are announced through the ad-hoc interface, by using a hop-limited flooding, so every MR becomes aware of the MNPs that can be reached through the VANET.

The MR's HoA is chosen to belong to the NEMO's Mobile Network Prefix. The length of the MNP is fixed to 64 bits (/64) due to security reasons that will be explained later. Hence, the MNP can be inferred directly from the HoA (it is the network part of it). With the MRs' announcements, every MR is aware of all the MR's HoAs (and associated Mobile Network Prefixes) that are available within the ad-hoc network.

6.3.2. Creation of a secure ad-hoc route

6.3.2.1. Building the ad-hoc route

In case a Mobile Router detects that there is an ongoing communication between a node attached to it and a node attached to another MR that is available through the VANET and this communication is decided to be optimised (how this decision is taken is out of the scope of this PhD thesis), the MR needs to build a multi-hop route to send packets directly through the ad-hoc network.

An example (Figure 6.3) is used to illustrate in more detail the proposed mechanism. A device (e.g., a back-seat embedded video game system) in car A is communicating with another device in car B[2]. This communication is initially being forwarded through the Internet, following the suboptimal path determined by the NEMO Basic Support protocol, thus traversing Home Networks A and B before being delivered to the destination. We call this

[1] The format of all the VARON protocol messages is described in Appendix B.

[2] Another example could be a car A from an emergency service convoy communicating with another emergency car B.

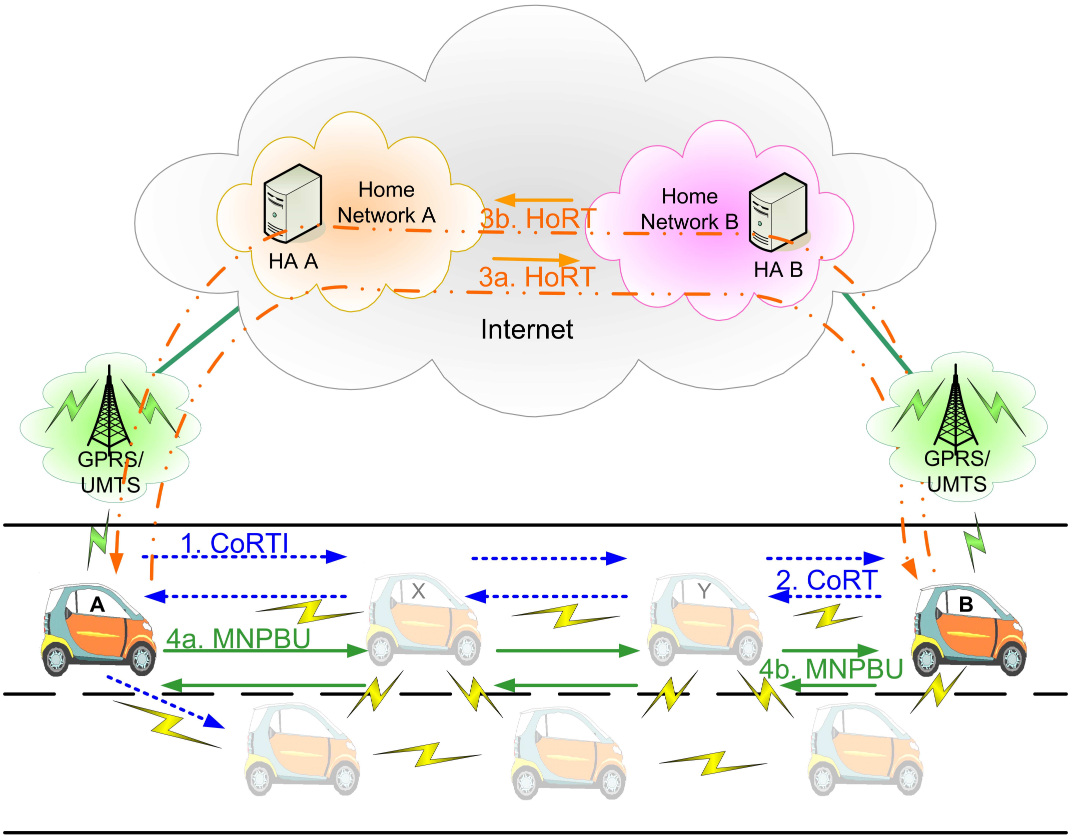


Figure 6.3: Care-of Route discovery and validation.

route *Home Route*. By listening to the announcements (i.e. HoAA messages) received in the ad-hoc interface, MR A becomes aware that the destination of such communication may be also reachable through a VANET formed by neighbouring VARON enabled vehicles. Then, MR A may decide to start using the vehicular ad-hoc network to route this traffic, instead of sending it through the Internet.

The first step in this optimisation process is that MR A must learn and set-up a bidirectional route through the vehicular ad-hoc network to MR B (the MR claiming to manage MNP B). We call this route *Care-of Route*. For doing this, MR A (the *originator MR*) sends – through its ad-hoc interface – a *Care-of Route Test Init* (CoRTI) message (Table 6.1 summarises our notation) to its one-hop neighbours:

$$\begin{array}{l} A \rightarrow \text{one-hop neighbours :} \\ [CoRTI, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}} \end{array}$$

This message includes, besides the identifier of the message (CoRTI), the destination MR's HoA (HoA_B), a nonce N_A (to uniquely identify a CoRTI message coming from a source; every time a MR initiates a route discovery, it increases the nonce), the IP address of MR A (HoA_A) and its public key (K_{A+}), all signed with the MR A's private key (K_{A-}). When a MR receives through its ad-hoc interface a CoRTI message, it sets up a reverse route back to HoA_A (MR A's HoA), by recording the MR from which it received the message

K_{A+}	Public Key (and CGA related information) of MR A
K_{A-}	Private Key of MR A
$[d]_{K_{A-}}$	Data d digitally signed by MR A
N_A	Nonce issued by MR A
HoA_A	Home Address of MR A
CoRTI	Care-of Route Test Init message type
CoRT	Care-of Route Test message type
CoRE	Care-of Route Error message type

Table 6.1: Table of variables and notation.

(so it knows how to send a reply in case it receives a message that has to be sent back to HoA_A). In order to authenticate the message, a mechanism that securely binds the IP address of MR A (HoA_A) with K_{A+} is needed. One possibility is to use certificates issued by a third trusted party, as proposed in ARAN [SLD$^+$05], but this solution seems unfeasible for vehicular environments. Instead, this secure binding is obtained by using a special type of addresses: Cryptographically Generated Addresses (CGAs) [Aur05].

Cryptographically Generated Addresses (CGA) are basically IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and the IPv6 prefix[3]. The binding between the public key and the address can be verified by re-computing the hash function and comparing the result with the interface identifier (see Figure 6.4). In this way, if the HoA used by MRs is a CGA, a secure binding between the MR's HoA and the MR's public key is provided, without requiring any Public Key Infrastructure (PKI) to be available. Notice that by itself, CGAs do not provide any guarantee of prefix ownership, since any node can create a CGA from any particular Mobile Network Prefix by using its own public-private key pair. But a node cannot spoof the CGA that another node is legitimately using, because it does not have the private key associated with the public key of that IP address.

A receiving MR (e.g., MR X in Figure 6.3) uses MR A's public key (included in the message) to validate the signature, then appends its own public key (K_{X+}) to the message, and signs it using its private key (K_{X-}). The signature prevents spoofing or message modification attacks, that may alter the route or form loops. Then, it forwards the CoRTI message:

$$\begin{aligned} &X \rightarrow \text{one-hop neighbours}: \\ &\Big[[CoRTI, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}}, K_{X+}\Big]_{K_{X-}} \end{aligned}$$

Upon receiving this CoRTI message from neighbour MR X, MR Y verifies the signatures from the originator MR A and the neighbour MR X, stores the received nonce to avoid reply attacks and adds a route to HoA_A through HoA_X (MR X). Then, the signature and public key of the neighbour MR X are removed, and MR Y appends its own public key, signs the message, and forwards it:

[3] There are additional parameters that are also used to build a CGA, in order to enhance privacy, recover from address collision and make brute-force attacks unfeasible. We intentionally skip these details. The interested reader may refer to [Aur05] for the complete procedure of CGA generation.

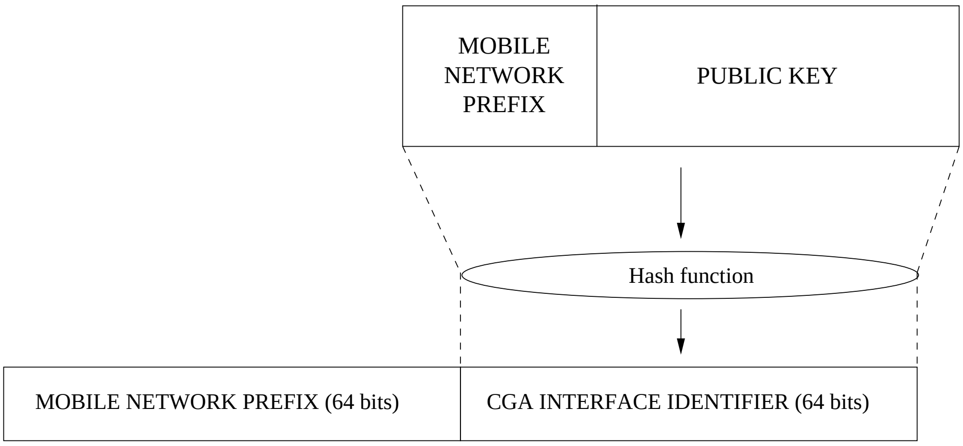

MOBILE NETWORK PREFIX
PUBLIC KEY
Hash function
MOBILE NETWORK PREFIX (64 bits)
CGA INTERFACE IDENTIFIER (64 bits)

Figure 6.4: Simplified overview of CGA creation and structure.

$$Y \rightarrow \text{one-hop neighbours :}$$
$$\Big[[CoRTI, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}}, K_{Y+}\Big]_{K_{Y-}}$$

This last step is repeated by any intermediate node along the path until the CoRTI message reaches the destination (the *target MR*, MR B) or the allowed hop limit expires. Notice that MR B, after receiving the CoRTI message, has the guarantee that only the node that has the private key associated with HoA_A (K_{A-}) could have sent the CoRTI message.

Once MR B receives the CoRTI message, it generates a reply message (including the received nonce N_A), called *Care-of Route Test* (CoRT), and unicasts it back following the previously learnt reverse path to the originator (MR A):

$$B \rightarrow Y :$$
$$[CoRT, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}$$

Each node in the reverse path performs a similar procedure that when forwarding the CoRTI: the first MR in the reverse path that forwards the message (i.e. MR Y) verifies the signature and, if correct, adds its public key K_{Y+}, signs the message and sends it to the next MR in the path:

$$Y \rightarrow X :$$
$$\Big[[CoRT, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}, K_{Y+}\Big]_{K_{Y-}}$$

The MR X also sets up a reverse route back to MR B's HoA by recording the MR from which it received the message.

The remaining MRs in the reverse multi-hop route, when receiving the CoRT message, verify the signature of the previous MR, remove it and the associated public key, add their public key, sign the message, forward it to the next MR, and set-up the reverse route. In the example, when MR X receives the message from MR Y, it sends the following to MR A:

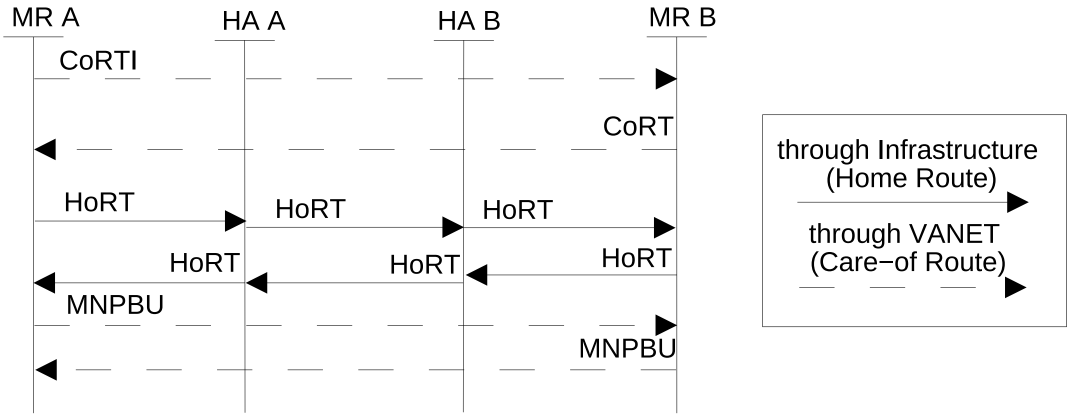

MR A
HA A
HA B
MR B
CoRTI
CoRT
HoRT
HoRT
HoRT
HoRT
HoRT
HoRT
MNPBU
MNPBU
through Infrastructure (Home Route)
through VANET (Care−of Route)

Figure 6.5: Care-of Route authentication signalling.

$$X \rightarrow A : \\ \Big[[CoRT, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}, K_{X+}\Big]_{K_{X-}}$$

When the originator MR (MR A in the example) receives the CoRT message, it verifies the signature and nonce returned by the destination MR (MR B). Once this procedure is completed, MR B has successfully established a route with MR A within the multi-hop vehicular ad-hoc network. This route is basically a temporal path (Care-of Route) to reach MR B's HoA, additional to the default route that MR A may always use to send packets towards MR B (through the Internet, using the Home Route), and vice-versa.

6.3.2.2. Authenticating the Care-of Route

The Care-of Route cannot be used to forward packets between NEMO A and NEMO B yet, since it has not been proved neither that MR A manages MNP A, nor that MR B manages MNP B. So far, only the validity of a route to a node (B and A) with an address (HoA_B and HoA_A) for which the node has the respective private key has been proved to MR A and MR B. It has not been verified that MR A and MR B are actually the routers authorised to manage MNP A and MNP B, respectively. Without further verification, nothing could prevent a MR from stealing a mobile network's traffic. For example, a malicious node could be able to claim the ownership of a given IP address (an address belonging to MNP A) and steal packets addressed to that prefix (MNP A). This issue is similar to that of Route Optimisation in Mobile IPv6, where a mechanism is required to enable the Mobile Node to prove that it *owns* both the Care-of Address and the Home Address.

The Return Routability procedure defined for Mobile IPv6 is based on two messages sent by the CN, one sent to the Mobile Node's Home Address and another to Mobile Node's Care-of Address. Based on the content of the received messages, the Mobile Node sends a message to the Correspondent Node [JPA04], [NAA^{+}05]. By properly authenticating the message, this procedure is enough to prove that the Mobile Node has received both messages and therefore it has been assigned (that is, *owns*) both the Home Address and the Care-of Address at that time.

In VARON, we borrow from the Return Routability (RR) procedure some of the underlying security concepts. With the RR, the Correspondent Node is provided with a mechanism to verify that a Mobile Node is able to send and receive packets from two different addresses. In VARON, what is needed is to provide a pair of end-point MRs (which are communicating with each other through the Home Route) with a mechanism to verify that the multi-hop route within the VANET connects each of them with the same node that is reachable through the infrastructure when addressing the respective HoA. In this way, the two end-point MRs may choose to use that Care-of Route instead of the Home Route.

The essence of the Care-of Route authentication procedure in VARON is that the two end-point MRs involved in a particular Route Optimisation procedure request each other to verify that the VANET Care-of Route may be used to send traffic between the two NEMOs. This is done (see Figure 6.5) as follows:

- Each Mobile Router generates a key, K_{mr}, which can be used with any other MR. In addition, the MR generates nonces at regular intervals. These nonces[4] and K_{mr} will be used to generate a security association between the two end-points MRs.

- Each MR creates two tokens and sends each of them through one of the possible routes (Care-of and Home routes). Tokens are generated from K_{mr} and a particular nonce.

- The first part of the Care-of Route authentication procedure is done at the same time – and using the same messages – as the Care-of Route setup (described in section 6.3.2.1). The first token, called *Care-of keygen token*, is sent piggybacked in the CoRTI message, plus a *Care-of cookie*, and the index of the nonce used to generate the token. The correspondent MR replies in the CoRT message, including its own Care-of keygen token, its nonce index and copying the cookie received in the CoRTI message.

- The second token, called *Home keygen token*, is sent, plus a *Home cookie* and a nonce index, in a separate message, called *Home Route Test* (HoRT), through the MRHA tunnel (protected by IPsec ESP in tunnel mode) configured by the NEMO Basic Support, using the routing infrastructure. In order to verify that the correspondent MR is actually managing the IPv6 network prefix it claims to, that is, the Mobile Network Prefix assigned to the NEMO, the HoRT message is sent to a random address within the MNP. The MR that manages the prefix has to intercept[5] that message therefore showing that it actually manages the MNP[6]. The Mobile Network Prefix length used by VARON MRs is fixed to 64 bits (/64), in order to avoid a malicious node to “steal” a prefix. Otherwise, for instance, if a MR was assigned a /64 prefix, then with probability $1/2$ it could try to spoof a /63 prefix (and steal its ”*neighbours*” packets). By fixing the MNP length, this attack is no longer feasible.

[4] Note that these nonces are different from the ones used during the ad-hoc route discovery and setup procedure.

[5] It is not required the MR to continuously examine every received packet in order to intercept HoRT messages. The MR may start inspecting packets after sending (or receiving) a CoRT message.

[6] This test does not guarantee that a node manages a certain prefix, but that this node is at least in the path toward that prefix. This provides the solution with a similar security level that today’s IPv4 Internet has.

As in the case of the Care-of Route test, the correspondent MR replies this message with another HoRT message, including its own Home keygen token and nonce index and copying the received cookie.

- Each MR uses the received Home and Care-of keygen tokens to create a key, K_{bm} that can be used to authenticate a *Mobile Network Prefix Binding Update* (MNPBU) message[7] – sent along the Care-of Route –, that enables the other MR to check that the Mobile Network (MNP) reachable through the VANET (Care-of Route) is the one reachable through the infrastructure. This verification can be done because each MR has the information required to produce the key when the MNPBU is received, and therefore authenticate the message.

At this point VARON signalling has finished. MR A has found out that MR B – which owns HoA_B and its associated private key – that is reachable through the VANET, is also capable of receiving and sending packets sent to any address from the Mobile Network Prefix (MNP) B through the infrastructure. This only happens if the HA responsible of routing packets addressed to this MNP (that is, HA B) is forwarding to MR B those packets addressed to MNP B. HA B only would be doing that if proper authentication has taken place and MR B is authorised to manage MNP B. The same guarantee also holds for MR B regarding MNP A and MR A.

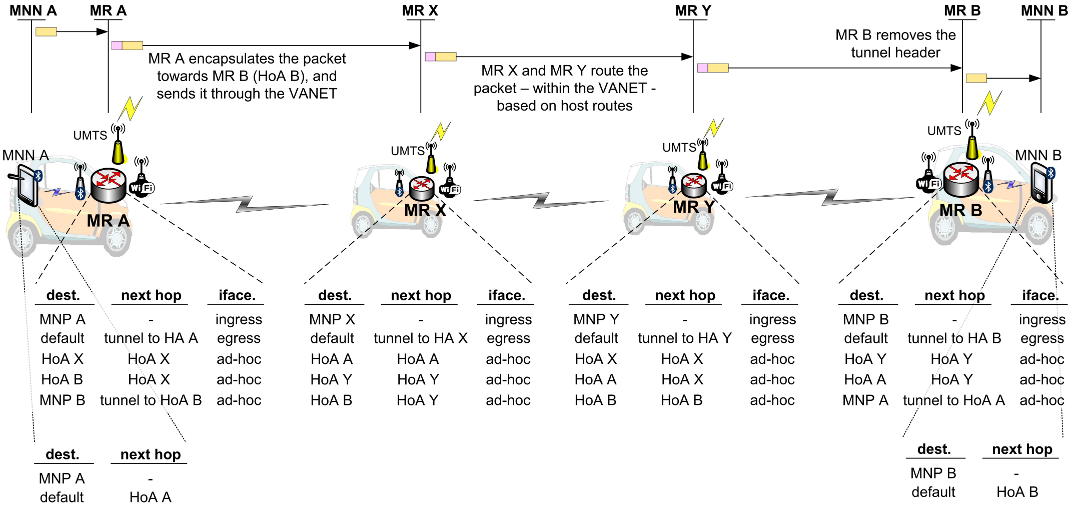
The Care-of Route authentication mechanism performed in VARON, as the Return Routability procedure defined in Mobile IPv6, implicitly assumes that the routing infrastructure is secure and trusted. As long as this is true, the mechanism defined is appropriate to secure the Mobile Network Prefix Binding Update, since it does not introduce any new vulnerability that was not possible in today's IPv4 Internet.

After this process is completed, the end-point MRs (MR A and MR B) may exchange traffic using the set-up Care-of Route within the VANET.

6.3.2.3. Optimised routing using the VANET

Once the Care-of Route authentication procedure has finished, all MRs involved in the creation of the ad-hoc route can forward packets to the HoAs of the end-point MRs (see an example in Figure 6.6). However, only the end-point MRs have verified the association of the corresponding MR' HoA and the respective MNP. Intermediate MRs (i.e. MR X and MR Y in the example) have only learnt host routes towards the Home Addresses of the two end-point MRs (i.e. HoA_A and HoA_B). In order to route data traffic between cars' nodes with addresses belonging to MNP A and MNP B, each end-point has to tunnel the packets towards the other MR's HoA, through the VANET route. In this way, intermediate MRs in the ad-hoc route just forward the packets based on the host routes (with the end-point MRs' HoAs as destination) added to their routing tables during the ad-hoc Care-of Route creation process (see Figure 6.6).

[7] The generation of this key (K_{bm}) and the keygen tokens, and the authentication of the message follows the same mechanism that the Return Routability procedure [JPA04], [NAA$^+$05] and the proposal to extend it to support network prefixes [NH04a]. The interested reader may refer to [JPA04], [NAA$^+$05] and Appendix B for additional information.


MNN A
MR A
MR X
MR Y
MR B
MNN B
MR A encapsulates the packet towards MR B (HoA B), and sends it through the VANET
MR X and MR Y route the packet – within the VANET - based on host routes
MR B removes the tunnel header
UMTS
UMTS
UMTS
UMTS
MNN A
MNN B
MR A
MR X
MR Y
MR B

dest.	next hop	iface.
MNP A	-	ingress
default	tunnel to HA A	egress
HoA X	HoA X	ad-hoc
HoA B	HoA X	ad-hoc
MNP B	tunnel to HoA B	ad-hoc

dest.	next hop	iface.
MNP X	-	ingress
default	tunnel to HA X	egress
HoA A	HoA A	ad-hoc
HoA Y	HoA Y	ad-hoc
HoA B	HoA Y	ad-hoc

dest.	next hop	iface.
MNP Y	-	ingress
default	tunnel to HA Y	egress
HoA X	HoA X	ad-hoc
HoA A	HoA X	ad-hoc
HoA B	HoA B	ad-hoc

dest.	next hop	iface.
MNP B	-	ingress
default	tunnel to HA B	egress
HoA Y	HoA Y	ad-hoc
HoA A	HoA Y	ad-hoc
MNP A	tunnel to HoA A	ad-hoc

dest.	next hop
MNP A	-
default	HoA A

dest.	next hop
MNP B	-
default	HoA B

Figure 6.6: Overview of packet routing within the VANET.

The Care-of Route discovery and validation signalling is repeated periodically, both to refresh the ad-hoc routes and to avoid time-shifting attacks. If an ad-hoc route becomes invalid (for example, because it expires) or it is broken, and traffic is received through this route, a *Care-of Route Error* (CoRE) message is sent (and forwarded) by each MR in the path to the source MR. For example, if intermediate MR Y in Figure 6.6 receives data traffic from MR A addressed to MR B and the link between MR Y and the next hop towards MR B (in this case, MR B itself) is broken, then MR Y sends a CoRE message to the next MR along the path towards the source MR (MR A), which is MR X, indicating that there is a problem with this Care-of Route:

$$\begin{array}{l} Y \rightarrow X : \\ [CoRE, HoA_A, HoA_B, N_Y, K_{Y+}]_{K_{Y-}} \end{array}$$

This message is received by MR X, which after verifying the authenticity of the received CoRE, signs the message, adds its public key K_{X+} and the signature to the message (as performed by intermediate MRs when processing and forwarding CoRTI and CoRT messages) and sends it to the next hop towards MR A.

$$\begin{array}{l} Y \rightarrow X : \\ \Big[[CoRE, HoA_A, HoA_B, N_Y, K_{Y+}]_{K_{Y-}}, K_{X+}\Big]_{K_{X-}} \end{array}$$

Upon reception of this error message, the source MR (MR A in the example) switches to use the Home Route for sending packets and it may start a new route discovery procedure to set-up a new optimised Care-of Route within the VANET. To avoid DoS attacks, a CoRE message indicating that a route has become invalid is only processed by a MR if the neighbour that is forwarding the message is the next hop of this route. Otherwise, malicious nodes would be able to set as invalid any Care-of Route.

There exist several possible mechanisms that can be used to detect that a Care-of Route is no longer working. As an example, Mobile Routers may check if the data packets forwarded within the VANET have been correctly received by the next hop making use of link layer acknowledgement frames (if the MAC layer supports that). If several data frames have not been acknowledged, this may be used as an indication that the next hop is no longer reachable and therefore the Care-of Route is broken.

6.4. Validation and evaluation of the proposed solution

This section presents a validation and evaluation of VARON. This includes a security analysis, where it is explained how VARON deals with the different attacks introduced in Section 6.2. It is also analysed how to improve the performance of the protocol – in terms of complexity – by means of the use of alternative authentication schemes. Last but not least, an extensive simulation study is included, in order to evaluate the performance of the solution, as well as comparing VARON to the use of plain Network Mobility Basic support and a generic Route Optimisation support (MIRON).

6.4.1. Security analysis

6.4.1.1. Robustness against attacks

This section provides a security analysis of VARON, by evaluating its robustness against the attacks introduced in Section 6.2.

A malicious node M could attempt several attacks to this scheme. Basically, there are two main types of attacks: those that try to modify the routing in the VANET (Ad-hoc routing attacks), and those that try to steal a prefix (Prefix ownership attacks). In order to modify the ad-hoc routing, an attacker out of the routing path could try to alter or fabricate routing messages. Such a kind of attack is not feasible because all routing messages are cryptographically signed. An additional attack could be to try to impersonate a legitimate node (spoofing its IP address), but this is not possible either, since the authenticity of a message is guaranteed by the use of CGAs and public key cryptography. Two possible examples of these attacks are described next.

A malicious node M can try to change an already established ad-hoc route by sending a CoRTI message to a MR X that belongs to this multi-hop route, claiming that M can reach a certain MR A. But MR X will not accept the message if it cannot validate it with the public key corresponding to the HoA of MR A associated with the route. Because M cannot create that part of the CoRTI message, it can try to copy it from a real CoRTI message previously sent by MR A, but the nonce included will not be greater than the one stored in MR X that is associated with the route. Notice that a legitimate update of the route by MR A is allowed because it knows its own private key and the nonce that must be included in the CoRTI message.

A malicious node M that receives a CoRTI message from a MR A could try to claim to a neighbour MR X that it is MR Z and not M (when sending the CoRTI message towards MR B). If MR Z is a legitimate network node, this could mean that afterwards all the traffic will be sent to it (DoS attack). But M will not be able to do that because it has not the private key associated with the HoA that MR Z is using.

One example of an attack based on spoofing a prefix will be as follows. A malicious node M could create a HoA belonging to the MNP managed by a legitimate MR A. The node M can create the HoA belonging to the MNP of MR A using its own public key so it can prove to other nodes that it has the private key corresponding to that address. However, the Home Route Test will fail, so it cannot make another MR send to it the traffic addressed to the MNP of MR A. In this situation, the node M can set-up an ad-hoc route for its HoA (using its own private key), since the routes created in the VANET only define the forwarding of packets addressed to MRs' HoAs (see Figure 6.6). Therefore, different routes for HoAs belonging to the same prefix could coexist (although only one at most will belong to non-malicious nodes). However, only legitimate end-point MRs will success in performing the Home Route Test and, therefore, will be able to generate and send a valid MNPBU (enabling the use of the Care-of Route).

There are some vulnerabilities and attacks that are still possible, resulting from the inherent nature of ad-hoc networks, such as certain Denial-of Service (DoS) – e.g., based on non-collaborating nodes – or route discovery flooding attacks. But, notice that VARON nodes can always revert communications to the Home Route in case of the Care-of Route is no longer working.

6.4.1.2. Complexity of the solution and alternative approaches

The security that VARON provides is mainly based on the use of public key cryptography and CGAs. By hop-by-hop signing all the routing messages, modification and fabrication attacks are very hard to perform. The use of CGAs makes very difficult to perform impersonation attacks, since an attacker would need to find a private/public key pair that produces the same address that the node to be impersonated has. Depending on the degree of security that is selected, the cost of performing a brute-force attack varies from $O(2^{59})$ to $O(2^{171})$. This is achieved by using the *Sec* parameter in the generation of the CGA [Aur03], [AAK$^+$02], [Aur05]. This parameter allows to increase the cost of performing a brute-force attack, but it also increases the cost of generating the CGA itself. A useful analysis on the complexity and robustness of CGAs can be found in [Aur03].

VARON security does not come for free, the use of public key cryptography has an important cost, not only in terms of energy consumption (this effect is relatively less important in vehicular environments, where nodes have a powerful and rechargeable source of energy), but also in terms of computational capacity. This may have an impact on the performance of the protocol, since every node has to make several computational operations during the processing of VARON signalling packets, which take some time. The evaluation of how long is this time is one of the key aspects that will be analysed later in Section 6.4.2.

Since the complexity of VARON regarding security is not negligible, it is important to evaluate alternative approaches addressing the same requirements that the combined use of public key cryptography combined with CGAs do (that is, the mitigation of the security attacks described in Section 6.2), but with a lower complexity. The use of *hash-chains* [Lam81], [HPT97] has been considered for the provision of authentication in different situations, because of their lower computational cost compared to public key cryptography. Next, an evaluation of how hash chains could be used in VARON is presented.

Basically, a hash chain $h^1(x), \cdots, h^i(x), \cdots, h^n(x)$ of length n is formed from a bit string x as follows: $h^0(x) = x$ and $h^i(x) = h(h^{i-1}(x))$ for $i = 1, \cdots, n$, where h can be any hash function, such as MD5 or SHA. Due to the properties of hash functions, given

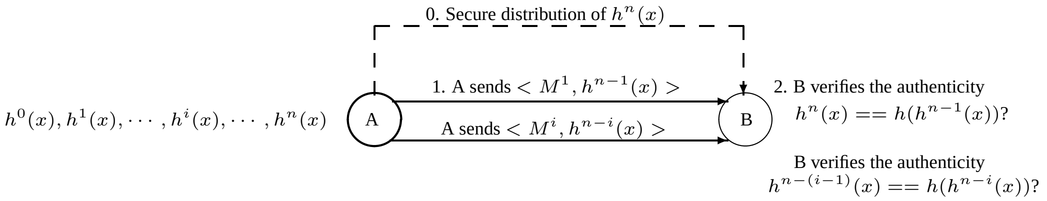

0. Secure distribution of $h^n(x)$
$h^0(x), h^1(x), \cdots, h^i(x), \cdots, h^n(x)$
A
1. A sends $< M^1, h^{n-1}(x) >$
A sends $< M^i, h^{n-i}(x) >$
B
2. B verifies the authenticity
$h^n(x) == h(h^{n-1}(x))$?
B verifies the authenticity
$h^{n-(i-1)}(x) == h(h^{n-i}(x))$?

Figure 6.7: Example of the use of hash-chains to authenticate messages.

$h^i(x)$ it is not easy to guess $h^{i-1}(x)$ and this can be used to provide authentication in network protocols.

Figure 6.7 illustrates an example of the use of hash chains to authenticate messages. Node A generates a hash chain $h^1(x), \cdots, h^i(x), \cdots, h^n(x)$ of length n. The last element of the chain $h^n(x)$ is distributed securely (usually, this is done using public key cryptography) to B. After that, A adds to the next message sent M^1 the following element of the hash chain $h^{n-1}(x)$. This enables B to check the authenticity of that message by just computing $h' = h(h^{n-1}(x))$. If $h' = h^n(x)$, then B has certain guarantees that A is the sender of that message. For subsequent messages, A adds to the messages the next values in the hash chain, that is, for M^2, it includes $h^{n-2}(x)$; for M^i, it includes $h^{n-i}(x)$, etc. It should be noted that using this mechanism, a hash-chain of length n can be used to authenticate at most n messages.

It may be argued that VARON could achieve a similar degree of security by making use of hash-chains instead of public-key cryptography. There are however certain aspects that may discourage the use of this approach:

- Hash-chains can be efficiently used to provide *authentication*, and this could be used in VARON for example to authenticate the originator and target MRs in the Care-of Route set-up procedure – $h^n(x)$ could be securely distributed using the infrastructure (i.e. Home Route). However, this scheme does not seem suitable for the authentication of intermediate MRs, as it would require using the Home Route to communicate with them as well (and this should be avoided, since using the egress interface usually has a higher cost than using the ad-hoc interface).

- Schemes using hash-chains as the one described in the previous example do not provide message *integrity*. Integrity is required by VARON in order to avoid a malicious node to perform modification attacks. There are schemes, such as Chained One-time Signature Protocol (COSP) [Zha98], that allow to use hash-chains to sign messages. However this scheme has the problem that it requires the distribution of hash-chains among the involved nodes, which is inefficient (and maybe even unfeasible) in highly dynamic scenarios, such as the vehicular one. Other proposals, such as Independent One-time Signature Protocol (IOSP) [Zha98] solve partially this problem, but on the other hand, are not tolerant of unreliable packet delivery (if a packet is lost, involved nodes have to re-setup).

Based on the previous rationale, it seems that completely removing the use of public key cryptography in VARON is not possible if it is required to avoid all the attacks described in

Section 6.2. Nevertheless, it seems very interesting to study and analyse the use of combined approaches of hash-chains, public-key cryptography and CGAs to improve the performance of the protocol. It seems possible, for example, to benefit from using hash-chains in certain phases of the protocol instead of public-key cryptography to reduce the computational cost (e.g., after an initial secure exchange using public-key cryptography). It is required to carefully analyse how and under which circumstances this could be done without impacting the security and performance of the protocol, but this is left as a future research issue for the purpose of this PhD thesis.

6.4.2. Performance evaluation

In this section, the performance of VARON is evaluated using measurements obtained through simulation and experimental evaluation of several parts of the protocol.

6.4.2.1. Computational cost

Each VARON Mobile Router must perform several cryptographic operations (such as signing and verifying signatures) on each signalling message along a Care-of Route. These cryptographic operations are relatively expensive, especially when compared to the operation of the NEMO Basic Support protocol and other (insecure) ad hoc routing protocols, that do very little (almost negligible) computation per signalling message. However, it is important to note that only the routing control messages that make the state of the MR change or the MR perform an action (e.g., modifying the routing table, forwarding a message, etc.) are subject to signing/verifying. The signature of those routing messages that are discarded (e.g., because they have been already processed and are received again forwarded by a different MR) is not verified. Data packets exchanged between nodes after a route has been set up are not processed by VARON either.

In order to evaluate the computational cost of VARON, several tests were conducted, measuring the raw processing time per VARON routing packet for different key sizes. These results have been used as input to the simulations of VARON in large and complex scenarios.

The raw processing time expended by a MR on a VARON control packet includes the verification of the CGA of the originator MR (and the forwarder of the message in case this has been forwarded by an intermediate MR), the verification of the signature of the originator MR (and the forwarder of the message in case this has been forwarded) and, if a new message has to be sent (e.g., forwarding of a CoRTI/CoRT or generation of a CoRT message), the computation of the signatures to be added to this new message. These measurements were conducted by mirroring the sequence of function calls that are performed when a VARON routing message is received, but without considering the time spent performing operations on the state that is maintained by a VARON MR (such as looking through the VARON and IP routing tables, e.g., to check whether a routing message has been already received or not). This simplified the test, focusing on the time spent on the cryptographic operations instead of state maintenance, which is negligible in comparison.

The cryptographic functions were implemented making use of the OpenSSL Library[8], which provides functions for general purpose cryptographic tasks such as public and private

[8] `http://www.openssl.org/`

Figure 6.8: Linksys WRT54GS router.

key encryption/decryption and signature creation/verification.

In order to evaluate the cost of processing VARON routing messages, these tests were conducted in two different types of devices that are likely to play the role of a vehicular Mobile Router:

- A Linksys WRT54GS router, which is a small home and office broadband router (see Figure 6.8), equipped with a 200 Mhz processor, an IEEE 802.11g WLAN interface and an IEEE 802.3 Ethernet interface connected to a VLAN capable 5-port switch. This is a very popular low-cost router (less than 75€ as of the time of writing this document), which seems to be a very good candidate for hosting Mobile Router's software, since its firmware is released under the GNU GPL and can be easily modified. For these tests, the open source *OpenWRT*[9] WhiteRussian RC 3 distribution was used in the Linksys Router.

- An Intel Core-duo 2.0 Ghz with 2 GB RAM laptop, running *Linux Debian etch*. This is a more powerful machine than the Linksys router, but still portable. It is expected that hardware configurations similar to the one of this laptop will be found in vehicles in the near future. Therefore, this machine is a good example of hardware that may host a Mobile Router implementation in a few years.

Tables 6.2 and 6.3 show the obtained results. Next, an explanation of what was measured is provided:

- *CoRTI 1:* time spent by an originator MR to generate a CoRTI message. This basically requires to perform a signature operation.

- *CoRTI 2:* time spent by an intermediate MR to process a CoRTI message sent by an originator MR (and that has not been forwarded by any intermediate MR) that

[9] `http://www.openwrt.org/`

RSA key	Average (ms) ± Std. Dev.				
size (bits)	CoRTI 1	CoRTI 2	CoRTI 3	CoRTI 4	CoRTI 5
Laptop					
512	2.36 ± 0.09	3.35 ± 0.19	3.72 ± 0.31	3.27 ± 0.18	3.71 ± 0.22
768	5.09 ± 0.16	6.12 ± 0.43	6.67 ± 0.18	6.13 ± 0.26	6.67 ± 0.32
1024	12.03 ± 0.27	13.40 ± 0.43	14.35 ± 0.40	13.47 ± 0.28	14.46 ± 0.72
Linksys					
512	45.90 ± 0.37	70.56 ± 0.31	81.57 ± 0.32	70.80 ± 1.88	83.78 ± 2.55
768	79.86 ± 0.78	107.44 ± 1.55	120.36 ± 1.87	107.29 ± 1.90	121.32 ± 2.02
1024	136.61 ± 0.41	164.86 ± 0.50	179.20 ± 0.44	164.66 ± 0.38	179.37 ± 0.64

Table 6.2: Raw time required to process VARON signalling packets (CoRTI).

RSA key	Average (ms) ± Std. Dev.			
size (bits)	CoRT 1	CoRT 2	CoRT 3	CoRT 4
Laptop				
512	3.32 ± 0.31	3.64 ± 0.12	0.87 ± 0.04	1.30 ± 0.12
768	6.30 ± 1.31	6.72 ± 0.27	0.98 ± 0.03	1.57 ± 0.39
1024	13.46 ± 0.36	14.49 ± 0.37	1.48 ± 0.15	2.13 ± 0.14
Linksys				
512	70.55 ± 0.34	84.66 ± 2.63	25.72 ± 0.97	36.84 ± 1.25
768	106.81 ± 1.82	117.94 ± 0.37	26.07 ± 0.27	39.72 ± 1.55
1024	164.77 ± 0.48	179.19 ± 0.47	28.06 ± 0.10	42.54 ± 0.15

Table 6.3: Raw time required to process VARON signalling packets (CoRT).

is then forwarded. This processing consists of the verification of the signature of the received CoRTI message, and the generation of a new CoRTI message to be forwarded (this requires the computation of a signature). The CGA of the originator MR is also checked (this requires to perform two hash operations).

- *CoRTI 3:* time spent by an intermediate MR to process a CoRTI message – forwarded by another intermediate MR – that is then forwarded again. This processing consists of the verification of the signatures of the received CoRTI message (this message is signed by the originator MR and the MR that has forwarded it), and the generation of a new CoRTI message (this requires the computation of a signature) to be forwarded. The CGAs of the originator and forwarder MRs have to be checked as well.

- *CoRTI 4:* time spent by a target MR to process a received CoRTI message – forwarded by an intermediate MR – and generate a CoRT message. This processing consists of the verification of the signatures of the received CoRTI message and the generation of the signature to be included in the new CoRT message. The CGAs of the originator and forwarder MRs have to be checked as well.

- *CoRTI 5:* time spent by a target MR to process a received CoRTI message sent by an originator MR (and that has not been forwarded by any intermediate MR). This consists of the verification of the signature of the received CoRTI message and the generation of the signature to be included in the new CoRT message. The CGA of the originator MR has to be checked as well.

- *CoRT 1:* time spent by an intermediate MR to process a received CoRT message sent by a target MR (and that has not been forwarded by any intermediate MR) and generate a new CoRT message to be forwarded. This processing consists of the verification of the signature of the received CoRT and the generation of the signature to be included in the new CoRT message. The CGA of the target MR has to be checked as well.

- *CoRT 2:* time spent by an intermediate MR to process a received CoRT message – forwarded by another intermediate MR – and generate a new CoRT message to be forwarded. This consists of the verification of the two signatures included in the received message and the computation of the signature to be added to the new CoRT message. The CGAs of the target and forwarder MRs have to be checked as well.

- *CoRT 3:* time spent by an originator MR to process a received CoRT message sent by a target MR (and that has not been forwarded by any intermediate MR). This processing consists of the verification of the signature included in the received message and the verification of the CGA of the target MR.

- *CoRT 4:* time spent by an originator MR to process a received CoRT message forwarded by an intermediate MR. This processing consists of the verification of two signatures and CGAs (of the target and forwarder MRs).

- *CoRE 1:* time spent by a MR that detects a problem in a Care-of Route to generate a CoRE message. This basically requires to perform a signature operation. This time is the same than *CoRTI 1*, since the sizes of the fields and the cryptographic operations needed are the same.

- *CoRE 2:* time spent by an intermediate MR to process a CoRE message sent by a MR (and that has not been forwarded by any intermediate MR) that is then forwarded. This processing consists of the verification of the signature of the received CoRE message, and the generation of a new CoRE message to be forwarded (this requires the computation of a signature). The CGA of the source MR is also checked. This time is the same that *CoRTI 2*, since the sizes of the fields and the cryptographic operations needed are the same.

- *CoRE 3:* time spent by an intermediate MR to process a CoRE message forwarded by another intermediate MR, than is then forwarded again. This processing consists of the verification of the signatures of the received CoRE message (this message is signed by the source and forwarder MRs), and the generation of a new CoRE message (this requires the computation of a signature) to be forwarded. The CGAs of the source and forwarder MR have to be checked as well. This time is the same that *CoRTI 3*, since the sizes of the fields and the cryptographic operations needed are the same.

- *CoRE 4:* time spent by a destination MR to process a received CoRE message sent by a MR (and that has not been forwarded by any intermediate MR). This processing consists of the verification of the signature included in the received message and the verification of the CGA of the source MR. This time is the same that *CoRT 3*, since the sizes of the fields and the cryptographic operations needed are the same.

- *CoRE 5:* time spent by a destination MR to process a received CoRE message forwarded by an intermediate MR. This processing consists of the verification of two signatures and CGAs (of the source and forwarder MRs). This time is the same that *CoRT 4*, since the sizes of the fields and the cryptographic operations needed are the same.

The processing time for the laptop and the Linksys router were measured over three different RSA key sizes: 512, 768, and 1024 bits. For both devices, an increase in the key size of 256 bits results in approximately doubling the processing time. It is also interesting, although not very surprising, the difference in processing times between the laptop and the Linksys router. For each key size, the processing time is between 10 and 20 times slower on the router than on the laptop. As of the day of writing this PhD thesis, it is more likely that devices deployed in vehicles will be similar (in terms of processing power) to the Linksys router. Therefore, only the values obtained for the Linksys router for the 1024-bit RSA key have been used as input to the simulations. This will provide us with more realistic results (that can be considered as a lower bound on the performance if more powerful devices were used instead).

6.4.2.2. Simulation of VARON

In order to complete our discussion about the proposed solution, an extensive simulation study was performed. Besides analysing the performance and costs of VARON, the value of some metrics using VARON are compared to the ones obtained when plain NEMO Basic Support protocol [DWPT05] or MIRON [CBB$^+$06] (as an example of a non ad-hoc Route Optimisation for NEMO) were used.

We performed our simulations using OPNET[10]. We simulated 50 vehicles within a road. Each vehicular MR is equipped, in addition to the ingress interface (to provide connectivity to the vehicular devices), with an emulated UMTS egress interface (1 Mbps, 150 ms of average one-way delay) and an IEEE 802.11 (WLAN) interface (2 Mbps, transmission power of 1 mW, receiver sensitivity of -95 dBm) in ad-hoc mode. The UMTS interface has been emulated because OPNET UMTS models did not properly support IPv6 as the time of performing the simulations of this PhD thesis. The UMTS channel has been modelled using a 1 Mbps WLAN 802.11b network, with an additional delay of 150 ms per way. The link delay has been chosen based on previous practical measurements [MdlOS$^+$06], [OMV$^+$06], [VBS$^+$06]. In order to achieve global coverage, the transmission power of the WLAN nodes (MRs and the Access Point) that emulates the UMTS was set to 1 W. Considering the kind of analysis that we were interested in performing, this set-up provided us with model of a UMTS network good enough.

The UMTS interface provides continuous Internet connectivity, whereas the WLAN interface enables forming multi-hop vehicular ad-hoc networks. UMTS and WLAN were chosen for the simulations because they are probably the most realistic candidate access

[10] OPNET University Program, `http://www.opnet.com/services/university/`

technologies for a vehicular communication scenario nowadays. However, different technologies may also be used by VARON (e.g., IEEE 802.16e WiMAX for the MR's egress interface), since the protocol is independent of the access technology used by the Mobile Router.

In order to evaluate the worst case scenario, VARON was simulated using 1024 bit RSA keys and the processing time shown in Tables 6.2 and 6.3 for the Linksys router as input for the simulations. All the VARON protocol, but the detection of broken links and the generation of CoRE messages, was implemented using the OPNET simulator[11]. By not implementing the detection of broken routes, a Care-of Route entry can only be removed from the IP routing table of a MR when it expires. Hence, it may happen that a MR tries to use a broken Care-of Route for some time (until it expires), since MRs along the path are not able to detect a broken route and therefore they do not send any CoRE message to the source MR – that would make it stop sending the traffic through the VANET and revert to use the Home Route. Thus, VARON performance obtained from the simulation results is worse than the one that would be obtained if the protocol were completely implemented.

In addition to the values of the timers used to refresh a Care-of Route, the protocol has a few parameters that can be configured. A description of these parameters and the values used in the simulations is included next:

- `VARONC_CORTI_TTL_MAX.` This is the maximum number of hops that a CoRTI message can traverse before being silently discarded. Each time a MR forwards a received CoRTI message, it decrements the TTL value of the packet by one. If the received packet has a TTL = 1, then it is not forwarded. Therefore, this value represents the flooding ratio of CoRTI messages. A default value of 10 hops was used in the simulations, since higher values would involve quite unstable routes with short useful lifetimes.

- `VARONC_HOAA_TTL_MAX.` This is the maximum number of hops that a HoAA message can traverse (the flooding ratio of this type of message) before being discarded. As for the CoRTI message, a default value of 10 hops was used in the simulations for this parameter. A random delay uniformly distributed between 0 and 1 second was added before forwarding a HoAA message in order to minimise collisions. This random delay was introduced because it was observed that the performance when HoAA messages were forwarded immediately after their reception was quite poor. This is related to the 802.11 MAC protocol, which does not perform a ready-to-send/clear-to-send (RTS/CTS) exchange for broadcast packets, and therefore does not prevent high probabilities of collision of broadcast packets from appearing in relatively dense networks such as the simulated one (50 nodes).

- `VARONC_HOAA_INTERVAL.` This is the average time between sending periodic HoAA messages. In the simulations a uniform distribution between 18 and 22 seconds (i.e. a mean value of 20 seconds) was used to minimise collisions.

- `VARONC_HOAA_LIFETIME.` This is the value of the *lifetime* field of the HoAA messages (see Appendix B.9). The default value used in the simulations was 20 seconds.

[11] VARON model has approximately 10000 lines of code.

- `VARONC_EXPIRY_TIMEOUT`. This is the amount of time elapsed since a Care-of Route entry is created until it is marked as *expired*. This expiration triggers the Care-of Route set-up process to be re-done to refresh the route. A value of 20 seconds was used in the simulations, since it is a good tradeoff between sending so much signalling overhead and being responsive enough to changes in the VANET topology due to vehicular mobility (since the detection of broken links and CoRE signalling was not implemented in the simulated model of VARON). This value was chosen after performing several sets of simulations aimed at finding a good value for this parameter.

- `VARONC_INVALID_TIMEOUT`. This is the amount of time that elapses since a Care-of Route entry is created until it is removed from the IP routing table. It is equal to `VARONC_EXPIRY_TIMEOUT` plus 10 seconds (that is, 30 seconds). This value was chosen so there is time enough to perform the Care-of Route discovery procedure once a route is marked as expired and before the route is deleted from the IP routing table (measurements showed that this time was always less than 10 seconds with the configured flooding ratio).

In order to evaluate the performance of VARON under different real-case scenarios, VARON experiments were performed varying the following two parameters:

a) *Vehicle speed.* Different simulations were run for average vehicle speeds of 1, 5, 10, 20, 40, 50, 70, 90, 100 and 120[12] km/h. The speed of a node is a random variable, uniformly distributed between $0.9v$ and $1.1v$, where v is one of the previous mean speed values. Therefore, in each simulation, nodes have different speeds, but still very similar. This represents real life scenarios, such as vehicles in a city or motorway, where the relative speed of vehicles moving in the same direction is low.

b) *Initial vehicle density.* Different simulations were run for initial vehicle densities of 200, 100, 50, 25, 20, 13.33, 10, 8, 6.67, 5, 4 and 3.33 vehicles/km[13].

For each combination of the previous parameters, thirty different simulations were performed, changing the speeds and initial positions of the vehicles, as well as the seed of the random number generator of the simulator. The following metrics were evaluated:

1. **Average end-to-end throughput.** This is the mean TCP throughput obtained when performing bulk file transfers. This evaluates the improvement in terms of throughput obtained when using VARON, as well as the possible effects that the use of VARON may have in TCP (e.g., due to the Home ↔ Care-of Route handovers).

2. **Average end-to-end delay of data packets.** This is the average time between the sending of a data packet by a vehicle and its receipt by another. This includes all the delays caused because of buffering and processing at intermediate nodes, and retransmission delays at the MAC layer. The route acquisition latency (see below) does not

[12] The maximum speed limit in Spain is 120 km/h.

[13] This means that at the beginning of each simulation, the 50 nodes were uniformly distributed within a road of a length of 0.25, 0.5, 1, 2, 2.5, 3.75, 5, 6.25, 7.5, 10, 12.5 and 15 km, respectively, and then they started to move at their respective speeds.

impact the end-to-end delay, since packets are sent through the Home Route while a Care-of Route is being set-up.

3. **Average end-to-end jitter of data packets.** This is the average variation of the delay (*jitter*) between the sending of a data packet by a vehicle and its receipt by another.

4. **Average Care-of Route acquisition latency.** This is the average delay between the sending of a Care-of Route Test Init packet by an originator MR for discovering and establishing a Care-of Route to a target MR, and the receipt of the Mobile Network Prefix Binding Update message that makes the MR add a Care-of Route entry to its IP routing table. This includes the delays of the signalling messages sent through the VANET (CoRTI, CoRT and MNPBU), the processing time due to the cryptographic operations performed on each routing message and the delay due to the use of the infrastructure (Home Route) to send HoRT messages.

5. **Average Care-of Route length.** This is the average length of the Care-of Route discovered and set-up by VARON. It is calculated by averaging the number of hops taken by MNPBU messages to reach their destination (the path followed by a MNPBU message is the same that the one that data packets sent through the VANET would follow afterwards).

6. **Average frequency of route changes.** This is the average number of Home ↔ Care-of Route changes per minute. This evaluates the stability of the Care-of routes discovered by VARON.

7. **Average Care-of Route data packet fraction.** This is the fraction of delivered data packets that are sent through a Care-of Route. This evaluates the fraction of data traffic that is actually forwarded through an optimised route, and therefore the likelihood of using VARON to optimise a traffic communication between two vehicles that are relatively close each other.

8. **Average VARON signalling load (bytes).** This is the ratio of overhead bytes to delivered data bytes using a Care-of Route. This metric was measured counting the amount of VARON signalling bytes received at a Mobile Router and the amount of data bytes received through the Care-of Route (data packets received through the Home Route were not taken into account for this calculation).

9. **Average VARON signalling load (packets).** Similar to the previous metric, but a ratio of signalling packet to data packet overhead.

On each simulation only two nodes out of the 50 were communicating each other. Simulations involving more nodes communicating simultaneously were also performed to validate the correct operation of the solution. The throughput and signalling load metrics were obtained simulating a scenario in which a 2 MByte file is transferred from a vehicle to another, using FTP. For the rest of the metrics, the scenario consisted of a UDP VoIP flow (GSM, 24.2 kbps, 50 packets per second) sent from a vehicle to another.

To simulate the delay added by the use of the NEMO Basic Support protocol [DWPT05] and the traversal of the respective Home Networks of the involved vehicles, an additional

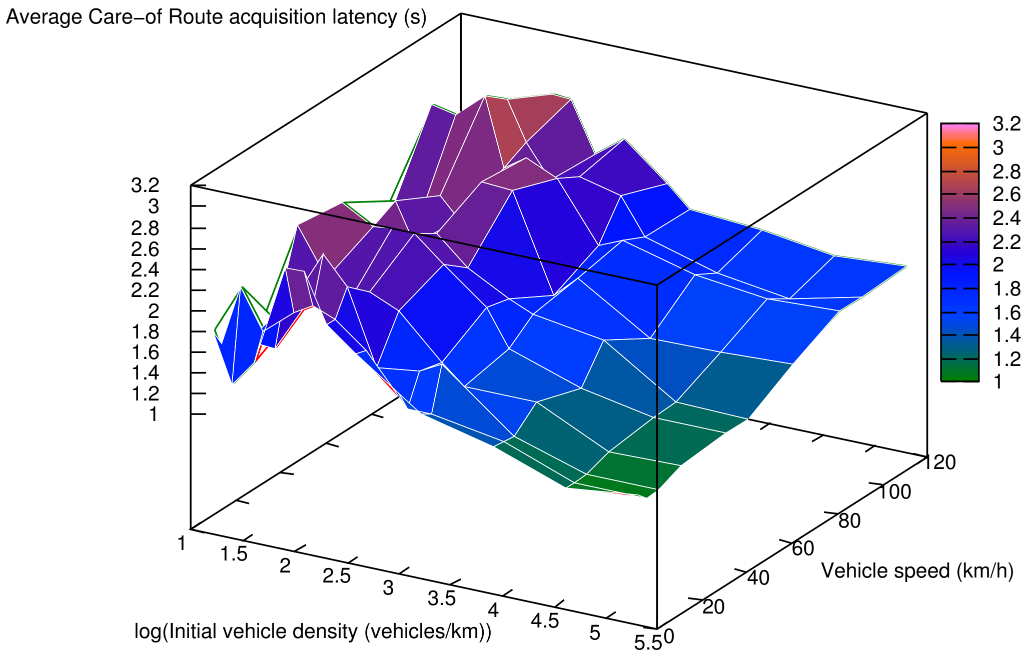


Figure 6.9: Average Care-of Route acquisition latency.

delay (one-way) of 36 ms was introduced in the infrastructure network. This additional latency represents the delay required to go through two Home Networks located in Europe (the value was chosen based on real RTT measurements[14] obtained from the PingER project [MC00a]).

6.4.2.3. Simulation results

Simulation results are presented next in Figures 6.9-6.18. Results are plotted using three-dimensional graphs, so the impact of the vehicle density and speed on each of the simulated metrics can be easily evaluated. Each data point is an average of thirty simulations run with different randomly generated mobility patterns (but following the considerations described above about speed and movement within a road).

Figure 6.9 shows the average route acquisition latency, that is the time taken by VARON to find and set-up a Care-of Route. VARON requires each MR along the path to perform several cryptographic operations when processing a control packet, such as the verification and generation of digital signatures and CGAs. This is computationally demanding and therefore adds additional delay to the overall route acquisition time. Another source of latency in the route acquisition time is the use of the infrastructure network (i.e. Home Route) in the Care-of Route validation process, that causes an additional delay – equal to the sum of the RTTs of each MR to its respective HA – in the Care-of Route discovery time. Therefore, the route acquisition time is higher in VARON than in other ad-hoc routing protocols, although in VARON this time does not have a direct impact on the performance, as data traffic delivery is guaranteed by the use of the Home Route. Since an important contribution to the overall

[14] Available at `http://www-iepm.slac.stanford.edu/pinger/`

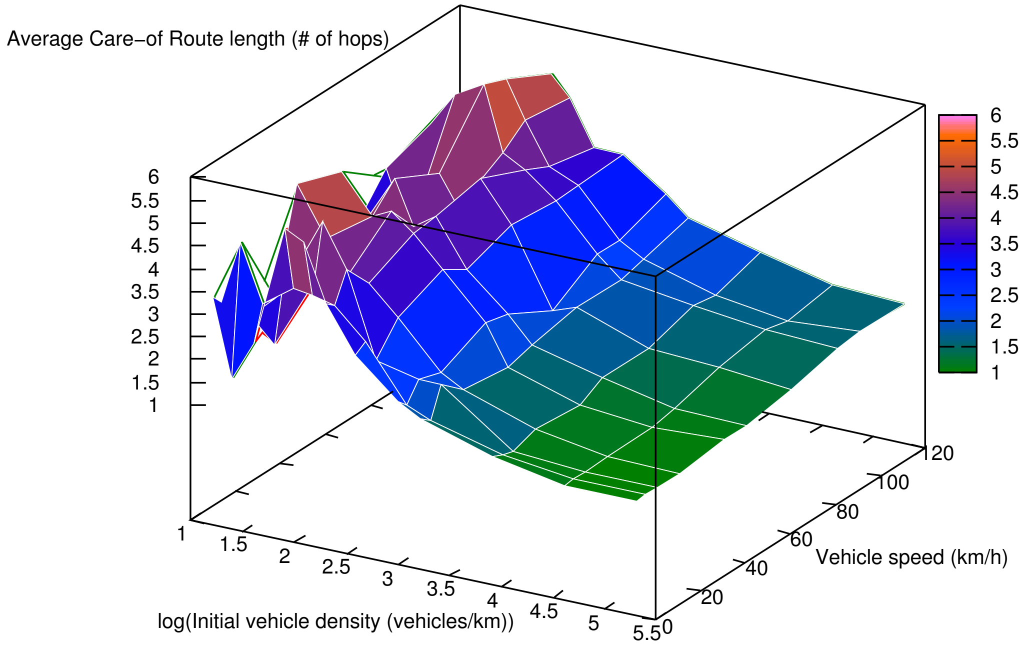


Figure 6.10: Average Care-of Route length.

route acquisition time comes from the cryptographic operations performed on each hop, this time is higher when the vehicle density decreases, because in a less populated VANET, the average number of intermediate MRs involved in a communication is higher (this will be shown later in Figure 6.10). However, if the average distance between vehicles is too high (that is, the vehicle density is low), this may lead to the situation where only direct 1-hop communications are possible (this explains why the route acquisition time decreases for very low vehicle densities).

Vehicle speed has also an effect on the Care-of Route acquisition time – although it is minor than the vehicle density – especially in highly populated scenarios. This effect is caused by the fact that it is more likely that more intermediate nodes are required to participate in the Care-of Route in high speed scenarios, since the distance between two vehicles that are communicating increases (because the relative speed of the vehicles is higher than in low mobility scenarios[15]).

Figure 6.10 shows the average Care-of Route length. The results shown in this graph basically confirms what has been discussed in the previous paragraph, that is, the strong dependency that the route acquisition time has on the number of hops of the Care-of Route. Since the delay caused by the HoRT messages traversing the infrastructure is the same for each route, independently of its length, the cost of performing cryptographic operations on each hop is an important factor in the route acquisition time. Obtained results show that for

[15] It should be recalled that in the simulations each vehicle moves with a constant velocity, which is a random variable uniformly distributed between $0.9v$ and $1.1v$ (the mean speed, v, is varied from from 1 to 120 km/h). This causes that in those scenarios where the mean speed (v) is higher, the relative speed of two moving vehicles will be also higher. For example, if v is 120 km/h, the speed of each vehicle is uniformly distributed between 108 and 132 km/h, so the relative velocity of two vehicles may be up to 24 km/h.

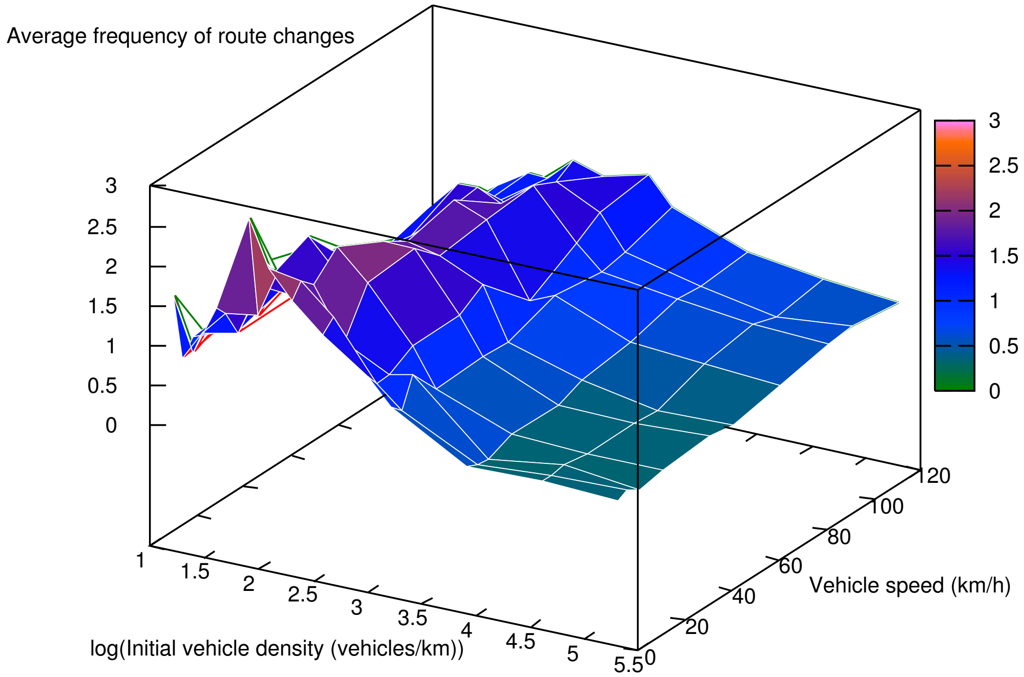


Figure 6.11: Average frequency of route changes.

highly populated scenarios, two MRs within the VANET are able to communicate directly almost always. For very low populated scenarios, the average number of hops of a Care-of Route decreases, since it is more difficult to establish a route within the VANET, unless when the two MRs can communicate directly. Vehicle speed has also an impact on the length of the route, at faster speeds the Care-of Route length increases (the reason for that is the same that the one for the increment in the acquisition time explained above).

From the obtained average number of hops involved in a Care-of Route, it may be deduced that VARON, although it is not designed to explicitly find the shortest path in terms of number of hops, usually finds the shortest route, since the first CoRTI received at the target MR normally travels along the shortest path (this may not be true in situations of network congestion, where the fastest path may not be the shortest). Therefore, VARON seems to perform well at finding the shortest Care-of Route.

Figure 6.11 shows the average frequency of route changes, that is the number of times during the lifetime of a communication flow that the route used to forward the packets switches from a Care-of Route to the Home Route, and vice-versa. This metric is important in order to evaluate the stability of the optimised Care-of routes. Obtained results show that the frequency of route changes grows when the vehicle density decreases, which is an expected behaviour, since in highly populated scenarios the Care-of route average length is small, so it is less probable that the route changes because there are less involved MRs. In very low populated scenarios, the frequency of route changes decreases, because it is less likely that a Care-of Route can be established and used, and therefore the number of route changes is smaller (i.e. most of the times traffic is forwarded through the Home Route).

Figure 6.12 shows the average Care-of Route data packet fraction, which is the fraction

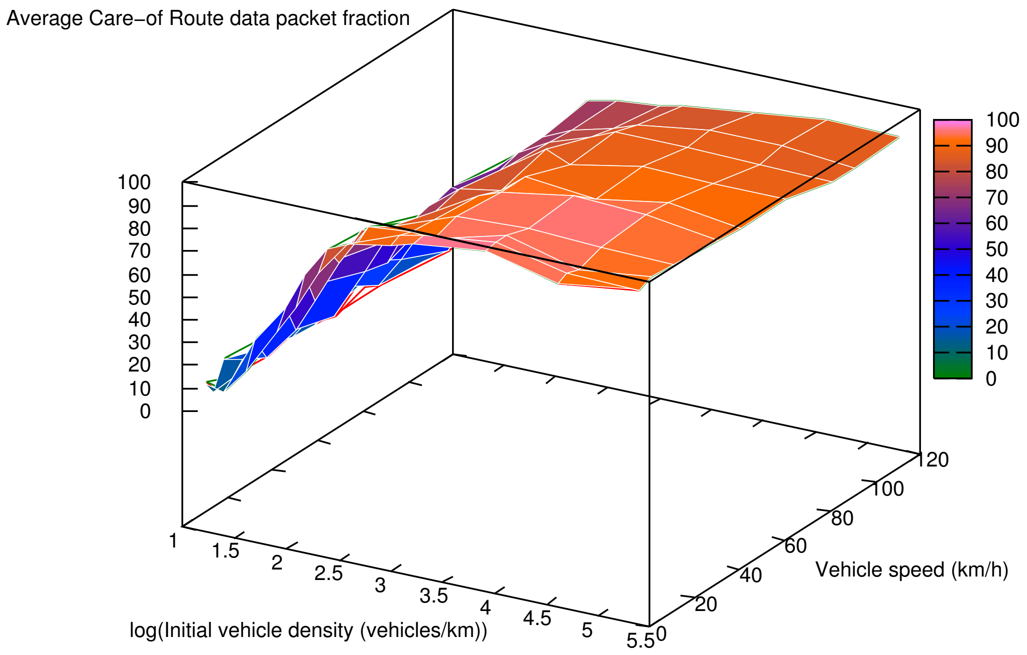
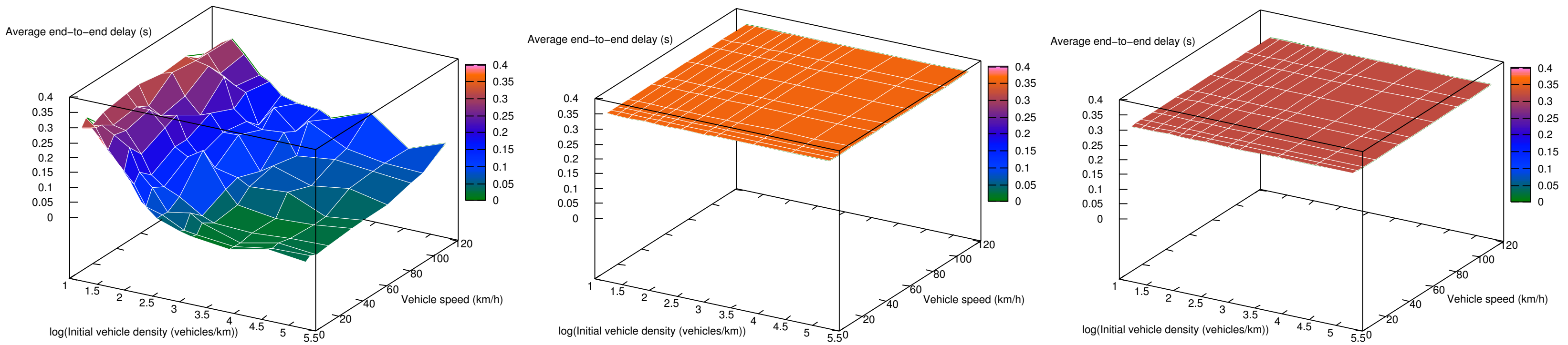


Figure 6.12: Average Care-of Route data packet fraction.

of delivered packets that are received through a Care-of Route. Therefore, this metric represents the likelihood of optimising the traffic by using the VANET. Obtained results show that there are more opportunities of optimising a communication in high populated scenarios and that the speed have also a small effect on the probability of establishing a Care-of Route (in highly mobile scenarios the probability is lower). This result is also expected, since in those situations where a small number of hops is required to communicate two MRs, it is easier to set-up a Care-of Route, which is, moreover, more stable.

Figure 6.13 shows the average end-to-end delay of data packets. The simulations were performed using three different protocols for the vehicle communication: VARON, NEMO Basic Support protocol and MIRON (as an example of application of a generic Route Optimisation for NEMO mechanism in car-to-car communications). The end-to-end delay experienced by data packets when the NEMO Basic Support protocol or MIRON were used is basically the one-way delay introduced by the access network plus the delay required to traverse the Home Networks (this delay is not present if the Route Optimisation support provided by MIRON is enabled). Therefore, this delay is independent of the vehicle density or speed. When VARON is enabled (Figure 6.13(a)), the end-to-end delay is drastically reduced, because when a Care-of Route is used to route traffic, packets do not traverse the infrastructure, and therefore the high delay introduced by UMTS is avoided. This end-to-end delay increases with decreasing vehicle density, since in low populated scenarios the probability of using a Care-of Route diminishes and the route length increases. For high vehicle densities, Figure 6.13(a) shows that vehicle speed has a small impact on the end-to-end delay, as the delay grows with faster speeds because, in highly dynamic scenarios, the stability of the the Care-of Routes decreases (see Figure 6.11) as well as the fraction of data packets sent through the VANET (see Figure 6.12).

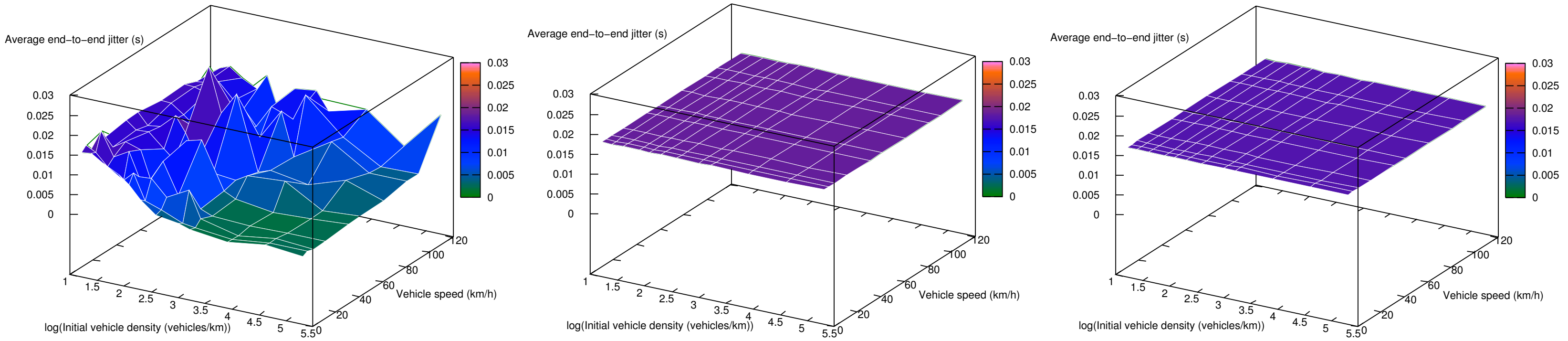


(a) VARON

(b) NEMO

(c) MIRON

Figure 6.13: Average end-to-end delay of data packets.



(a) VARON

(b) NEMO

(c) MIRON

Figure 6.14: Average end-to-end jitter of data packets.

Figure 6.14 shows the average end-to-end jitter of data packets. As for the end-to-end delay, simulations were run using VARON, plain NEMO Basic Support protocol and MIRON. Obtained results show that the end-to-end jitter is higher with VARON (Figure 6.14(a)) than with the NEMO Basic Support protocol (Figure 6.14(b)) and MIRON (Figure 6.14(c)). This is caused by the Home ↔ Care-of Route handovers. Besides, the end-to-delay jitter increases with decreasing vehicle density and with the speed, since in low populated scenarios, the stability of Care-of routes is lower (the same effect is caused by a faster speed, but in a minor extend).

Since the TCP receive buffer size [Pos81] and the TCP Window Scale option [JBB92] have a strong impact on the TCP throughput, and different TCP configurations can be found in practice (depending on the O.S., memory and processing capabilities, etc.), TCP throughput simulations were run using two different configurations:

- *Standard TCP configuration.* A TCP receive buffer size of 87380 bytes is configured and the TCP Window Scale option is enabled. This represents a standard TCP configuration nowadays[16].

- *Limited device configuration.* Portable devices – such as PDAs and cellular phones – and embedded devices have memory and processing constraints. Because of that, the memory available for handling a TCP connection is limited and less than the one used by normal machines (e.g., PCs). In order to evaluate the performance of this kind of machine, a TCP receive buffer size of 8760 bytes was configured with the TCP Window Scale option disabled.

Figure 6.15 shows the average end-to-end TCP throughput obtained using the standard TCP configuration. In order to compare the performance obtained by VARON with other approaches, the TCP throughput obtained with the NEMO Basic Support protocol and MIRON are also shown. Figure 6.15(a) shows the results when VARON is enabled in the vehicles. The TCP throughput decreases with decreasing vehicle density, since in scenarios with low population of vehicles, it is harder to set-up a Care-of Route, longer paths (see Figure 6.10) are usually required, and the configured routes have short lifetimes (see Figure 6.11). As it was shown in Figure 6.12, this leads to a low fraction of data traffic being sent through the VANET, and therefore the overall performance is poor. Besides, the fact of not having implemented the detection of broken routes has also an impact on the obtained TCP throughput, since the packet loss – that may be experienced when a route breaks until it is deleted from the IP routing table (after its expiration) – makes TCP congestion protocol reduce its transmission rate[17]. Actually, for very low vehicle densities, the performance obtained with the NEMO Basic Support protocol (approximately 275 kbit/s, as shown in Figure 6.15(b)) or MIRON (approximately 300 kbit/s, as shown in Figure 6.16(c)) is better than with VARON. However, obtained results show that for scenarios not so low populated – as urban or even inter-urban scenarios, where vehicles are typically distributed within roads with inter-vehicle distances of less than 150 m – VARON outperforms both NEMO Basic Support protocol and MIRON. For high vehicle densities (e.g., traffic jams), the TCP throughput obtained with

[16] This is the default configuration of a Linux-2.6 machine.

[17] The retransmission threshold behaviour used in the simulations was configured according to the TCP standard and ensuring that connections could not break because of excessive retransmission attempts.

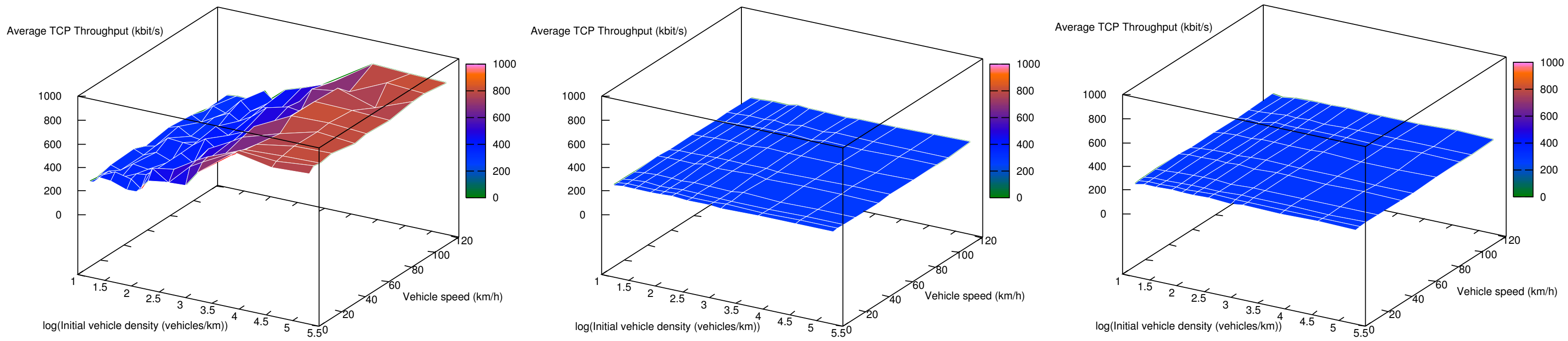
VARON is close to 1 Mbit/s, which is a great improvement over the non vehicular optimised protocols (NEMO and MIRON). This improvement is provided by VARON because of two main reasons:

- VARON enables the use of a VANET network built using an access technology – such as IEEE 802.11 – that typically has more bandwidth that the access technology used by a vehicle to connect to the Internet (e.g., GPRS/UMTS).
- VARON enables direct data packet forwarding within the VANET, avoiding to use the infrastructure network and therefore reducing drastically the end-to-end delay (as shown in Figure 6.13(a)). Since TCP performance is heavily dependent on the round trip time (RTT) between the communication peers, this end-to-end delay reduction contributes to the TCP throughput improvement.

Figure 6.16 shows the TCP throughput results for the limited device TCP configuration. Because of the relatively small TCP receive buffer size used and the high delays introduced by cellular access technologies, such as GPRS/UMTS, the TCP throughput obtained with the NEMO Basic Support protocol (Figure 6.16(b)) or MIRON (Figure 6.16(c)), is very low (less than 100 kbit/s). On the other hand, with VARON (Figure 6.16(a)) the obtained TCP throughput is the same that with the standard TCP configuration, since the impact of having a smaller TCP receive buffer size is almost null because of the low end-to-end delay enabled by VARON. Therefore, a conclusion that can be derived from these results is that the TCP throughput improvement introduced by VARON is more relevant for those devices that are memory and processing limited. This is important, since it is likely that some of the devices that will be deployed within a car will be limited to some extend in terms of memory and/or processing power.

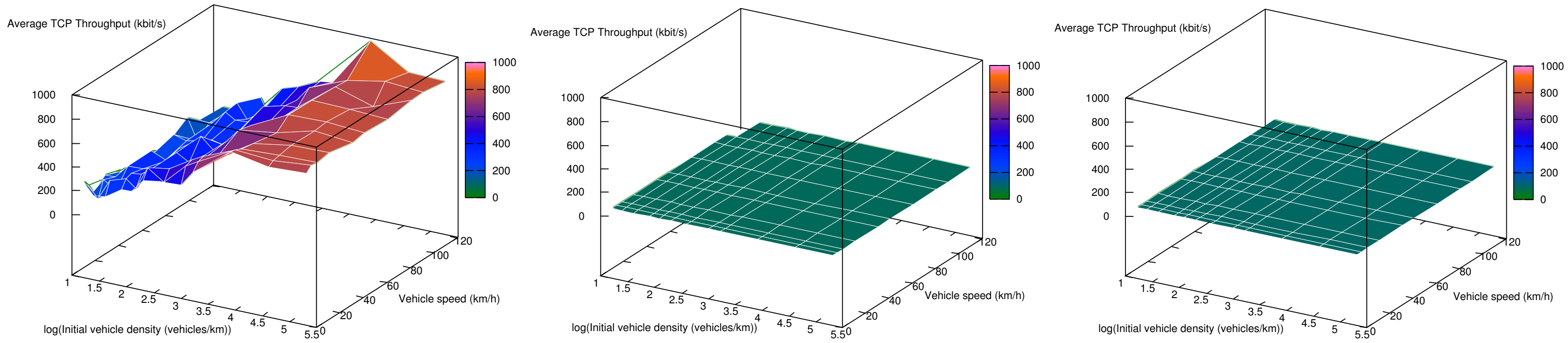
The last metric that was simulated was the signalling load introduced by VARON. Figures 6.17 and 6.18 show the signalling load, measured both in bytes and packets. Simulations were performed both using the standard and the limited device TCP configurations. Obtained results show that the overhead introduced by VARON, because of periodic HoAA messages and the Care-of Route discovery, is not negligible. VARON's byte signalling load (shown in Figure 6.17) reaches almost 70% in low populated and high speed scenarios, although it is about 20% for the rest of the scenarios (e.g., urban and inter-urban). Results show that there is a constant amount of overhead caused by the periodic HoAA flooding, but the main contribution to this overhead comes from the Care-of Route discovery and set-up signalling.

Obtained results show that VARON's overhead is less with the limited device TCP configuration (see Figures 6.17(b) and 6.18(b)) than with the standard TCP configuration (see Figures 6.17(a) and 6.18(b)). This may be caused by the fact that VARON optimises more the routing of data packets for limited TCP configurations, which means that more packets are received through the Care-of Route and therefore the quotient of the signalling packets divided by the data packets received through a Care-of Route is smaller.



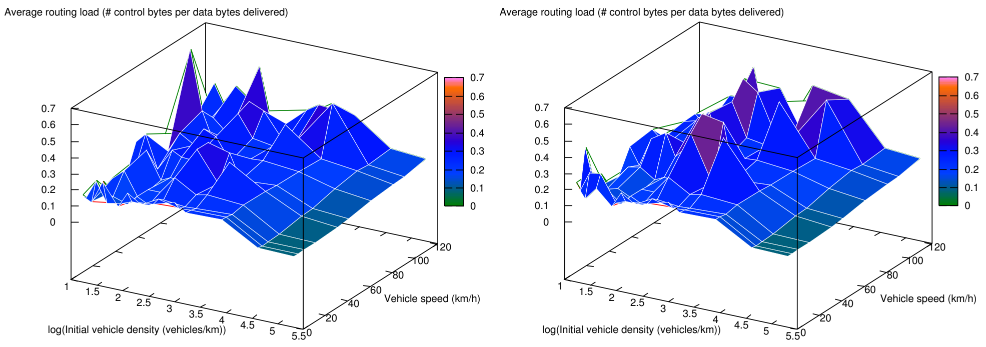
(a) VARON (b) NEMO (c) MIRON

Figure 6.15: Average end-to-end TCP throughput (standard TCP configuration).



(a) VARON (b) NEMO (c) MIRON

Figure 6.16: Average end-to-end TCP throughput (limited device TCP configuration).



(a) Standard TCP configuration.

(b) Limited device TCP configuration.

Figure 6.17: Average VARON signalling load (bytes).

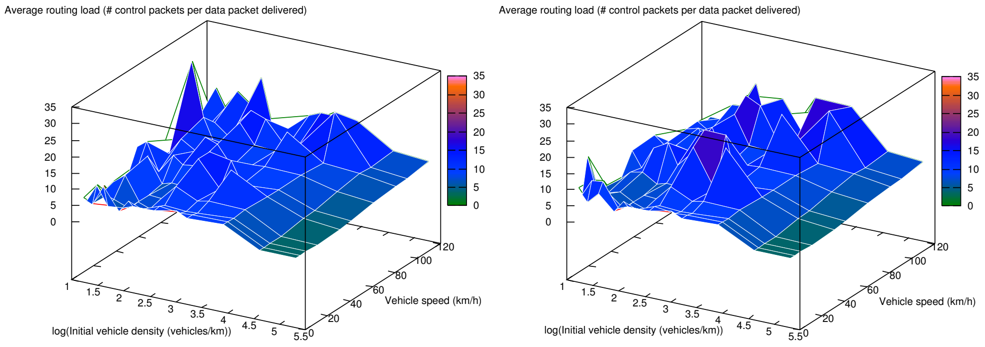
Although VARON's byte signalling is not negligible but relatively low in most of the scenarios, VARON's packet overhead (shown in Figure 6.18) results show that VARON requires a great amount of small signalling packets to work (the number of received VARON signalling packets even reaches 35 times the number of data packets in the worst case scenario). This is caused by the periodic HoAA flooding and also by the flooding nature of the Care-of Route discovery signalling. Besides, the same signalling is required periodically to refresh an already established route.

VARON's overhead may seem to be very high and therefore it may be argued that it is not a good optimisation mechanism. However, there are several considerations that should be taken into account:

- Almost all the signalling required by VARON is sent through the ad-hoc interface. This interface is not used to send non optimised regular traffic and it has typically no cost associated. It may be argued that sending so many packets imposes a non negligible energy cost, but in vehicles this cost is not so important, since they have a powerful and rechargeable source of energy. On the other hand, the computational cost associated to sending this signalling may have an impact on the overall performance of the Mobile Router. Simulations have taken into account the cost associated to the cryptographic computations performed on each packet, but forwarding a packet has also a cost, that depending on the MR's capabilities may be relevant.

- The VARON simulated model does not implement the detection of broken links and the CoRE associated signalling. By implementing this missing part, other configuration parameters – such as the periodic timers involved in the Care-of Route discovery and refreshment –, could be set to less aggressive values (in terms of periodicity and, therefore, associated overhead). The refreshment of a Care-of Route could even be removed if the algorithm followed to detect broken links is good enough and ensures that all broken links can be detected. If not, it could always be optimised, for example by not re-doing the full Care-of Route discovery process (that involves a partial flooding of the VANET), but just sending a probe packet through the established Care-of Route to check if it is still working.

Although graphs only display average values for the different simulated metrics, the



(a) Standard TCP configuration.

(b) Limited device TCP configuration.

Figure 6.18: Average VARON signalling load (packets).

normalised standard deviation has also been calculated. Obtained results show that the normalised standard deviation is higher in the low populated and high mobile scenarios than in the high populated and low mobile scenarios, meaning that former scenarios are more unstable than the latter ones.

One important conclusion that can be derived from the simulation work is that in highly mobile and low populated scenarios, it is more difficult to set-up a multi-hop route between two vehicles, mainly because of the instability in the ad-hoc routing. Therefore, most of the opportunities of communication involve routes with a very low number of hops. An example of communication scenario that will greatly benefit from VARON optimisations would be that of military convoys or emergency service operations, where a group of vehicles move together.

6.5. Conclusions

In this chapter we have described VARON, a solution that enables optimal direct vehicle-to-vehicle communication, by using a multi-hop vehicular ad-hoc network for communications involving vehicles that are relatively close to each other. Although the proposed solution does not preclude the possibility of performing some Denial of Service attacks, that are inherent to the ad-hoc environment, these attacks only affect the ad-hoc route and vehicles can always fall back to the communication through the infrastructure if needed. The benefit of the proposed mechanism is a clear improvement in throughput and end-to-end delay with security guarantees similar to those available in infrastructure communications.

The robustness of VARON against ad-hoc routing attacks is build on the hop-by-hop authentication and message integrity of routing messages, and the use of CGAs (that makes the spoofing attack against the IPv6 address much harder and allows to sign messages with the owner's private key, without requiring any upgrade or modification in the infrastructure). However, this involves a performance cost, since cryptographic operations, such as signature generation/verification, consume time and energy. This cost could be of some concern, specially in energy and resource constrained devices. However, in the case of Mobile Routers deployed in cars, this is not a big issue, since vehicles have a powerful and rechargeable source of energy.

The proposed protocol has been validated and evaluated through extensive simulation conducted with OPNET. Results show that VARON improves significantly the performance in terms of TCP throughput and end-to-end delay when compared to other approaches such as the use of plain NEMO Basic Support protocol or a generic Route Optimisation solution for NEMO – such as MIRON – not suited for vehicular environments that obtain Internet access from low-bandwidth and high-delay access technology (e.g., GPRS/UMTS). Simulation has also shown that in highly mobile and low populated scenarios, the probability of using the VANET to route traffic is low, because of the instability in the ad-hoc routing. Most of the opportunities of optimised communication involve routes with a very low number of hops (less than 5 hops). Hence, scenarios such as urban and inter-urban communications (e.g., traffic jams, vehicles in a motorway) may greatly benefit from deploying VARON, especially in the case a group of vehicles moving together, such as military convoys or emergency service operations. On the other hand, it is not worth using VARON in highly mobile and low populated scenarios – such as highways – since the probability of optimising a communication is very low and its lifetime would be very short.

Although this chapter has presented VARON as a solution suited for vehicular environments, its applicability is not limited to that scenario. Actually, any scenario involving mobile networks where an ad-hoc network can be set-up is a good candidate for VARON deployment. For example, passengers on a train carrying their Personal Area Networks (PANs) may play online games from the train while travelling (e.g., by using a PDA connected to a mobile phone acting as the Mobile Router). If two players are located within the same train, their MRs may decide to bypass the routing infrastructure and directly send their traffic using a direct ad-hoc communication.

Part III

Conclusions and future work

Conclusiones y Trabajos Futuros

Chapter 7

Conclusions

Over the last decade, a considerable effort has been invested to enable mobility in IP networks. Internet is evolving towards a ubiquitous network – accessible anytime, anywhere – that integrates voice and data services, with billions of users seamlessly connected through wireless IP terminals. To achieve this convergence of wireless networks and the Internet, several mechanisms have been defined to enable true transparent IP mobility of hosts roaming across different heterogeneous networks.

A step forward in the mobility support is required by users, that do not only expect to have Internet access available from fixed locations, but also at mobile platforms, such as buses, aircrafts 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 this thesis we have proposed an architecture – consisting of a set of mechanisms – to enable optimal Route Optimisation in Mobile Networks with the following features:

Deployment. The proposed architecture provides support for legacy nodes and requires no changes on the operation of any node but the Mobile Router.

Universality. The proposed mechanisms support the optimisation of communications of any kind of node attached to a Mobile Network: Local Fixed Nodes and Visiting Mobile Nodes. Route Optimisation for nested configurations is also supported.

Security. The designed solutions provide a level of security similar than today's IPv4 Internet, by means of reusing Mobile IPv6 security concepts, and the use of public key cryptography and Cryptographically Generated Addresses (CGAs). For those scenarios where a higher level of security is required, alternative approaches based on the secure delegation of signalling rights have been also proposed and analysed.

Scalability. Since the resources required by the proposed mechanisms grow linearly with the number of optimisations being performed, the architecture scales well with the number of users.

Vehicular optimisation support. The proposed architecture provides specific mechanisms that further improve the performance in vehicular scenarios, by enabling vehicles that are able to form a multi-hop ad-hoc network to communicate each other directly through the formed VANET.

The proposed Route Optimisation architecture consists of two mechanisms. The first one is a generic solution, called *MIRON: Mobile IPv6 Route Optimisation for NEMO*. 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) to manage their own Route Optimisation.

The second mechanism has been designed to deal with the vehicular scenario. Communications in vehicular scenarios are expected to become very important in the near future. A first step to solve the problem of enabling communications from and between vehicles is the provision of connectivity to the Internet. Cars will likely have specialised devices (i.e. Mobile Routers) that will provide network access to the rest of the devices in the car, i.e. the car will contain a Mobile Network. For this reason we have proposed the application of Network Mobility solutions to this scenario. The NEMO Basic Support protocol is the straightforward option. The performance limitations of this scenario can be partially overcome through the application of a generic NEMO Route Optimisation solution, such as MIRON.

Besides the Internet access, there are several applications which involve a vehicle-to-vehicle communication. This kind of scenario may be supported by using Network Mobility solutions, so cars can communicate through the fixed infrastructure but, in this case, when the cars are close enough, a further optimisation is possible, namely to communicate directly using an ad-hoc network. In this way, better bandwidth than the one in the communication through the infrastructure can be achieved. Typically, this will be true even if we use a NEMO Route Optimisation solution for the communication through the fixed Internet. The reason is that, although the number of hops can be similar, the communication with the infrastructure will use usually a technology with lower bandwidth (for example, UMTS) than the ad-hoc network (for example, WLAN). Also, the ad-hoc route will probably result in lower costs. The mechanism proposed in this work, called *VARON: Vehicular Ad-hoc Route Optimisation for NEMO*, consists in a secure combination of the Network Mobility and Ad-hoc concepts to optimise local car-to-car communications.

The performance of the two proposed mechanisms has been validated via:

- Experiments with a Linux implementation (MIRON).
- Simulations with the OPNET tool (VARON).

Both simulation and experimental results have shown that the designed solutions outperforms the NEMO Basic Support protocol and enables true Route Optimisation support for generic and vehicular scenarios.

Capítulo 7

Conclusiones

En la última década, una cantidad considerable de esfuerzo ha sido invertida con objeto de habilitar la movilidad en redes IP. Internet está evolucionando hacia una red ubicua – accesible en cualquier momento y desde cualquier lugar – que integra servicios de voz y datos, con miles de millones de usuarios conectados a través de terminales IP inalámbricos. Para alcanzar esta convergencia entre las redes inalámbricas e Internet, varios mecanismos han sido definidos para habilitar la movilidad transparente real de nodos moviéndose entre diferentes redes heterogéneas.

Un paso más en el soporte de movilidad viene demandado por los usuarios, que no esperan sólo disponer de acceso a Internet en localizaciones fijas, sino también en plataformas móviles, como autobuses, aviones o coches. El mecanismo básico definido para soportar movilidad de redes (el protocolo de Soporte Básico de Movilidad de Redes) es una extensión del protocolo definido para habilitar movilidad en nodos individuales (IPv6 Móvil), pero sin algunas de las optimizaciones que IPv6 Móvil proporciona. Una de estas piezas que faltan es el soporte de optimización de rutas.

En esta Tesis proponemos una arquitectura – consistente en un conjunto de mecanismos – para habilitar la optimización de rutas en redes móviles de forma óptima, con las siguientes características:

Desplegabilidad. La arquitectura propuesta proporciona soporte a nodos legados y no requiere de ningún cambio en el funcionamiento de ningún nodo, salvo el router móvil.

Universalidad. Los mecanismos propuestos soportan la optimización de las comunicaciones de cualquier tipo de nodo conectado a la red móvil: Nodos Locales Fijos y Nodos Móviles Visitantes. La optimización de rutas para configuraciones anidadas también es soportada.

Seguridad. Las soluciones diseñadas proporcionan un nivel de seguridad similar a la Internet IPv4 actual, mediante la reutilización de algunos conceptos de seguridad de IPv6 Móvil, el uso de criptografía de clave pública y Direcciones Criptográficamente Generadas (CGAs, Cryptographically Generated Addresses). Para aquellos escenarios en los que se requiere un nivel de seguridad mayor, se han propuesto y analizado alternativas basadas en la delegación segura de los derechos de señalización.

Escalabilidad. Dado que los recursos requeridos por los mecanismos propuestos crecen linealmente con el número de optimizaciones realizadas, la arquitectura escala bien con el número de usuarios.

Soporte de optimización vehicular. La arquitectura propuesta proporciona mecanismos específicos que mejoran aún más el rendimiento en escenarios vehiculares, habilitando que los vehículos que sean capaces de formar una red ad-hoc multi-salto puedan comunicarse directamente a través de la VANET creada.

La arquitectura de optimización de rutas propuesta consta de dos mecanismos. El primero de ellos es una solución genérica, llamada *MIRON: Mobile IPv6 Route Optimisation for NEMO*. MIRON hace posible la comunicación directa entre un nodo de la red móvil – soportando cualquier tipo de nodo, con y sin soporte de movilidad – y cualquier otro nodo en 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 capacidades de movilidad, y un modo adicional, basado en PANA y DHCP, que posibilita que los nodos con soporte de movilidad (p.e., los nodos móviles que estén visitando la red móvil) y los routers móviles (redes móviles anidadas) puedan gestionar su propia optimización de rutas.

El segundo mecanismo ha sido diseñado específicamente para el entorno vehicular. Se espera que las comunicaciones vehiculares adquieran una gran importancia en un futuro cercano. Un primer paso para resolver el problema de las comunicaciones vehiculares es la provisión de conectividad con Internet. Muy probablemente, los coches dispondrán de dispositivos especializados (los routers móviles) para proporcionar conectividad al resto de dispositivos en el coche, es decir, el coche contendrá una red móvil. Por esta razón, hemos propuesto la aplicación de soluciones de movilidad de redes en este tipo de escenario. El protocolo de Soporte Básico de Movilidad de Redes es la opción más directa. Las limitaciones en rendimiento de este escenario pueden solventarse parcialmente mediante la aplicación de una solución genérica de optimización de rutas como MIRON.

Además del acceso a Internet, existen algunas aplicaciones que involucran una comunicación inter-vehicular. Esta clase de escenario puede soportarse mediante la aplicación de soluciones de movilidad de redes, de forma que los coches se comunican entre sí pasando por la infraestructura fija, pero en ese caso, cuando los vehículos están lo suficientemente cerca, una optimización más es posible, consistente en comunicarse directamente utilizando una red ad-hoc. De esta forma, se consigue un ancho de banda mayor que el obtenido cuando se atraviesa la infraestructura. Típicamente, esto sera cierto incluso si se utiliza una solución de optimización de rutas genérica para la comunicación que atraviesa la Internet fija. La razón es que, aunque el número de saltos intermedios puede ser similar, la comunicación con la infraestructura utilizará típicamente una tecnología con un ancho de banda menor (por ejemplo, UMTS) que la red ad-hoc (por ejemplo, WLAN). Además, probablemente será más barato utilizar la ruta ad-hoc. El mecanismo propuesto en esta Tesis, llamado *VARON: Vehicular Ad-hoc Route Optimisation for NEMO*, consiste en una combinación segura de los conceptos de movilidad de redes y ad-hoc para optimizar comunicaciones locales entre vehículos.

El rendimiento de los dos mecanismos propuestos ha sido validado vía:

- Experimentos con una implementación en Linux (MIRON).
- Simulaciones con la herramienta OPNET (VARON).

Tanto las simulaciones como los resultados experimentales han mostrado que las soluciones diseñadas proporcionan un considerable incremento sobre el rendimiento ofrecido por el protocolo de Soporte Básico de Movilidad de Redes, proporcionando un soporte de optimización de rutas real en escenarios genéricos y vehiculares.

Chapter 8

Future work

This chapter presents some research topics that are still open and that we consider of interest within the field of Route Optimisation in IPv6 heterogeneous networks.

8.1. Route Optimisation flow decision

MIRON and VARON require an additional mechanism to make the decision whether to perform Route Optimisation for a certain flow or not. How this decision is taken is very relevant for the scalability of the solution, especially in large mobile networks.

The algorithms and heuristics designed to take this decision may even benefit from feedback of the Mobile Router's current load and take into account user or administrative preferences. The same algorithms can be applied (maybe with minor modifications) to the host mobility scenario (Mobile IPv6).

8.2. Handover latency optimisation

Due to the PANA and DHCPv6 signalling, MIRON takes longer to finish its handover than in NEMO Basic Support. Similarly to the case of Mobile IPv6 – where the Route Optimisation support also increases the raw handover latency – micromobility solutions such as Fast Handovers for Mobile IPv6 [Koo05], should be designed/adapted to MIRON to alleviate the increase in the handover delay [BSM+05]. The designed mechanism should support nested configurations, since this is the worst case scenario due to the amount of signalling that has to be generated and the number of entities involved.

8.3. MNN visibility in visited networks

It is worth looking into the issues and tradeoffs involved in making network movement visible to some mobile network nodes, by making them *NEMO aware*. This would allow several nodes to manage their own Route Optimisation (in a similar fashion that MIRON enables VMNs to manage their mobility). Actually, this is currently being discussed within the IETF NEMO WG and it seems that this approach would be explored as a possible mechanism to provide Route Optimisation in several deployment scenarios. PANA may be a good candidate to enable some nodes to be aware of the movement of the network (in fact, several parts of MIRON can be considered as a first step within this research line).

8.4. HIP-based Route Optimisation

Currently, the IP address play both the role of the identifier and the locator in a communication. Although, mapping both concepts into a single name (the IP address), provides some benefits (e.g., the mapping is direct and therefore secure), it also brings some intrinsic problems, such as those related to mobility and multihoming. There have been several authors proposing to break this union [Chi99], and there also exists some particular protocols and solutions doing that, such as HIP (Host Identity Protocol) [MN05], [MNJH06] and CGAs (Cryptographically Generated Addresses) [MC02], [Aur05].

Given the increasing importance of HIP, it is interesting to explore approaches that enable Network Mobility and Route Optimisation in HIP-based architectures [Yli05].

Capítulo 8

Trabajos futuros

Este capítulo presenta algunos temas de investigación que todavía están abiertos y que consideramos de interés dentro del campo de la optimización de rutas en entornos IPv6 heterogéneos.

8.1. Decisión de optimización de ruta para un flujo

MIRON y VARON requieren de un mecanismo adicional para tomar la decisión sobre si se debe realizar una optimización de ruta para un determinado flujo o no. Cómo se toma esta decisión es muy relevante de cara a la escalabilidad de la solución, especialmente en redes móviles grandes.

Los algoritmos y heurísticos que se diseñen para tomar esta decisión deben obtener realimentación acerca de la carga actual del router móvil y tener en cuenta preferencias del usuario o del administrador del sitio. Los mismos algoritmos que se desarrollen para el caso de optimización de rutas para redes móviles podrán ser aplicados (quizás con pequeños cambios) al escenario de movilidad de terminal (IPv6 Móvil).

8.2. Optimización de la latencia de traspaso

Debido a la señalización PANA y DHCP necesaria, MIRON necesita de más tiempo para completar un traspaso que el protocolo de Soporte Básico de Movilidad de Redes. De manera análoga al caso de IPv6 móvil – dónde el soporte de optimización de rutas también incrementa la latencia de un traspaso – soluciones de micro-movilidad como Traspasos Rápidos para IPv6 Móvil (FMIPv6, Fast Handovers for Mobile IPv6 [Koo05]), deben ser diseñados/adaptados a MIRON para aliviar el incremento en el tiempo de handover [BSM$^+$05]. Los mecanismos que se diseñen deben soportar configuraciones anidadas, ya que este es el peor escenario debido a la carga de señalización que se genera y al número de entidades involucradas.

8.3. Visibilidad de la red visitada en el MNN

Merece la pena estudiar los problemas y ventajas que conlleva hacer la movilidad visible a algunos Nodos de Red Móvil, convirtiéndolos en nodos *conscientes de la movilidad de la red*. Esto permitiría que algunos nodos pudieran gestionar su propia optimización de rutas (de una forma similar a como MIRON permite que lo hagan los VMNs). De hecho, esto está siendo actualmente discutido en el grupo NEMO del IETF y parece que este enfoque será explorado como posible mecanismo para proporcionar optimización de rutas en ciertos casos de uso. PANA puede ser un buen candidato para permitir que ciertos nodos sean conscientes de la movilidad de la red (de hecho, algunas partes de MIRON pueden considerarse como un primer paso en esta línea de investigación).

8.4. Optimización de rutas basada en HIP

Actualmente, la dirección IP juega el rol de identificador y el de localizador en una comunicación simultáneamente. Aunque el mapeo de ambos conceptos en un único nombre (la dirección IP) proporciona algunas ventajas (p.e., la traducción entre uno y otro es directa y por lo tanto segura), también origina algunos problemas intrínsecos, como todos los relacionados con movilidad y multihoming. Ha habido algunos autores proponiendo romper esta unión [Chi99], y también existe ciertos protocolos y soluciones que lo hacen, como HIP (Host Identity Protocol) [MN05], [MNJH06] y las CGAs (Cryptographically Generated Addresses) [MC02], [Aur05].

Dada la incipiente importancia del protocolo HIP, resulta interesante explorar soluciones que permitan soportar la movilidad de redes y proporcionar optimización de rutas en arquitecturas basadas en la utilización de HIP [Yli05].

Part IV

Appendixes

Apéndices

Appendix A

Network Authentication and Access Control: A brief introduction to PANA

Nowadays, most of the public wireless access networks deploy some authentication and access control mechanisms in order to avoid unauthorised clients gaining access to the network. Nevertheless, these mechanisms are either limited to specific access media technologies (e.g., 802.1X for IEEE 802 links) or based on proprietary solutions (e.g., web access-based authentication methods) [YOP+05]. This fact, together with the expectation that future mobile devices will have several access technologies to gain network connectivity, triggered the creation of a new working group within the IETF, called PANA (Protocol for Carrying Authentication for Network Access), aimed at the definition and specification of a standard network-layer solution for authenticating clients for network access. This appendix briefly introduces the PANA protocol and its basic operation.

The PANA protocol [FOP+06], [JLO+06] is designed to facilitate authentication and authorisation of clients in access networks. Basically, it is a link-layer agnostic network access authentication protocol – encapsulating Extensible Authentication Protocol (EAP) [ABV+04] authentication methods – that runs between an entity (called PANA Client, PaC) in a node that wants to gain access to the network and an agent (called PANA Authentication Agent, PAA) in a server on the network side [JLO+06]. PANA is responsible for enabling the authentication process between these two entities, but it is just a part of the overall process of Authentication, Authorisation and Accounting (AAA) and access control. The complete picture, with AAA and access control functions, comprises four entities (Figure A.1):

- *PANA Client (PaC)*. Entity residing in the node that requests network access and implements the client part of the PANA protocol.

- *PANA Authentication Agent (PAA)*. Entity implementing the server part of the PANA protocol that interacts with the PaCs for authenticating and authorising them to access the network. The PAA consults the Authentication Server (AS) in order to verify the credentials and rights of a PaC and also updates the access control state, such as filters, in the Enforcement Points (EPs) in the network. The PAA usually resides in

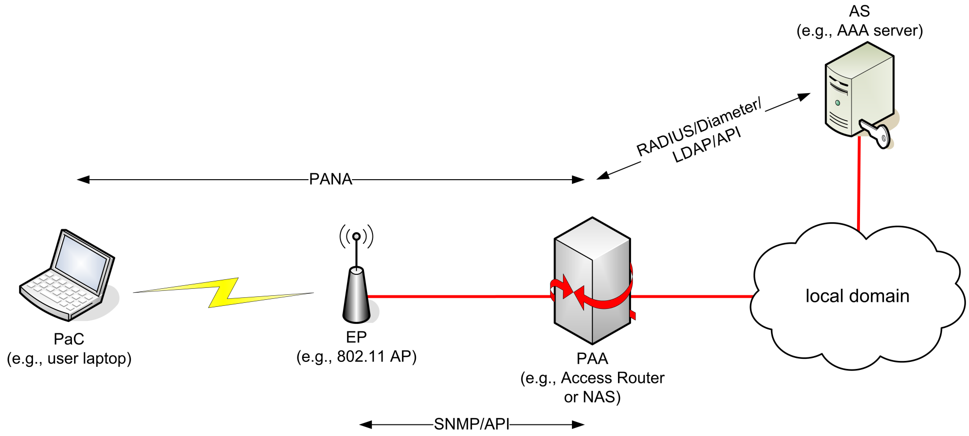


Figure A.1: PANA functional model overview. Some entities can be also collocated on a same physical node.

the Network Access Server (NAS) node, but it can be hosted in any node that is in the same subnet (within 1-hop distance) as the PaC.

- *Authentication Server (AS)*. Server-side entity in charge of verifying the credentials of a PaC requesting access (sent by the PAA on behalf of the PaCs).
- *Enforcement Point (EP)*. Entity implementing the access control function by allowing access to authorised clients and preventing access from others.

PANA is a UDP-based protocol [FOP$^+$06], consisting of a series of requests and responses. Each message can carry zero or more Attribute Value Pairs (AVPs) as payload. The main payload of PANA is EAP, which is responsible for performing authentication (PANA just helps the PaC and PAA establish an EAP session). Messages are sent between PaC and PAA as part of a PANA session, that consists of five different phases:

1. *Discovery and handshake phase.* This phase starts the PANA session. The PaC discovers the PAA(s) by either explicitly soliciting advertisements to the PAA(s) or receiving unsolicited advertisements. The PaC's answer, sent in response to an advertisement, starts a new session.
2. *Authentication and authorisation phase.* EAP execution between the PAA and PaC, by carrying an EAP method inside the EAP payload.
3. *Access phase.* If the authentication and authorisation phase is successful, the host gains access to the network and can send and receive IP data traffic through the EP(s).
4. *Re-authentication phase.* This phase is usually initiated by the PAA before the session lifetime expires (carrying EAP to perform authentication), although this phase may be triggered by either the PaC or PAA regardless of the session lifetime.
5. *Termination phase.* The PaC or the PAA may choose to discontinue the access service at any time, by sending an explicit disconnect message.

Appendix B

VARON protocol message format

B.1. Introduction

This appendix provides a detailed description of the VARON protocol message format. VARON messages are encapsulated in UDP[1] (all participants should agree on a port number if no well-known port number is assigned). All VARON message options are 64-bit aligned.

Next sections describes each of the messages options defined by the VARON protocol.

B.2. Care-of Route Test Init (CoRTI)

This message option is sent (encapsulated in a UDP datagram) by the originator MR. The source IP address of the UDP packet is set to the originator MR's HoA and the destination IP address is set to the *link-local All Routers* multicast IPv6 address (FF02:0:0:0:0:0:0:2) [HD06]. The TTL of the packet is set to `VARONC_CORTI_TTL_MAX` (default value: 10). This option has the format shown in Figure B.1. Next, a brief description of each option field is provided:

- *Type:* 8-bit selector. It identifies the CoRTI option.
- *Reserved:* 8-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.
- *Nonce:* 32-bit field which contains the Nonce N_A issued by the originator MR.
- *Originator HoA:* The Home Address (128-bit) of the originator Mobile Router (that is, the sender MR that wants to set-up a Care-of Route towards the target HoA). This address must be a unicast routable address.
- *Target HoA:* The Home Address (128-bit) of the target Mobile Router (that is, the destination to which it is wanted to set-up a Care-of Route). This address must be a unicast routable address.

[1] UDP was chosen so the protocol is IPv4 compatible, in case an IPv4 solution was needed.

<table>
<tr><td>Type</td><td>Reserved</td><td>Care-of Nonce index</td></tr>
<tr><td colspan="3">Nonce</td></tr>
<tr><td colspan="3">Originator
HoA</td></tr>
<tr><td colspan="3">Target
HoA</td></tr>
<tr><td colspan="3">CGA option (originator MR)</td></tr>
<tr><td colspan="3">RSA Signature option (originator MR)</td></tr>
<tr><td colspan="3">Care-of Init
cookie</td></tr>
<tr><td colspan="3">Care-of Keygen token
token</td></tr>
</table>

Figure B.1: CoRTI message option (sent by the originator MR) format.

- *CGA option (originator MR):* A variable length field containing the CGA option data structure (as defined in Section 5.1 of RFC 3971 [AKZN05], and included below - see Figure B.3 - for convenience) of the originator HoA.

- *RSA Signature option (originator MR):* A variable length field containing the RSA Signature option (as defined in Section 5.2 of RFC 3971 [AKZN05], and included below - see Figure B.5 - for convenience).

- *Care-of Nonce index:* 16-bit field which contains the nonce used by the originator MR to generate the Care-of Keygen token. This field will be echoed back by the target MR to the originator MR in a subsequent Mobile Network Prefix Binding Update.

- *Care-of Init cookie:* 64-bit field which contains a random value, the Care-of Init cookie.

- *Care-of Keygen token:* This field contains the 64 bit Care-of Keygen token used in the Care-of Route authentication signalling.

A CoRTI message forwarded by an intermediate MR has a slightly different format, since the forwarder MR adds its CGA information and signature. The format of this option is shown in Figure B.2.

Type	Reserved	Care-of Nonce index
Nonce		
Originator HoA		
Target HoA		
CGA option (originator MR)		
RSA Signature option (originator MR)		
CGA option (forwarder MR)		
RSA Signature option (forwarder MR)		
Care-of Init cookie		
Care-of Keygen token token		

Figure B.2: CoRTI message option (forwarded by an intermediate MR) format.

B.3. CGA option

The CGA option allows the verification of the sender's CGA. The format of the CGA option (Section 5.1 of RFC 3971 [AKZN05]) is described next:

- *Type:* 11
- *Length:* The length of the option (including the Type, Length, Pad Length, Reserved, CGA Parameters, and Padding fields) in units of 8 octets.
- *Pad Length:* The number of padding octets beyond the end of the CGA Parameters field but within the length specified by the Length field. Padding octets must be set to zero by senders and ignored by receivers.
- *Reserved:* An 8-bit field reserved for future use. The value must be initialised to zero by the sender and must be ignored by the receiver.

Type	Length	Pad Length	Reserved
CGA Parameters			
Padding			

Figure B.3: CGA option format.

- *CGA Parameters:* A variable-length field containing the CGA Parameters data structure described in Section 3 of [Aur05] (and included below for convenience).

  RFC 3971 [AKZN05] requires that if both the CGA option and the RSA Signature option are present, then the public key found from the CGA Parameters field in the CGA option must be that referred by the Key Hash field in the RSA Signature option. Packets received with two different keys must be silently discarded. Note that a future extension may provide a mechanism allowing the owner of an address and the signer to be different parties.

- *Padding:* A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

B.4. CGA parameters

Each CGA is associated with a CGA Parameters data structure, which has the following format (specified in Section 3 of RFC 3972 [Aur05] and included here for convenience):

- *Modifier:* This field contains a 128-bit unsigned integer, which can be any value. The modifier is used during CGA generation to implement the hash extension and to enhance privacy by adding randomness to the address.

- *Subnet Prefix:* This field contains the 64-bit subnet prefix of the CGA (that is, the Mobile Network Prefix when VARON is used).

- *Collision Count:* This is an eight-bit unsigned integer that must be 0, 1, or 2. The collision count is incremented during CGA generation to recover from an address collision detected by Duplicate Address Detection (DAD).

- *Public Key:* This is a variable-length field containing the public key of the address owner. The public key must be formatted as a DER-encoded ASN.1 structure of the type SubjectPublicKeyInfo, defined in the Internet X.509 certificate profile [HFPS02].

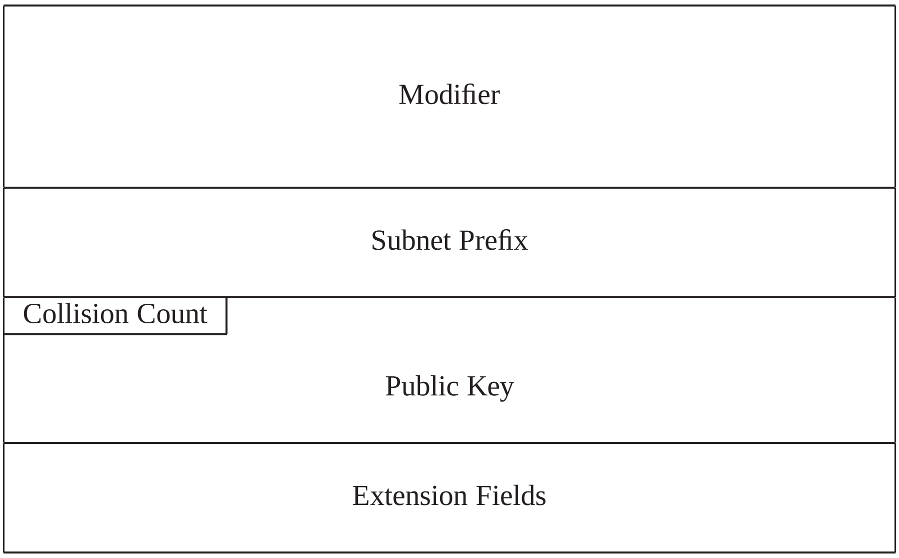


Figure B.4: CGA parameters format.

VARON should use an RSA public/private key pair. When RSA is used, the algorithm identifier must be rsaEncryption, which is 1.2.840.113549.1.1.1, and the RSA public key must be formatted by using the RSAPublicKey type as specified in Section 2.3.1 of RFC 3279 [PHB02]. The RSA key length should be at least 384 bits.

Other public key types are undesirable in VARON, as they may result in incompatibilities between implementations. The length of this field is determined by the ASN.1 encoding.

- *Extension Fields:* This is an optional variable-length field that is not used in the current specification of CGA [Aur05]. Future versions of the CGA specification may use this field for additional data items that need to be included in the CGA Parameters data structure. Implementations must ignore the value of any unrecognised extension fields.

B.5. RSA Signature option

The format of the RSA Signature option, defined in Section 5.2 of RFC 3971 [AKZN05], is shown in Figure B.5 and described next:

- *Type:* 12

- *Length:* The length of the option (including the Type, Length, Reserved, Key Hash, Digital Signature, and Padding fields) in units of 8 octets.

- *Reserved:* A 16-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.

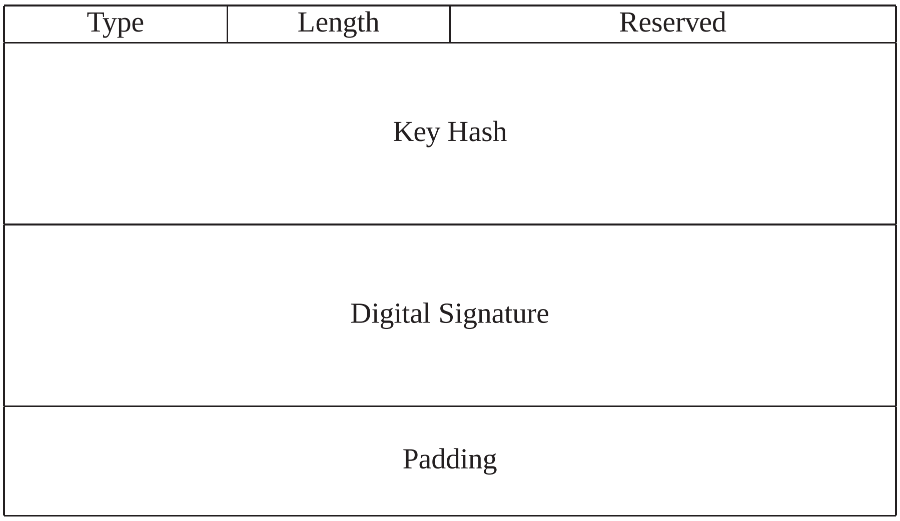


Figure B.5: RSA Signature option format.

- *Key Hash:* A 128-bit field containing the most significant (leftmost) 128 bits of a SHA-1 hash of the public key used for constructing the signature. The SHA-1 hash is taken over the presentation used in the Public Key field of the CGA Parameters data structure carried in the CGA option. Its purpose is to associate the signature to a particular key known by the receiver. Such a key can either be stored in the certificate cache of the receiver or be received in the CGA option in the same message.

- *Digital Signature:* A variable-length field containing a PKCS#1 v1.5 signature, constructed by using the sender's private key over the following sequence of octets:

  1. The 8-bit Type and 8-bit Reserved fields from the VARON message (the 16-bit Care-of Nonce index is set to zero for this computation).
  2. The 32-bit Nonce fields from the VARON message.
  3. The 128-bit Source Address (that is, the Home Address of the sender MR) field from the IP header.
  4. The 128-bit Destination Address field from the IP header.
  5. The variable-length CGA option.
  6. If the message is forwarded by an intermediate MR, then the CGA option and RSA signature of the originator MR.

  The signature value is computed with the RSASSA-PKCS1-v1_5 algorithm and SHA-1 hash, as defined in [Lab02].

  This field starts after the Key Hash field. The length of the Digital Signature field is determined by the length of the RSA Signature option minus the length of the other fields (including the variable length Padding field).

Type	Reserved	Care-of Nonce index
Nonce		
Originator HoA		
Target HoA		
CGA option (target MR)		
RSA Signature option (target MR)		
Care-of Init cookie		
Care-of Keygen token token		

Figure B.6: CoRT message option (sent by the originator MR) format.

- *Padding:* This variable-length field contains padding, as many bytes long as remain after the end of the signature.

B.6. Care-of Route Test (CoRT)

This message option is sent by the target MR in response to a CoRTI message. The source IP address of the UDP packet containing this option is set to the target MR's HoA and the destination IP address is set to the originator MR's HoA. This option has the format shown in Figure B.6. The option fields are analogous to the ones included in the CoRTI message (in this case the nonce value is a copy of the nonce received in the CoRTI message, N_A).

As in the CoRTI case, the format of a CoRT message forwarded by an intermediate MR is slightly different, since the forwarder MR has to add its CGA information and signature. The format of this option is shown in Figure B.7.

B.7. Home Route Test (HoRT)

This message option is sent by the target MR, routed through the infrastructure. The source and destination IP addresses of the UDP packet carrying this option are set to the respective MRs' HoAs. This option has the format shown in Figure B.8. Next, a brief

<table>
<tr><td>Type</td><td>Reserved</td><td colspan="2">Care-of Nonce index</td></tr>
<tr><td colspan="4">Nonce</td></tr>
<tr><td colspan="4">Originator
HoA</td></tr>
<tr><td colspan="4">Target
HoA</td></tr>
<tr><td colspan="4">CGA option (target MR)</td></tr>
<tr><td colspan="4">RSA Signature option (target MR)</td></tr>
<tr><td colspan="4">CGA option (forwarder MR)</td></tr>
<tr><td colspan="4">RSA Signature option (forwarder MR)</td></tr>
<tr><td colspan="4">Care-of Init
cookie</td></tr>
<tr><td colspan="4">Care-of Keygen token
token</td></tr>
</table>

Figure B.7: CoRT message option (forwarded by an intermediate MR) format.

description of each field is provided:

- *Type:* 8-bit selector. It identifies the HoRT option.
- *Reserved 1:* 24-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.
- *Home Nonce index:* 16-bit field which contains the nonce used by the sender MR to generate the Home-of Keygen token. This field will be echoed back by the recipient MR in a subsequent Mobile Network Prefix Binding Update.
- *Reserved 2:* 16-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.
- *Home Init cookie:* 64-bit field which contains a random value, the Home Init cookie.
- *Home Keygen token:* This field contains the 64 bit Home Keygen token used in Care-of Route authentication signalling.

<table>
<tr><td>Type</td><td colspan="3">Reserved 1</td></tr>
<tr><td colspan="2">Home Nonce index</td><td colspan="2">Reserved 2</td></tr>
<tr><td colspan="4">Home Init
cookie</td></tr>
<tr><td colspan="4">Home Keygen token
token</td></tr>
</table>

Figure B.8: HoRT message option format.

<table>
<tr><td>Type</td><td colspan="3">Reserved 1</td></tr>
<tr><td colspan="2">Home Nonce index</td><td colspan="2">Care-of Nonce index</td></tr>
<tr><td colspan="4">Authenticator</td></tr>
<tr><td colspan="4">Reserved 2</td></tr>
</table>

Figure B.9: MNPBU message option format.

B.8. Mobile Network Prefix Binding Update (MNPBU)

This message option is sent by the MR to set-up a Care-of Route to the recipient MR. The source and destination IP addresses of the UDP packet are set to the respective MRs' HoAs. This option has the format shown in Figure B.9. All the option fields but the last one have been already described:

- *Authenticator:* 96-bit field which contains the *authenticator* data calculated as defined in Section 6.2.7 of RFC 3775 [JPA04]:

$$Mobility\ Data = sender\ MR's\ HoA \mid recipient\ MR's\ HoA$$

$$Authenticator = First\,(96,\ HMAC_{SHA1}\,(K_{bm},\ Mobility\ Data))$$

B.9. Home Address Advertisement (HoAA)

This message option is periodically sent by every MR. The source IP address of the UDP packet is set to the sender MR's HoA and the destination IP address is set to the *link-local All Routers* multicast IPv6 address (FF02:0:0:0:0:0:0:2) [HD06]. The TTL of the packet is set to `VARONC_HOAA_TTL_MAX` (default value: 10). This option has the format shown in Figure B.10. Next, a brief description of each field is provided:

- *Type:* 8-bit selector. It identifies the HoAA option.
- *Reserved:* 8-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.

<table>
<tr><td>Type</td><td>Reserved</td><td colspan="2">Lifetime</td></tr>
<tr><td colspan="4">Nonce</td></tr>
<tr><td colspan="4">Home
Address</td></tr>
</table>

Figure B.10: HoAA message option format.

- *Lifetime:* 16-bit unsigned integer. The lifetime associated with the Home Address advertisement contained in this option in units of seconds. The maximum value corresponds to 18.2 hours. A value of 0 must not be used.

- *Home Address:* The Home Address (128-bit) of the sender Mobile Router (from which the MNP of the sender MR may be inferred). This address must be a unicast routable address and it must be the same than the source address of the IP packet that contains this option.

- *Nonce:* 32-bit field which contains a nonce issued by the sender MR to uniquely identify a HoAA coming from a MR and, in this way, avoid the processing of already received HoAA messages.

B.10. Care-of Route Error (CoRE)

This message option is sent by an intermediate MR when detects that a route from *Source HoA* to *Destination HoA* is broken. The source IP address of the UDP packet is set to the sender MR's HoA and the destination IP address is set its neighbour towards *Source HoA*. This option has the format shown in Figure B.11. Next, a brief description of each field is provided:

- *Type:* 8-bit selector. It identifies the CoRE option.

- *Reserved:* 24-bit field reserved for future use. The value must be initialised to zero by the sender, and must be ignored by the receiver.

- *Nonce:* 32-bit field which contains the Nonce N_C issued by the sender MR. It is meant for ensuring the CoRE message freshness.

- *Source HoA:* The Home Address (128-bit) of the source end of the route that is broken.

- *Destination HoA:* The Home Address (128-bit) of the destination end of the route that is broken.

- *CGA option (sender MR):* A variable length field containing the CGA option data structure (as defined in Section 5.1 of RFC 3971 [AKZN05]) of the sender MR.

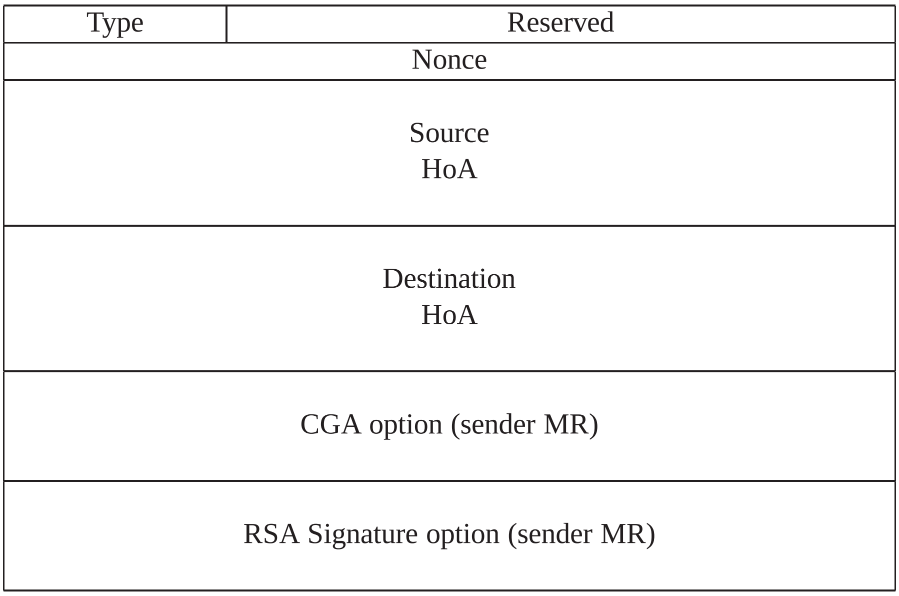


Figure B.11: CoRE message option format.

- *RSA Signature option (sender MR):* A variable length field containing the RSA Signature option (as defined in Section 5.2 of RFC 3971 [AKZN05]). This field contains the signature of the CoRE message.

As in the case of CoRTI and CoRT messages, the format of the CoRE option is slightly different when the message is forwarded by an intermediate MR along the path to Source MR, since the message includes also the signature of the MR forwarding the message (see Figure B.12).

<table>
<tr><td>Type</td><td>Reserved</td></tr>
<tr><td colspan="2">Nonce</td></tr>
<tr><td colspan="2">Source
HoA</td></tr>
<tr><td colspan="2">Destination
HoA</td></tr>
<tr><td colspan="2">CGA option (sender MR)</td></tr>
<tr><td colspan="2">RSA Signature option (sender MR)</td></tr>
<tr><td colspan="2">CGA option (forwarder MR)</td></tr>
<tr><td colspan="2">RSA Signature option (forwarder MR)</td></tr>
</table>

Figure B.12: CoRE message option (forwarded by an intermediate MR along the path) format.

References

[AAK$^+$02] Jari Arkko, Tuomas Aura, James Kempf, Vesa-Matti Mäntylä, Pekka Nikander, and Michael Roe. Securing IPv6 Neighbor and Router Discovery. In *Proceedings of the 3rd ACM workshop on Wireless security (WiSE '02)*, pages 77–88, 2002.

[ABB$^+$06] Rui Aguiar, Albert Banchs, Carlos J. Bernardos, María Calderón, Marco Liebsch, Telemaco Melia, Piotr Pacyna, Susana Sargento, and Ignacio Soto. Scalable QoS-aware Mobility for Future Mobile Operators. *IEEE Communications Magazine*, 44(6), June 2006.

[ABV$^+$04] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson, and Henrik Levkowetz. Extensible Authentication Protocol (EAP). Internet Engineering Task Force, RFC 3748 (Proposed Standard), June 2004.

[ADA$^+$04] Soren Vang Andersen, Alan Duric, Henrik Astrom, Roar Hagen, W. Bastiaan Kleijn, and Jan Linden. Internet Low Bit Rate Codec (iLBC). Internet Engineering Task Force, RFC 3951 (Experimental), December 2004.

[aIMY05] Toshihiro Suzuki andKen Igarashi, Akira Miura, and Masami Yabusaki. Care-of Prefix Routing for Moving Networks. *IEICE Transactions on Communications*, E88-B(7):2756–2764, July 2005.

[AKZN05] Jari Arkko, James Kempf, Brian Zill, and Pekka Nikander. SEcure Neighbor Discovery (SEND). Internet Engineering Task Force, RFC 3971 (Proposed Standard), March 2005.

[Aur03] Tuomas Aura. Cryptographically generated addresses (CGA). In *Proc. 6th Information Security Conference (ISC'03)*, volume 2851 of *Lecture Notes in Computer Science*, pages 29–43, Bristol, UK, October 2003. Springer.

[Aur05] Tuomas Aura. Cryptographically Generated Addresses (CGA). Internet Engineering Task Force, RFC 3972 (Proposed Standard), March 2005.

[AVH06] Jari Arkko, Christian Vogt, and Wassim Haddad. Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6). Internet Engineering Task Force, draft-arkko-mipshop-cga-cba-04.txt (work in progress), June 2006.

[AVN00] Oreste Andrisano, Roberto Verdone, and Masao Nakagawa. Intelligent transportation systems: the role of third generation mobile radio networks. *IEEE Communications Magazine*, 38(9):144–151, September 2000.

[AWD04] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Elsevier journal of Ad Hoc Networks*, 2:1–22, 2004.

[AWW05] Ian F. Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. *Computer Networks*, 47:445–487, 2005.

[Bag04] Marcelo Bagnulo. Application of a multi6 protocol to nemo. Internet Engineering Task Force, draft-bagnulo-nemo-multi6-00.txt (work-in-progress), November 2004.

[BB04] John Bender and Don Bowman. Global Network Mobility. Presented at RIPE 48, May 2004.

[BBC04] Carlos J. Bernardos, Marcelo Bagnulo, and María Calderón. MIRON: MIPv6 Route Optimization for NEMO. In *Proceedings of the 4th Workshop on Applications and Services in Wireless Networks (ASWN 2004)*, pages 189–197, Boston, MA, USA, August 2004.

[BBCS05] Carlos J. Bernardos, Marcelo Bagnulo, María Calderón, and Ignacio Soto. Mobile IPv6 Route Optimisation for Network Mobility (MIRON). draft-bernardos-nemo-miron-00.txt (work-in-progress), July 2005.

[BC05] Carlos J. Bernardos and María Calderón. Survey of IP address autoconfiguration mechanisms for MANETs. Internet Engineering Task Force, draft-bernardos-manet-autoconf-survey-00.txt (work-in-progress), July 2005. Presented at 63rd IETF.

[BC06] Carlos J. Bernardos and María Calderón. A DHCP-based IP address autoconfiguration for MANETs. In *Proceedings of the I International Conference on Ubiquitous Computing: Applications, Technology and Social Issues (ICUC 2006)*, pages 59–62, Alcalá de Henares (Spain), June 2006.

[BCS$^+$06] Carlos J. Bernardos, María Calderón, Ignacio Soto, Fernando Boavida, and Arturo Azcorra. VARON: Vehicular Ad-hoc Route Optimisation for NEMO. *Computer Communications*, 2006. submitted.

[BGMBA06] Marcelo Bagnulo, Alberto García-Martínez, Carlos J. Bernardos, and Arturo Azcorra. Scalable Support for Globally Moving Networks. In *Proceedings of the 3rd International Symposium on Wireless Communication Systems (ISWCS)*, Valencia (Spain), September 2006.

[BMA$^+$04] Mounir Benzaid, Pascale Minet, Khaldoun Al Agha, Cedric Adjih, and Geraud Allard. Integration of Mobile-IP and OLSR for a Universal Mobility. *Wireless Networks*, 10(4):221–250, July 2004.

[BN06] Marcelo Bagnulo and Erik Nordmark. Level 3 multihoming shim protocol. Internet Engineering Task Force, draft-ietf-shim6-proto-04.txt (work-in-progress), March 2006.

[BOC$^+$06] Carlos J. Bernardos, Antonio De La Oliva, María Calderón, Dirk von Hugo, and Holger Kahle. NEMO: Network Mobility. Bringing ubiquity to the Internet access. Demonstration at IEEE INFOCOM 2006, April 2006.

[BS04] Salman A. Baset and Henning Schulzrinne. An analysis of the skype peer-to-peer internel telephony protocol, 2004.

[BSC$^+$05a] Carlos J. Bernardos, Ignacio Soto, María Calderón, Dirk von Hugo, and Emmanuel Riou. NEMO: Movilidad de Redes en IPv6. *Novatica*, 174:37–43, March-April 2005.

[BSC$^+$05b] Carlos J. Bernardos, Ignacio Soto, María Calderón, Dirk von Hugo, and Emmanuel Riou. NEMO: Network Mobility in IPv6. *UPGRADE - The European Journal for the Informatics Professional*, VI(2):36–42, April 2005.

[BSM$^+$05] Carlos J. Bernardos, Ignacio Soto, José Ignacio Moreno, Telemaco Melia, Marco Liebsch, and Ralf Schmitz. Experimental evaluation of a handover optimization solution for multimedia applications in a mobile IPv6 network. *European Transactions on Telecommunications*, 16(4):317–328, April 2005.

[BW05] Marc Bechler and Lars Wolf. Mobility Management for Vehicular Ad Hoc Networks. In *Proceedings of the 61st IEEE Semiannual Vehicular Technology Conference. VTC 2005-Spring*, volume 4, pages 2294 – 2298, June 2005.

[BWSF03] Marc Bechler, Lars Wolf, Oliver Storz, and Walter J. Franz. Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems. In *Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference. VTC 2003-Spring*, volume 2, pages 965–969, April 2003.

[BYK$^+$05] Sungmin Baek, Jinkyu Yoo, Taekyoung Kwon, Eunkyoung Paik, and Minji Nam. Routing Optimization in the same nested mobile network. Internet Engineering Task Force, draft-baek-nemo-nested-ro-00.txt (work-in-progress), October 2005.

[CAI06] Pulak K Chowdhury, Mohammed Atiquzzaman, and William Ivancic. SINEMO: An IP-diversity based Approach for Network Mobility in Space. In *Proceedings of the Second IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT 20006)*, pages 109–115, July 2006.

[CBB$^+$06] María Calderón, Carlos J. Bernardos, Marcelo Bagnulo, Ignacio Soto, and Antonio de la Oliva. Design and Experimental Evaluation of a Route Optimisation Solution for NEMO. *IEEE Journal on Selected Areas in Communications*, 24(9):1702–1716, September 2006.

[CBBS05] María Calderón, Carlos J. Bernardos, Marcelo Bagnulo, and Ignacio Soto. Securing Route Optimisation in NEMO. In *Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT)*, pages 248–254, Trentino, ITALY, April 2005.

[CBH03] Srdjan Capkun, Levente Buttyán, and Jean-Pierre Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64, January-March 2003.

[CBW05] Thomas Clausen, Emmanuel Baccelli, and Ryuji Wakikawa. Route Optimization in Nested Mobile Networks (NEMO) using OLSR. In *Proceedings of the IASTED International Conference on Networks and Communication Systems (NCS 2005)*, April 2005.

[CCL03] Imrich Chlamtac, Marco Conti, and Jennifer J.-N. Liu. Mobile ad hoc networking: imperatives and challenges. *Elsevier journal of Ad Hoc Networks*, 1:13–64, 2003.

[Chi99] J. Nöel Chiappa. Endpoints and Endpoint Names: A proposed Enhancement to the Internet Architecture. Internet Draft, 1999.

[CJ03] Thomas Heide Clausen and Philippe Jacquet. Optimized Link State Routing Protocol (OLSR). Internet Engineering Task Force, RFC 3626 (Experimental), October 2003.

[CKC06] Hosik Cho, Taekyoung Kwon, and Yanghee Choi. Route Optimization Using Tree Information Option for Nested Mobile Networks. *IEEE Journal on Selected Areas in Communications*, 24(9):1717–1724, September 2006.

[CM99] M. Scott Corson and Joseph Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Internet Engineering Task Force, RFC 2501 (Informational), January 1999.

[CPC04] Hosik Cho, Eun Kyoung Paik, and Yanghee Choi. HMRA: Hierarchical Mobile Router Advertisement for Nested Mobile Networks. In *Proceedings of the First IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, pages 78–80, January 2004.

[CSB$^+$04] Antonio Cuevas, Pablo Serrano, Carlos J. Bernardos, José Ignacio Moreno, Jurgen Jaehnert, H-W. Kim, Jie Zhou, Diogo Gomes, Pedro Gonçalves, and Rui L. Aguiar. Field Evaluation of a 4G True-IP network. In *Proceedings of the 13th IST Mobile Summit*, volume 1, pages 277–281, Lyon, FRANCE, 2004.

[CSM$^+$05] Antonio Cuevas, Pablo Serrano, José Ignacio Moreno, Carlos J. Bernardos, Jürgen Jähnert, Rui L. Aguiar, and Victor Marques. Usability and Evaluation of a Deployed 4G Network Prototype. *Journal of Communications and Networks*, 7(2):222–230, June 2005.

[DBV+03] Ralph Droms, Jim Bound, Bernie Volz, Ted Lemon, Charles E. Perkins, and Mike Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Internet Engineering Task Force, RFC 3315 (Proposed Standard), July 2003.

[DH98] Stephen E. Deering and Robert M. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Internet Engineering Task Force, RFC 2460 (Draft Standard), December 1998.

[dlOBC05] Antonio de la Oliva, Carlos J. Bernardos, and María Calderón. Practical evaluation of a network mobility solution. In *Proceedings of the EUNICE 2005: Networked Applications - 11th Open European Summer School*, pages 60–66, Colmenarejo, Madrid (SPAIN), July 2005.

[dlOBC06] Antonio de la Oliva, Carlos J. Bernardos, and María Calderón. EUNICE 2005: Networks and Applications Towards a Ubiquitously Connected World. In *Practical Evaluation of a Network Mobility Solution*, IFIP International Federation for Information Processing, pages 133–144. Springer Boston, 2006.

[Dro97] Ralph Droms. Dynamic Host Configuration Protocol. Internet Engineering Task Force, RFC 2131 (Draft Standard), March 1997.

[Dul05] Andrew L. Dul. Global IP Network Mobility Using Border Gateway Protocol (BGP). Presented at 62nd IETF, March 2005.

[Dul06] Andrew L. Dul. Global IP Network Mobility using Border Gateway Protocol (BGP). Technical report, The Boeing Company, March 2006.

[DWPT05] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. Network Mobility (NEMO) Basic Support Protocol. Internet Engineering Task Force, RFC 3963 (Proposed Standard), January 2005.

[EC04] Thierry Ernst and Julien Charbon. Multihoming with NEMO Basic Support. In *Proceedings of the First International Conference on Mobile Computing and Ubiquitous Computing (ICMU)*, January 2004.

[EL06] Thierry Ernst and Hong-Yon Lach. Network Mobility Support Terminology. Internet Engineering Task Force, draft-ietf-nemo-terminology-05.txt (work-in-progress), March 2006.

[EMU03] Thierry Ernst, Koshiro Mitsuya, and Keisuke Uehara. Network Mobility from the InternetCAR perspective. *Journal of Interconnection Networks (JOIN)*, 4(3):329–343, September 2003.

[EOB+02] Thierry Ernst, Alexis Olivereau, Ludovic Bellier, Claude Castelluccia, and Hong-Yon Lach. Mobile Networks Support in Mobile IPv6. Internet Engineering Task Force, draft-ernst-mobileip-v6-network-03.txt (work-in-progress), March 2002.

[EP02] Mustafa Ergen and Anuj Puri. MEWLANA-Mobile IP Enriched Wireless Local Area Network Architecture. In *Proceedings of the IEEE 56th Semiannual Vehicular Technology Conference. VTC 2002-Fall*, volume 4, pages 2449–2453, 2002.

[Ern05] Thierry Ernst. Network Mobility Support Goals and Requirements. Internet Engineering Task Force, draft-ietf-nemo-requirements-05.txt (work-in-progress), October 2005.

[Ern06] Thierry Ernst. The information technology era of the vehicular industry. *SIGCOMM Computer Communication Review*, 36(2):49–52, 2006.

[Esa04] Hiroshi Esaki. Multi-Homing and Multi-Path Architecture Using Mobile IP and NEMO Framework. In *Proceedings of the 2004 International Symposium on Applications and the Internet*, page 6, 2004.

[EU02] Thierry Ernst and Keisuke Uehara. Connecting Automobiles to the Internet. In *Proceedings of the ITST workshop*, November 2002.

[FJL00] Magnus Frodigh, Per Johansson, and Peter Larsson. Wireless ad hoc networking–The art of networking without a network. *Ericsson Review*, 4:248–263, 2000.

[FOP+06] Dan Forsberg, Yoshihiro Ohba, Basavaraj Patil, Hannes Tschofenig, and Alper E. Yegin. Protocol for Carrying Authentication for Network Access (PANA). Internet Engineering Task Force, draft-ietf-pana-pana-11.txt (work-in-progress), March 2006.

[FSK+06] Hanane Fathi, SeongHan Shin, Kazukuni Kobara, Shyam S. Chakraborty, Hideki Imai, and Ramjee Prasad. LR-AKE-Based AAA for Network Mobility (NEMO) Over Wireless Links. *IEEE Journal on Selected Areas in Communications*, 24(9):1725–1737, September 2006.

[FTMT+05] Holger Füßler, Marc Torrent-Moreno, Matthias Transier, Andreas Festag, and Hannes Hartenstein. Thoughts on a Protocol Architecture for Vehicular Ad-Hoc Networks. In *Proc. of 2nd International Workshop in Intelligent Transportation (WIT 2005)*, pages 41–45, Hamburg, Germany, March 2005.

[GYK04] ZhiJun Gu, Dongmin Yang, and Cheeha Kim. Mobile IPv6 extensions to support nested mobile networks. In *Proceedings of the 18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004*, volume 1, pages 488–491, 2004.

[HBC01] Jean-Pierre Hubaux, Levente Buttyán, and Srdan Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '01)*, pages 146–155, 2001.

[HCH06] Youn-Hee Han, JinHyeock Choi, and Seung-Hee Hwang. Reactive Handover Optimization in IPv6-Based Mobile Networks. *IEEE Journal on Selected Areas in Communications*, 24(9):1758–1772, September 2006.

[HD06] Robert M. Hinden and Stephen E. Deering. IP Version 6 Addressing Architecture. Internet Engineering Task Force, RFC 4291 (Draft Standard), February 2006.

[Hen03] Thomas R. Henderson. Host Mobility for IP Networks: A comparison. *IEEE Network*, 17:18–26, November/December 2003.

[HFPS02] Russell Housley, Warwick Ford, Tim Polk, and David Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force, RFC 3280 (Proposed Standard), April 2002. Updated by RFC 4325.

[HJP02] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networksu. In *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*, pages 3–13, June 2002.

[HLWC05] Ren-Hung Hwang, Cheng-Ying Li, Chiung-Ying Wang, and Yuh-Shyan Chen. Mobile IPv6-based ad hoc networks: its development and application. *IEEE Journal on Selected Areas in Communications*, 23(11):2161–2171, November 2005.

[HLZ06] Chung-Ming Huang, Chao-Hsien Lee, and Ji-Ren Zheng. A Novel SIP-Based Route Optimization for Network Mobility. *IEEE Journal on Selected Areas in Communications*, 24(9):1682–1691, September 2006.

[HPJ05] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*, 11(1-2):21–38, January 2005.

[HPT97] Ralf Hauser, Tony Przygienda, and Gene Tsudikt. Reducing The Cost Of Security In Link-State Routing. In *Proceedings of the 1997 Symposium on Network and Distributed System Security*, pages 93–99, 1997.

[HSFN04] Vinh Dien Hoang, Zhenhai Shao, Masayuki Fujise, and Hoang Minh Nguyen. A Novel Solution for Global Connectivity in MANET. In *Proceedings of the IEEE 60th Semiannual Vehicular Technology Conference. VTC 2004-Fall*, volume 4, pages 2810–2823, September 2004.

[HY03] Suk Yu Hui and Kai Hau Yeung. Challenges in the Migration to 4G Mobile Systems. *IEEE Communications Magazine*, 41(12):54–59, December 2003.

[JAL$^+$00] Ulf Jonsson, Fredrik Alriksson, Tony Lasson, Per Johansson, and Gerald Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad Hoc Networks. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, pages 75–85, 2000.

[JBB92] V. Jacobson, R. Braden, and D. Borman. TCP Extensions for High Performance. Internet Engineering Task Force, RFC 1323 (Proposed Standard), May 1992.

[JdLC01] William H. Jones and Michael de La Chapelle. Connexion by Boeing (SM)-Broadband Satellite Communication System for Mobile Platforms. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*, volume 2, pages 755–758, 2001.

[JLO+06] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy, and A. Yegin. PANA Framework. Internet Engineering Task Force, draft-ietf-pana-framework-06.txt (work-in-progress), March 2006.

[JLPK04a] Jaehoon Jeong, Kyeongjin Lee, Jungsoo Park, and Hyoungjun Kim. Route Optimization based on ND-Proxy for Mobile Nodes in IPv6 Mobile Networks. In *Proceedings of the 59th IEEE Semiannual Vehicular Technology Conference. VTC 2004-Spring*, volume 5, pages 2461–2465, May 2004.

[JLPK04b] Jaehoon Paul Jeong, Kyeongjin Lee, Jungsoo Park, and Hyoungjun Kim. ND-Proxy based Route and DNS Optimizations for Mobile Nodes in Mobile Network. Internet Engineering Task Force, draft-jeong-nemo-ro-ndproxy-02.txt (work-in-progress), February 2004.

[JMB01] David B. Johnson, David A. Maltz, and Josh Broch. *Ad Hoc Networking*, chapter 5, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, pages 139–172. Addison-Wesley, 2001.

[JMH04] David B. Johnson, David A. Maltz, and Yih-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). Internet Engineering Task Force, draft-ietf-manet-dsr-10.txt (work-in-progress), July 2004.

[JPA04] David B. Johnson, Charles E. Perkins, and Jari Arkko. Mobility Support in IPv6. Internet Engineering Task Force, RFC 3775 (Proposed Standard), June 2004.

[KBS+01] Wolfganf Kellerer, Christian Bettstetter, Christian Schwingenschlogl, Peter Sties, Karl-Ernst Steinberg, and Hans-Jörg Vögel. (Auto) Mobile Communication in a Heterogeneous and Converged World. *IEEE Personal Communications*, 8(6):41–47, December 2001.

[KCC05] Stuart Kurkowski, Tracy Camp, and Michael Colagrosso. MANET Simulation Studies: The Incredibles. *Mobile Computing and Communications Review*, 9(4):50–60, October 2005.

[KKH+03] Hyunsik Kang, Keecheon Kim, Sunyoung Han, Kyeong-Jin Lee, and Jung-Soo Park. Route Optimization for Mobile Network by Using Bi-directional Between Home Agent and Top Level Mobile Router. Internet Engineering Task Force, draft-hkang-nemo-ro-tlmr-00.txt (work-in-progress), June 2003.

[KLE05] Romain Kuntz, Jean Lorchat, and Thierry Ernst. Real-life demonstrations using IPv6 and mobility support mechanisms. In *Proceedings of the Journéees Scientifiques Francophones (JSF)*, November 2005.

[KMI$^+$04] Masayuki Kumazawa, Taisuke Matsumoto, Shinkichi Ikeda, Makoto Funabiki, Hirokazu Kobayashi, and Toyoki Kawahara. Router Selection for Moving Networks. In *Proceedings of the First IEEE Consumer Communications and Networking Conference, 2004. CCNC 2004*, pages 99–104, January 2004.

[KMW06] Romain Kuntz, Koshiro Mitsuya, and Ryuji Wakikawa. Performance Evaluation of NEMO Basic Support Implementations. In *Proceedings of The First International Workshop on Network Mobility (WONEMO)*, January 2006.

[Koo05] Rajeev Koodli. Fast Handovers for Mobile IPv6. Internet Engineering Task Force, RFC 4068 (Experimental), July 2005.

[KT01] Mansour J. Karam and Fouad A. Tobagi. Analysis of the Delay and Jitter of Voice Traffic Over the Internet. In *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 2, pages 824–833. IEEE, April 2001.

[Lab02] RSA Laboratories. RSA Encryption Standard, Version 2.1. PKCS, November 2002.

[Lam81] Leslie Lamport. Password Authentication with Insecure Communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[LD03] Eliot Lear and Ralph Droms. What's in a name: Thoughts from the nsrg. Internet Research Task Force, draft-irtf-nsrg-report-10.txt (work in progress), September 2003.

[LG04] David Lundberg and Per Gunningberg. Feasibility study of WLAN technology for the Uppsala - Stockholm commuter train. Technical report, Uppsala University, Department of Information Technology, June 2004.

[LJP03] Hong-Yon Lach, Christophe Janneteau, and Alexandru Petrescu. Network Mobility in Beyond-3G. *IEEE Communications Magazine*, 41(7):52–57, July 2003.

[LJPK04] Kyeong-Jin Lee, Jae-Hoon Jeong, Jung-Soo Park, and Hyoung-Jun Kim. Route Optimization for Mobile Nodes in Mobile Network based on Prefix Delegation. Internet Engineering Task Force, draft-leekj-nemo-ro-pd-02.txt (work-in-progress), February 2004.

[LLKC05] Hyung-Jin Lim, Dong-Young Lee, Tae-Kyung Kim, and Tai-Myoung Chung. A Model and Evaluation of Route Optimization in Nested NEMO Environment. *IEICE Transactions on Communications*, E88-B(7):2765–2776, July 2005.

[LN03] Hong-Yon Lach and Nat Natarajan. Support of Mobile Networks in B3G Systems. In *Proceedings of the International Conference on Communication Technology Proceedings (ICCT)*, volume 2, pages 1381–1383, April 2003.

[MBJ01] David A. Maltz, Josh Broch, and David B. Johnson. Lessons from a Full-Scale Multihop Wireless Ad Hoc Network Testbed. *IEEE Personal Communications*, 8(1):8–15, February 2001.

[MC00a] Warren Matthews and Les Cottrell. The PingER project: active Internet performance monitoring for the HENP community. *IEEE Communications Magazine*, 38(5):130–136, May 2000.

[MC00b] Sean McCreary and Kc Claffy. Trends in wide area IP traffic patterns - A view from Ames Internet Exchange. Technical report, CAIDA, 2000.

[MC02] Gabriel Montenegro and Claude Castelluccia. Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. In *Proceedings of the Symposium Network and Distributed Systems Security (NDSS)*, pages 87–99, 2002.

[MdlOS$^+$06] Telemaco Melia, Antonio de la Oliva, Ignacio Soto, Carlos J. Bernardos, and Albert Vidal. Analysis of the effect of mobile terminal speed on WLAN/3G vertical handovers. In *Proceedings of the 2006 IEEE Global Telecommunications Conference (GLOBECOM)*, San Francisco, California (USA), November 2006.

[MEN04] Nicolas Montavont, Thierry Ernst, and Thomas Noel. Multihoming in Nested Mobile Networking. In *Proceedings of the 2004 International Symposium on the Applications and the Internet Workshops, 2004. SAINT 2004 Workshops*, pages 184–189, January 2004.

[MIUM05] Koshiro Mitsuya, Manabu Isomura, Keisuke Uehara, and Jun Murai. Adaptive Application for Mobile Network Environment. In *Proceedings of the 5th International Conference on ITS Telecommunications (ITST)*, pages 211–214, June 2005.

[MK04] Jukka Manner and Markku Kojo. Mobility Related Terminology. Internet Engineering Task Force, RFC 3753 (Informational), June 2004.

[MN05] Robert Moskowitz and Pekka Nikander. Host Identity Protocol Architecture. Internet Engineering Task Force, draft-ietf-hip-arch-03.txt (work-in-progress), August 2005.

[MNJH06] Robert Moskowitz, Pekka Nikander, Petri Jokela, and Thomas R. Henderson. Host Identity Protocol. Internet Engineering Task Force, draft-ietf-hip-base-05.txt (work-in-progress), March 2006.

[MUM03] Koshiro Mitsuya, Keisuke Uehara, and Jun Murai. The In-vehicle Router System to support Network Mobility. In *Information Networking: Networking*

Technologies for Enhanced Internet Services, volume 2662 of *Lecture Notes in Computer Science*, pages 633–642. Springer-Verlag Heidelberg, October 2003.

[NA03] Pekka Nikander and Jari Arkko. Security protocols. In *Delegation of Signalling Rights*, number 2845 in Lecture Notes in Computer Science, pages 203–214. Springer Berlin / Heidelberg, 2003.

[NAA$^+$05] Pekka Nikander, Jaru Arkko, Tuomas Aura, Gabriel Montenegro, and Erik Nordmark. Mobile IP Version 6 Route Optimization Security Design Background. Internet Engineering Task Force, RFC 4225 (Informational), December 2005.

[NCK$^+$03] Jongkeun Na, Seongho Cho, Chongkwon Kim, Sungjin Lee, Hyunjeong Kang, and Changhoi Koo. Secure Nested Tunnels Optimization using Nested Path Information. Internet Engineering Task Force, draft-na-nemo-nested-path-info-00.txt (work-in-progress), September 2003.

[NCK$^+$04] Jongkeun Na, Seongho Cho, Chongkwon Kim, Sungjin Lee, Hyunjeong Kang, and Changhoi Koo. Route Optimization Scheme based on Path Control Header. Internet Engineering Task Force, draft-na-nemo-path-control-header-00.txt (work-in-progress), April 2004.

[NE04] Chan-Wah Ng and Thierry Ernst. Multiple Access Interfaces for Mobile Nodes and Networks. In *Proceedings of the 12th IEEE International Conference on Networks, 2004. (ICON 2004)*, volume 2, pages 774–779, November 2004.

[NH04a] Chan-Wah Ng and Jun Hirano. Extending Return Routability Procedure for Network Prefix (RRNP). Internet Engineering Task Force, draft-ng-nemo-rrnp-00.txt (work-in-progress), October 2004.

[NH04b] Chan-Wah Ng and Jun Hirano. Securing Nested Tunnels Optimization with Access Router Option. Internet Engineering Task Force, draft-ng-nemo-access-router-option-01.txt (work-in-progress), July 2004.

[NNS98] Thomas Narten, Erik Nordmark, and William A. Simpson. Neighbor Discovery for IP Version 6 (IPv6). Internet Engineering Task Force, RFC 2461 (Draft Standard), December 1998.

[NPEB06] Chan-Wah Ng, Eun Kyoung Paik, Thierry Ernst, and Marcelo Bagnulo. Analysis of Multihoming in Network Mobility Support. Internet Engineering Task Force, draft-ietf-nemo-multihoming-issues-05.txt (work-in-progress), February 2006.

[NTWZ06] Chan-Wah Ng, Pascal Thubert, Masafumi Watari, and Fan Zhao. Network Mobility Route Optimization Problem Statement. Internet Engineering Task Force, draft-ietf-nemo-ro-problem-statement-03.txt (work-in-progress), September 2006.

[NZWT06] Chan-Wah Ng, Fan Zhao, Masafumi Watari, and Pascal Thubert. Network Mobility Route Optimization Solution Space Analysis. Internet Engineering Task Force, draft-ietf-nemo-ro-space-analysis-03.txt (work-in-progress), September 2006.

[OK04] Jörg Ott and Dirk Kutscher. The ”Drive-thru” Architecture: WLAN-based Internet Access on the Road. In *Porceedings of the IEEE 59th Semiannual Vehicular Technology Conference. VTC 2004-Spring*, volume 5, pages 2615–2622, May 2004.

[OMV$^+$06] Antonio De La Oliva, Telemaco Melia, Albert Vidal, Carlos J. Bernardos, Ignacio Soto, and Albert Banchs. A case study: IEEE 802.21 enabled mobile terminals for optimised WLAN/3G handovers. *Mobile Computing and Communications Review*, 2006. Accepted to appear.

[OST03] Hiroyuki Ohnishi, Keisuke Sakitani, and Yasushi Takagi. HMIP based Route optimization method in a mobile network. Internet Engineering Task Force, draft-ohnishi-nemo-ro-hmip-00.txt (work-in-progress), October 2003.

[OWUM04] Kouji Okada, Ryuji Wakikawa, Keisuke Uehara, and Jun Murai. OLSR for InternetCar System. In *Proceedings of the OLSR Interop and Workshop*, August 2004.

[PB94] Charles Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM’94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 1994.

[PBRD03] Charles E. Perkins, Elisabeth M. Belding-Royer, and Samir R. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Internet Engineering Task Force, RFC 3561 (Experimental), July 2003.

[PCEC04] Eun Kyoung Paik, Hosik Cho, Thierry Ernst, and Yanghee Choi. Load Sharing and Session Preservation with Multiple Mobile Routers for Large Scale Network Mobility. In *Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA)*, volume 1, pages 393–398, 2004.

[PCKC04] Eun Kyoung Paik, Hosik Cho, Taekyoung Kwon, and Yanghee Choi. Mobility-Aware Mobile Router Selection and Address Management for IPv6 Network Mobility. *Journal of Network and Systems Management*, 12(4):485–505, December 2004.

[Per02] Charles E. Perkins. IP Mobility Support for IPv4. Internet Engineering Task Force, RFC 3344 (Proposed Standard), August 2002.

[PH02] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad hoc Networks. In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, pages 193–204, January 2002.

[PHB02] Tim Polk, Russell Housley, and Larry Bassham. Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force, RFC 3279 (Proposed Standard), April 2002. Updated by RFCs 4055, 4491.

[PHS03] Eranga Perera, Robert Hsieh, and Aruna Seneviratne. Extended Network Mobility Support. Internet Engineering Task Force, draft-perera-nemo-extended-00.txt (work-in-progress), July 2003.

[PL03] Pekka Pääkkönen and Juhani Latvakoski. IPv6 Prefix Delegation-Based Addressing Solution for a Mobile Personal Area Network. In *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops*, pages 819–824, May 2003.

[PMW$^+$02] Charles E. Perkins, Jari T. Malinen, Ryuji Wakikawa, Anders Nilsson, and Antti J. Tuominen. Internet connectivity for mobile ad hoc networks. *Wireless Communications and Mobile Computing*, 2(5):465–482, August 2002.

[POD$^+$04] Christos Politis, Toshikane Oda, Sudhir Dixit, Andreas Schieder, Hong-Yon Lach, Michael I. Smirnov, Sami Uskela, and Rahim Tafazolli. Cooperative Networks for the Future Wireless World. *IEEE Communications Magazine*, 42(9):70–79, September 2004.

[Pos81] J. Postel. Transmission Control Protocol. Internet Engineering Task Force, RFC 793 (Standard), September 1981. Updated by RFC 3168.

[PPK$^+$04] Min Ho Park, Chang Min Park, Sung Hei Kim, Sung Baek Hong, and Jin Seek Choi. A Novel Routing Protocol for Personal Area Network Mobility (PANEMO) Environment. In *Proceedings of the 6th International Conference on Advanced Communication Technology*, volume 1, pages 11–14, 2004.

[PPLS06] Henrik Petander, Eranga Perera, Kun-Chan Lan, and Aruna Seneviratne. Measuring and Improving the Performance of Network Mobility Management in IPv6 Networks. *IEEE Journal on Selected Areas in Communications*, 24(9):1671–1681, September 2006.

[PSS04a] Eranga Perera, Aruna Seneviratne, and Vijay Sivaraman. Optinets: an Architecture to Enable Optimal Routing for Network Mobility. In *Proceedings of the International Workshop on Wireless Ad-Hoc Networks*, pages 68–72, May 2004.

[PSS04b] Eranga Perera, Vijay Sivaraman, and Aruna Seneviratne. Survey on Network Mobility Support. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(2):7–19, April 2004.

[RGS04] Pedro M. Ruiz and Antonio Gomez-Skarmeta. Enhanced Internet connectivity for hybrid ad hoc networks through adaptive gateway discovery. In *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pages 370–377, November 2004.

[RK03] Prashant Ratanchandani and Robin Kravets. A hybrid approach to Internet connectivity for mobile ad hoc networks. In *Proceedings of the IEEE Wireless Communications and Networking (WCNC)*, volume 3, pages 1522–1527, March 2003.

[RRGS05] Pedro M. Ruiz, Francisco J. Ros, and Antonio Gomez-Skarmeta. Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges. *IEEE Communications Magazine*, 43(10):118–125, October 2005.

[RSCS06] Simone Ruffino, Patrick Stupar, Thomas Heide Clausen, and Shubhranshu Singh. Connectivity Scenarios for MANET. Internet Engineering Task Force, draft-ruffino-autoconf-conn-scenarios-00.txt (work-in-progress), February 2006.

[RT99] Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, 6(2):46–55, April 1999.

[SA99] Frank Stajano and Ross J. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Proceedings of the 7th International Workshop on Security Protocols*, volume 1796 of *Lecture Notes In Computer Science*, pages 172–194. Springer-Verlag London, 1999.

[SB00] Alex C. Snoeren and Hari Balakrishnan. An End-to-End Approach to Host Mobility. In *MobiCom ’00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 155–166, New York, NY, USA, 2000. ACM Press.

[SBGE05] Lucian Suciu, Jean-Marie Bonnin, Karine Guillouard, and Thierry Ernst. Multiple Network Interfaces Management for Mobile Routers. In *Proceedings of the 5th International Conference on ITS Telecommunications (ITST)*, June 2005.

[SBK01] Alex C. Snoeren, Hari Balakrishnan, and M. Frans Kaashoek. Reconsidering Internet Mobility. In *Proceedings of the 8th Workshop Hot Topics in Operating Systems*, pages 41–46, May 2001.

[SBR03] Swaminathan Sundaramurthy and Elisabeth M. Belding-Royer. The AD-MIX protocol for encouraging participation in mobile ad hoc networks. In *Proceedings of the 11th IEEE International Conference on Network Protocols*, pages 156–167, November 2003.

[SBS$^+$05] Jatinder Pal Singh, Nicholas Bambos, Bhaskar Srinivasan, Detlef Clawin, and Yonchun Yan. Empirical Observations on Wireless LAN Performance in Vehicular Traffic Scenarios and Link Connectivity Based Enhancements for Multihop Routing. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, volume 3, pages 1676–1682, March 2005.

[SBSC02] Jatinder Pal Singh, Nicholas Bambos, Bhaskar Srinivasan, and Detlef Clawin. Wireless LAN Performance Under Varied Stress Conditions in Vehicular Traffic Scenarios. In *Proceedings of the IEEE 56th Semiannual Vehicular Technology Conference. VTC 2002-Fall*, volume 2, pages 743–747, 2002.

[SCFJ03] Henning Schulzrinne, Stephen L. Casner, Ron Frederick, and Van Jacobson. RTP: A Transport Protocol for Real-Time Applications. Internet Engineering Task Force, RFC 3550 (Standard), July 2003.

[SCMB05] Hesham Soliman, Claude Castelluccia, Karim El Malki, and Ludovic Bellier. Hierarchical Mobile IPv6 Mobility Management (HMIPv6). Internet Engineering Task Force, RFC 4140 (Experimental), August 2005.

[SDL$^+$02] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, and Elizabeth M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. In *Proceedings of the 10th IEEE International Conference on Network Protocols*, pages 78–87, November 2002.

[SKP$^+$06] Shubhranshu Singh, JaeHoon Kim, Charles E. Perkins, Thomas Heide Clausen, and Pedro M. Ruiz. Ad hoc network autoconfiguration: definition and problem statement. Internet Engineering Task Force, draft-singh-autoconf-adp-03.txt (work-in-progress), March 2006.

[SLD$^+$05] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer. Authenticated routing for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 23(3):598–610, March 2005.

[SVK$^+$04] Csaba Simon, Rolland Vida, Péter Kersch, Christophe Janneteau, and Gösta Leijonhufvud. Seamless IP Multicast Handovers in OverDRiVE. In *Proceedings of the 13th IST Mobile and Wireless Communications Summit*, volume 2, pages 606–610, June 2004.

[TD03] Ole Troan and Ralph Droms. IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6. Internet Engineering Task Force, RFC 3633 (Proposed Standard), December 2003.

[TL05] Mazen Tlais and Houda Labiod. Resource Reservation for NEMO Networks. In *Proceedigns of the International Conference on Wireless Networks, Communications and Mobile Computing*, pages 232–237, June 2005.

[TLN03] Christian Tschudin, Henrik Lundgren, and Erik Nordström. Embedding MANETs in the Real World. In *Personal Wireless Communications (PWC)*, volume 2775 of *Lecture Notes in Computer Science*, pages 578–589. Springer-Verlag Heidelberg, 2003.

[TM04a] Pascal Thubert and Marco Molteni. IPv6 Reverse Routing Header and its application to Mobile Networks. Internet Engineering Task Force, draft-thubert-nemo-reverse-routing-header-05.txt (work-in-progress), June 2004.

[TM04b] Pascal Thubert and Nicolas Montavont. Nested Nemo Tree Discovery. Internet Engineering Task Force, draft-thubert-tree-discovery-01.txt (work-in-progress), October 2004.

[TN98] Susan Thomson and Thomas Narten. IPv6 Stateless Address Autoconfiguration. Internet Engineering Task Force, RFC 2462 (Draft Standard), December 1998.

[TWD05] Pascal Thubert, Ryuji Wakikawa, and Vijay Devarapalli. Global HA to HA protocol. Internet Engineering Task Force, draft-thubert-nemo-global-haha-01.txt (work-in-progress), October 2005.

[USM03] Keisuke Uehara, Hideki Sunahara, and Jun Murai. Problems and tentative solutions in InternetCAR testing with IPv6. In *Proceedings of the Symposium on Applications and the Internet Workshops*, pages 178–183, January 2003.

[vB04] I. van Beijnum. Crypto Based Host Identifiers. Internet Engineering Task Force, draft-van-beijnum-multi6-cbhi-00.txt (work-in-progress), January 2004.

[VBM$^+$05] Pablo Vidales, Carlos J. Bernardos, Glenford Mapp, Frank Stajano, and Jon Crowcroft. A Practical Approach for 4G Systems: Deployment of Overlay Networks. In *Proceedings of the First International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005*, pages 172 – 181, Trento, ITALY, February 2005. Best Paper Award.

[VBS$^+$06] Pablo Vidales, Carlos J. Bernardos, Ignacio Soto, David Cottingham, Javier Baliosian, and Jon Crowcroft. MIPv6 Experimental Evaluation using Overlay Networks. *Computer Networks*, 2006. Accepted to appear.

[vHKBC06] Dirk v. Hugo, Holger Kahle, Carlos J. Bernardos, and María Calderón. Efficient Multicast support within moving IP sub-networks. In *Proceedings of the IST Mobile & Wireless Communications Summit 2006*, Myconos (GREECE), June 2006.

[WKUM03] Ryuji Wakikawa, Susumu Koshiba, Keisuke Uehara, and Jun Murai. ORC: Optimized Route Cache Management Protocol for Network Mobility. In *Proceedings of the 10th International Conference on Telecommunications (ICT)*, volume 2, pages 1194–1200, March 2003.

[WMK$^+$04] Ryuji Wakikawa, Hiroki Matsutani, Rajeev Koodli, Anders Nilsson, and Jun Murai. Mobile Gateway: Integration of MANET and NEMO. In *ACM Mobihoc 2004 Poster*, May 2004.

[WMK$^+$05] Ryuji Wakikawa, Hiroki Matsutani, Rajeev Koodli, Anders Nilsson, and Jun Murai. Mobile Gateways for Mobile Ad-Hoc Networks with Network Mobility Support. In *Proceedings of the 4th International Conference on Networking (ICN)*, pages 361–368, April 2005.

[WOKN05] Ryuji Wakikawa, Kouji Okada, Rajeev Koodli, and Anders Nilsson. Design of vehicle network: mobile gateway for MANET and NEMO converged communication. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 81–82, September 2005.

[WOM05] Ryuji Wakikawa, Yasuhiro Ohara, and Jun Murai. Virtual Mobility Control Domain for Enhancements of Mobility Protocols. In *Proceedigns of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 4, pages 2792–2797, March 2005.

[WS03] Michael Wolf and Michael Scharf. Evaluation of Mobility Management Approaches for IPv6 based Mobile Car Networks. In *Proceedings of the "Kommunikation in verteilten Systemen" KiVS 2003*, February 2003.

[WTD06] Ryuji Wakikawa, Pascal Thubert, and Vijay Devarapalli. Inter Home Agents Protocol Specification. Internet Engineering Task Force, draft-wakikawa-mip6-nemo-haha-spec-01.txt (work-in-progress), March 2006.

[WW04] Ryuji Wakikawa and Masafumi Watari. Optimized Route Cache Protocol (ORC). Internet Engineering Task Force, draft-wakikawa-nemo-orc-00.txt (work-in-progress), July 2004.

[WWEM05] Masafumi Watari, Ryuji Wakikawa, Thierry Ernst, and Jun Murai. Mobility Management for Vehicular Ad Hoc Networks. In *Proceedings of the 62nd IEEE Semiannual Vehicular Technology Conference. VTC 2005-Fall*, volume 4, pages 2302 – 2306, September 2005.

[WYT+05] Ryuji Wakikawa, Tomoyoshi Yokota, Kazuyuki Tasaka, Hiroki Horiuchi, Keisuke Uehara, and Jun Murai. Experimentation of Networked Vehicle with Multihomed Mobile Router. In *Proceedings of the 62nd IEEE Semiannual Vehicular Technology Conference. VTC 2005-Fall*, volume 1, pages 334–338, September 2005.

[Yli05] Jukka Ylitalo. Re-thinking Security in Network Mobility. In *Proceedings of NDSS '05 Wireless and Mobile Security Workshop*, February 2005.

[YOP+05] A. Yegin, Y. Ohba, R. Penno, G. Tsirtsis, and C. Wang. Protocol for Carrying Authentication for Network Access (PANA) Requirements. Internet Engineering Task Force, RFC 4058 (Informational), May 2005.

[ZA02] Manel Guerrero Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In *Proceedings of the 3rd ACM workshop on Wireless security (WiSE '02)*, pages 1–10, 2002.

[ZEB+05] Saber Zrelliand, Thierry Ernst, Julien Bournelle, Guillaume Valadon, and David Binet. Access Control Architecture for Nested Mobile Environments in IPv6. In *Proceedings of the 4th Conference on Security and Network Architecture (SAR)*, June 2005.

[ZH99] Lidong Zhou and Zygmunt J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November/December 1999.

[Zha98] Kan Zhang. Efficient Protocols for Signing Routing Messages. In *Proceedings of Symposium on Network and Distributed Systems Security (NDSS '98)*, March 1998.

[ZR03] Jing Zhu and Sumit Roy. MAC for Dedicated Short Range Communications in Intelligent Transport Systema. *IEEE Communications Magazine*, 41(12):60–67, December 2003.

Acronyms

AODV *Ad hoc On-Demand Distance Vector (AODV) Routing* [PBRD03].

AR *Access Router.*

ARAN *Authenticated Routing for Ad Hoc Networks [SLD^{+}05].*

AS *Authentication Server.*

BC *Binding Cache.* (From [JPA04]) A cache of bindings for other nodes. This cache is maintained by home agents and correspondent nodes. The cache contains both ’correspondent registration’ entries and ’home registration’ entries.

BU *Binding Update*. Signalling message defined in Mobile IPv6 [JPA04] (and also used in the NEMO Basic Support protocol [DWPT05]) to convey location information.

CA *Certification Authority*

CGA *Cryptographically Generated Address* [Aur05].

CN *Correspondent Node.* (From [EL06]) Any node that is communicating with one or more MNNs. A CN could be either located within a fixed network or within another mobile network, and could be either fixed or mobile.

CoA *Care-of Address.* IP address from the visited network acquired by the Mobile Router when the NEMO is away from home, where the routing architecture can deliver packets without additional mechanisms.

CoRE *Care-of Route Error.* Message defined by VARON to announce to a MR that the Care-of Route that is using is broken.

CoRT *Care-of Route Test.* Message defined by VARON to reply to a Care-of Route Test Init (CoRTI) message.

CoRTI *Care-of Route Test Init.* Message defined by VARON to start the discovery and set-up of a Care-of Route.

CR *Correspondent Router.*

DAD *Duplicate Address Detection.*

DHCP *Dynamic Host Configuration Protocol* [DBV^{+}03].

DoS *Denial-of Service.*

DSDV *Destination-sequenced distance vector* ad-hoc routing protocol [PB94].

DSR *Dynamic Source Routing (DSR) Protocol for Mobile Ad Hoc Networks* [JMH04].

DSRC *Dedicated Short Range Communication.*

EP *Enforcement Point.*

FA *Foreign Agent.*

GNU *GNU's not Unix.*

GPL *General Public License.*

GPRS *General Packet Radio Service.*

HA *Home Agent.* Special node located in the Home Network of the NEMO that forwards packets addressed to an MNN to the location of the NEMO, by tunnelling them through the MRHA bidirectional tunnel.

HIP *Host Identity Protocol* [MN05], [MNJH06].

HoAA *Home Address Advertisement.* Message defined by VARON used by the Mobile Routers to periodically advertise their Home Address within the VANET.

HoRT *Home Route Test.* Message defined by VARON to help checking that a Mobile Router is actually managing an associated Mobile Network Prefix.

IETF *Internet Engineering Task Force.*

IGW *Internet Gateway.*

IRTF *Internet Research Task Force.*

ITS *Intelligent Transportation Systems.*

IVAN *Intra-Vehicular Network.*

IVC *Inter-Vehicular Communication.*

LFN *Local Fixed Node.* A fixed node that belongs to a mobile network and is unable to change its point of attachment while maintaining ongoing sessions. Its address is taken from an MNP.

LMN *Local Mobile Node.* A mobile node (MN), assigned to a home link belonging to the mobile network and which is able to change its point of attachment while maintaining ongoing sessions. Its address is taken from an MNP.

MANET *Mobile Ad-hoc Network.*

MIPv6 *Mobile IPv6.* Protocol defined in [JPA04] to provide terminal mobility support.

MIRON *Mobile IPv6 Route Optimisation for NEMO*. Generic Route Optimisation mechanism for Network Mobility designed in this PhD thesis.

MNN *Mobile Network Node*. Any host located within a mobile network, either permanently or temporarily.

MNP *Mobile Network Prefix.* (From [MK04]) A bit string that consists of some number of initial bits of an IP address which identifies the entire mobile network within the Internet topology. All nodes in a mobile network necessarily have an address containing this prefix.

MNPBU *Mobile Network Prefix Binding Update.* Message defined by VARON to update in a Mobile Router the Care-of Route information of a certain Mobile Network Prefix.

MR *Mobile Router.* The router within the mobile network that connects to the Internet is called the Mobile Router (MR).

MRHA *Mobile Router* - *Home Agent* bidirectional tunnel.

NAS *Network Access Server.*

NEMO *NEMO* can mean NEtwork MObility or NEtwork that MOves according to the context. A Mobile Network is (from [MK04]) an entire network, moving as a unit, which dynamically changes its point of attachment to the Internet and thus its reachability in the topology. The mobile network is composed of one or more IP-subnets and is connected to the global Internet via one or more Mobile Routers (MR). The internal configuration of the mobile network is assumed to be relatively stable with respect to the MR.

OLSR *Optimized Link State Routing (OLSR) Protocol* [CJ03].

Originator MR The Mobile Router that starts a VARON Care-of Route discovery and set-up procedure.

PaC *PANA Client.*

PAN *Personal Area Network.*

PANA *Protocol for Carrying Authentication for Network Access.* Protocol designed to facilitate the authentication and authorisation of clients in access networks [FOP$^+$06].

parent-MR The MR of the parent-NEMO.

parent-NEMO The upstream mobile network providing Internet access to another mobile network further down the hierarchy.

RA *Router Advertisement.*

RO *Route Optimisation.*

root-MR The MR of the root-NEMO that connects the nested mobile network to the fixed Internet.

root-NEMO The mobile network at the top of the hierarchy connecting the aggregated nested mobile network to the Internet.

SA *Security Association.*

sub-MR The MR of the sub-NEMO which is connected to a parent-NEMO.

sub-NEMO The downstream mobile network attached to another mobile network up in the hierarchy. The sub-NEMO is getting Internet access through the parent-NEMO and does not provide Internet access to the parent-NEMO.

Target MR The Mobile Router to which a Care-of Route is discovered and set-up by VARON.

TLMR *Top-Level Mobile Router.* See root-MR.

UMTS *Universal Mobile Telecommunications System.*

VANET *Vehicular Ad-Hoc Network.*

VARON *Vehicular Ad-hoc Route Optimisation for NEMO*. Route Optimisation mechanism suited for vehicular environments designed in this PhD thesis.

VMN *Visiting Mobile Node.* A mobile node (MN) assigned to a home link that does not belong to the mobile network and which is able to change its point of attachment while maintaining ongoing sessions. A VMN that is temporarily attached to a mobile subnet (used as a foreign link) obtains an address on that subnet (i.e. the CoA is taken from an MNP).